Comunicação Lógica Digital Relé-A-Relé para Controle, Monitoramento e Proteção de Linhas de Transmissão

Kenneth C. Behrendt
Schweitzer Engineering Laboratories, Inc.

A edição revisada foi lançada em novembro de 1998

Apresentado previamente na
12th Annual CEPSI Exhibition, novembro de 1998,
International Conference Modern Trends in the Protection Schemes of Electric Power Apparatus and Systems, outubro de 1998,
Beijing Electric Power International Conference on Transmission and Distribution, novembro de 1997,
Power Delivery Asia ‘97/DistribuTECH Asia ‘97, setembro de 1997,
51st Annual Georgia Tech Protective Relaying Conference, abril de 1997,
e 23rd Annual Western Protective Relay Conference, outubro de 1996

Originalmente apresentado na
32nd Annual Minnesota Power Systems Conference, outubro de 1996

Traduzido para o português em julho de 2017

COMUNICAÇÃO LÓGICA DIGITAL RELÉ-A-RELÉ PARA CONTROLE, MONITORAMENTO E PROTEÇÃO DE LINHAS DE TRANSMISSÃO

Kenneth C. Behrendt, P.E.
Schweitzer Engineering Laboratories, Inc.
Pullman, Washington USA

INTRODUÇÃO

Engenheiros de proteção, em cooperação com fabricantes de relés de proteção e de produtos de comunicação, se empenharam em alcançar disparos rápidos para todas as faltas em linhas de transmissão através do uso de releamento de proteção com comunicação. Esquemas de distância e de sobrecorrente direcionais, com interfaces de equipamentos de comunicação, enviam e recebem informações lógicas entre relés de terminais para determinar se a falta é externa ou interna à seção da linha protegida. Esquemas de relés tradicionais requerem equipamentos de comunicação externos com certos custos. Este trabalho discute uma nova abordagem para encontrar controle, monitoramento e proteção de linha de alta velocidade, utilizando comunicação lógica digital relé-a-relé microprocessado. Inovadoras aplicações de baixo custo se fizeram possíveis por esta nova capacidade de comunicação e considerações para seleção de canais de comunicação são também apresentadas.

ESTADO LÓGICO DE RELÉS

O estado lógico dos relés é uma parte integral dos esquemas de controle, monitoramento e proteção. Quando dividido com outros relés, o estado lógico de relés formam a base para um esquema que melhora muito a habilidade singular de um relé. O estado lógico dos relés inclui o estado de um elemento do relé (atuado ou desatuado), o estado de um contato de saída (fechado ou aberto), e o estado de uma entrada de controle (presente ou ausente). Em termos de lógica de relé baseado a microprocessador, o estado de um ponto lógico é dado através de um valor lógico, ou binário, 1 ou 0. Este relacionamento digital é a chave para a nova comunicação lógica relé-a-relé discutida neste trabalho.

O exemplo mais comum de estado lógico compartilhado de relé é o esquema de teleproteção "lógico"[1] de linha de transmissão. Relés operando independentemente em cada terminal de linha tem que temporizar o disparo para faltas próximas do terminal oposto da linha para garantir a coordenação com relés nas estações remotas. O compartilhamento do estado lógico dos relés entre cada terminal de linha permite que relés de distância ou de sobrecorrente em ambos terminais de uma linha de transmissão disparem com pequena ou nenhuma temporização intencional para faltas em qualquer lugar da seção de linha protegida. Esta informação lógica compartilhada forma a base dos esquemas de disparo permissivos, esquemas de disparos (diretos ou transferência de disparo) e esquemas de bloqueio de disparo.

[1] Para os objetivos deste trabalho, nós diferenciamos entre esquema de teleproteção de "dados", tais como um esquema de corrente diferencial, que compartilha dados de relé entre relés, e esquema de teleproteção "lógica", que compartilha estados lógicos de relé entre relés.

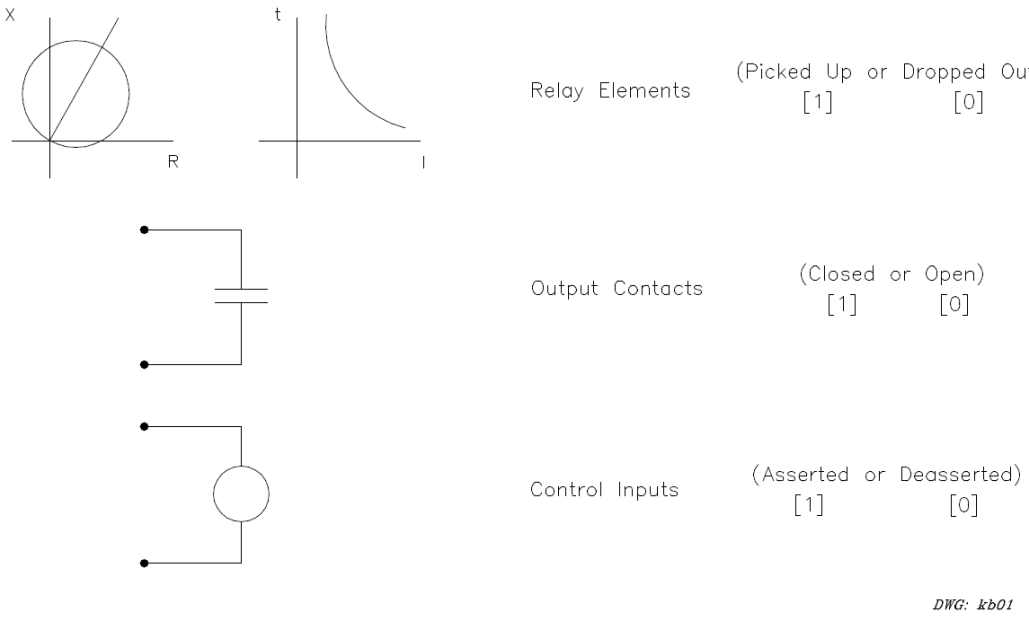


Figura 1: Elementos de Estado Lógico de Relés

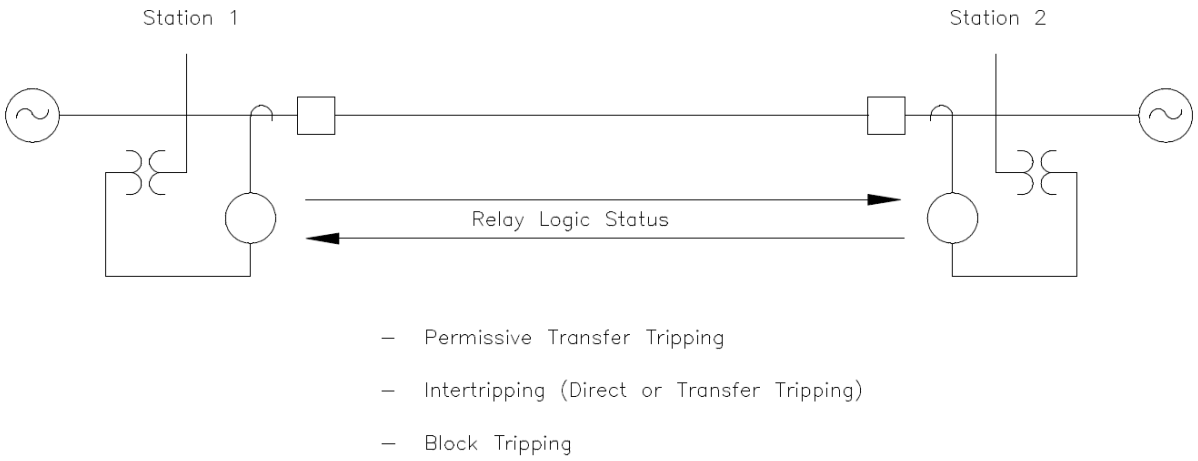


Figura 2: Estados Lógicos Compartilhados de Relés em Esquemas de Teleproteção Lógica

Outras aplicações incluem esquemas de ação corretiva, monitoramento de estado, e controle remoto—efetivamente qualquer aplicação que requer a comunicação de um estado de ponto lógico ou de contato para um local remoto. Esquemas básicos podem somente precisar compartilhar um ponto lógico simples, enquanto esquemas mais complexos podem requerer compartilhamento de múltiplos pontos lógicos.

ESQUEMA DE TELEPROTEÇÃO DE LINHA

Muitos tipos de esquemas de teleproteção de linha estão em uso hoje, incluindo Sobrealcance Permissivo (Permissive Overreaching Transfer Trip - POTT), Subalcance Permissivo (Permissive Underreaching Transfer Trip - PUTT), Comparação Direcional por Bloqueio (Directional Comparison Blocking - DCB), Comparação Direcional por Desbloqueio (Directional Comparison Unblocking - DCUB), Transferência de Disparo Direto por Subalcance (Direct Underreaching Transfer Trip - DUTT), e Transferência de Disparo Direto (Direct Transfer Trip - DTT). Cada um desses esquemas requer que o relé em um terminal se

comunique com o relé no outro terminal que “vê” ou não a falta na direção direta ou reversa. De posse desta informação do relé remoto, cada relé rapidamente toma uma decisão informada de disparo, se a falta é interna à seção da linha protegida, ou de não disparo, se a falta é externa à seção da linha protegida.

Idealmente, nós podemos tentar completar esta comunicação interligando um circuito de controle de um contato de saída de um relé para uma entrada do relé no terminal oposto da linha.

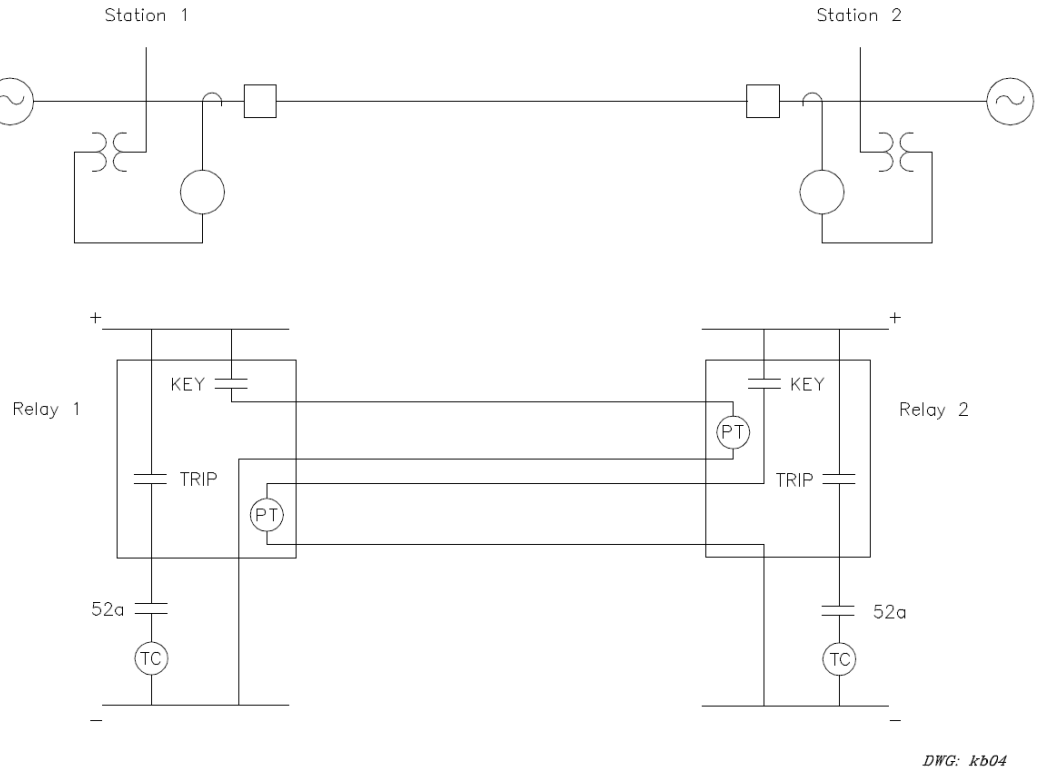


Figura 3: Esquema de Teleproteção de Disparo Permissivo Ideal com Conexões Interligadas

Se esta conexão direta for possível, será permitida uma comunicação simples, rápida, segura e confiável—todos os atributos altamente desejáveis necessários para se alcançar uma proteção de linha rápida, segura e confiável. Adicionar canais de comunicação lógicos seria tão simples quanto interligar um contato adicional de um relé de um terminal a uma entrada de controle no relé de outro terminal.

Infelizmente, as realidades da física nos proíbem de fazer uma conexão de circuito de controle simples, direta, com interligação fiada entre relés. Diferenças de potencial de terra, quedas de tensão e correntes e tensões induzidas apresentam insuperáveis obstáculos a conexão metálica direta. Como resultado, uma variedade de interfaces de comunicação alternativas foram desenvolvidas para se alcançar o resultado desejado : comunicação de estado lógico de relés.

COMUNICAÇÃO LÓGICA DOS ESQUEMAS DE TELEPROTEÇÃO TRADICIONAIS

Efetivamente, todas as técnicas de esquemas de comunicação lógica em serviço hoje foram desenvolvidas durante as eras dos relés eletromecânicos e estáticos, algumas há mais de 40 anos. Os relés de proteção e os equipamentos de comunicação são dispositivos separados e discretos que servem cada um a objetivos únicos. Os dispositivos de proteção e de

comunicação são tipicamente interfaceados com contatos eletromecânicos, apesar de que alguns sistemas de relés estáticos podem usar chaves transistorizadas para interfacear eletronicamente os dispositivos. De qualquer forma, as funções dos dispositivos permanecem separadas e distintas.

A maioria desses esquemas convertem uma saída de contato de relé para um sinal de comunicação seguro e confiável que é transmitido de um terminal de linha para o outro. No terminal receptor, o sinal é convertido para uma saída de contato, que é conectado para ativar uma entrada de controle no esquema lógico do relé.

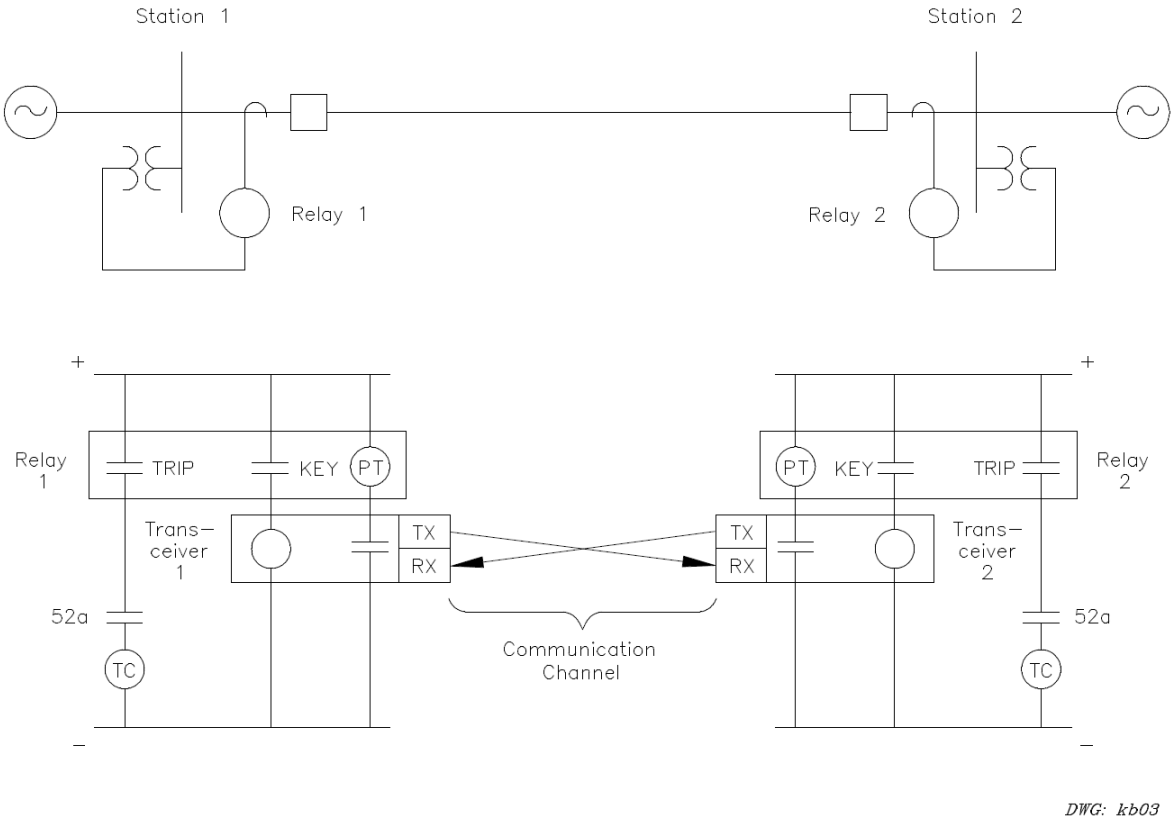


Figura 4: Esquema de Teleproteção de Disparo Permissivo Tradicional com Equipamentos Relé e Comunicação Separados

Equipamentos de comunicação de esquemas de teleproteção tradicionais tipicamente transmitem e recebem sinais de comunicação analógicos. Sinais de áudio-tom (300 a 3.000 Hz) são mais comumente utilizados em circuitos de fonia alugados ou proprietários ou em rádio microondas analógico. A banda de rádio de baixa freqüência (80 a 250 Khz) é comumente utilizada para comunicação carrier PLC (power line carrier). Essas técnicas oferecem isolação metálica e filtragem de sinal para assegurar comunicação segura e confiável relé-a-relé, mas a um custo.

O equipamento de comunicação, que inclui uma combinação de geradores de freqüência, amplificadores, filtros, transformadores de isolamento, lógica eletrônica, relés de saída e entradas de controle, é onerosa, algumas vezes excedendo o custo dos relés de proteção. Engenharia, instalação, espaço de painel, cablagem, ajuste, teste e manutenção para equipamento de comunicação separado aumenta significativamente o custo do equipamento básico. Esses custos são compostos para cada canal de comunicação adicional requerido

Hoje, na moderna era do relé microprocessado, essas técnicas de comunicação tradicionais são ainda amplamente utilizadas :

- o equipamento de comunicação permanece separado e distinto do relé de proteção,
- o contato eletromecânico permanece como interface mais comum entre o relé e o equipamento de comunicação,
- e um equipamento de comunicação adicional e espaço de canal são requeridos para cada bit de estado lógico de relé adicional a ser comunicado.

Todos esses atributos são mantidos desde a era dos relés eletromecânicos.

Este contraste de tecnologias pede por uma nova, inovadora abordagem para simplificar e melhorar o processo de compartilhamento de estados lógicos de relés entre relés de terminais diferentes.

UMA NOVA ABORDAGEM: A COMUNICAÇÃO LÓGICA RELÉ-A-RELÉ

Uma nova, inovadora abordagem tem sido desenvolvida para compartilhar estado lógico de relé entre relés. Esta nova abordagem usa a vantagem da capacidade de comunicação interna e da capacidade de processamento lógico-digital inerente do relé microprocessado. Efetivamente todo relé baseado a microprocessador tem uma porta de comunicação que é capaz de enviar e receber mensagens digitais. E o relé baseado a microprocessador processa dados digitais representando o estado de elementos de medida do relé, entradas de controle e saídas de controle. É apenas natural que estas duas capacidades sejam combinadas para permitir comunicação lógico-digital relé-a-relé direta.

A nova, patenteada técnica de comunicação lógica relé-a-relé envia repetidamente o estado de oito programáveis elementos internos de relé, codificados em uma mensagem digital, de um relé para outro através de uma porta de comunicação serial EIA-232.

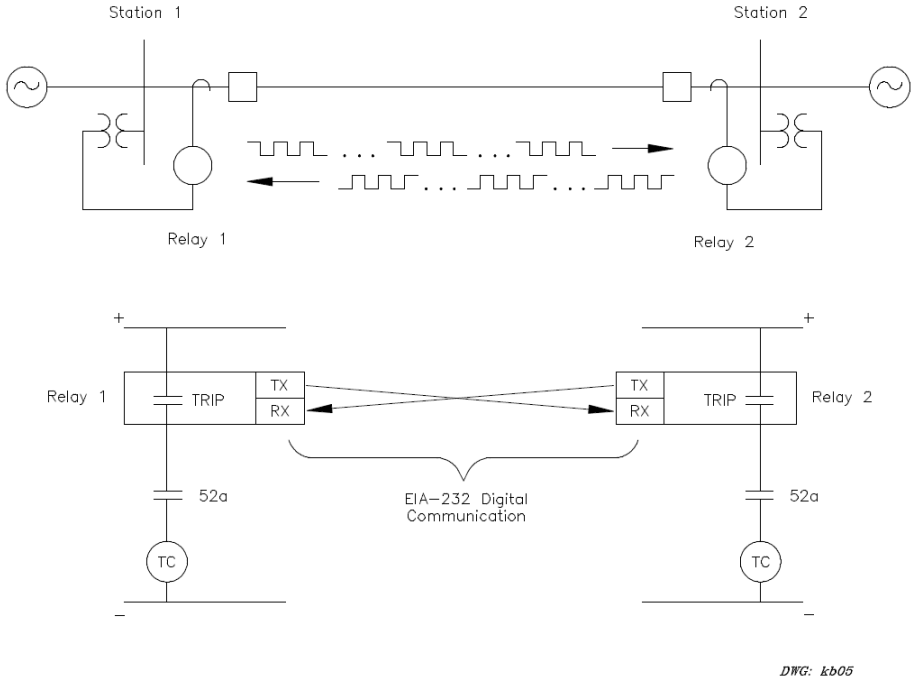


Figura 5: Uma Nova Abordagem: Comunicação Lógica Digital Direta Relé-a-Relé

Esta nova técnica de comunicação lógica relé-a-relé cria oito saídas adicionais “virtuais” em cada relé, “fiadas” através do canal de comunicação a oito entradas de controle “virtuais” no outro relé.

As oito entradas “virtuais”, RMB1 a RMB8, são elementos de relé internos no relé receptor que segue, ou “espelha” (mirrored), os estados respectivos das saídas “virtuais” TMB1 a TMB8 no relé transmissor, como apresentado na figura 6.

Os estados lógicos de cada bit espelhado receptor (Receive Mirrored Bit), RMB1 a RMB8, em um relé “espelha” o estado lógico de cada bit espelhado transmissor (Transmit Mirrored Bit) respectivo, TMB1 a TMB8, no outro relé. Uma alteração no estado de TMB1 do relé 2 de lógico 0 para lógico 1 causa o estado de RMB1 do relé 1 ser alterado de lógico 0 para 1. Isto cria uma conexão virtual entre os dois relés, uma vez que os bits espelhados receptores, RMBs, de um relé seguem o estado dos bits espelhados transmissores, TMBs, do outro relé.

Cada bit espelhado transmissor é programado, tal como você faria com um contato de saída, com uma equação lógica que representa o estado de um elemento de relé interno, entrada de controle, contato de saída, ou qualquer combinação desses. A cada bit espelhado receptor é atribuído uma função, assim como você faria com uma função para uma entrada de controle. Essas parametrizações incluem funções tais como disparo permissivo, bloqueio de disparo, estado do disjuntor 52A, etc.

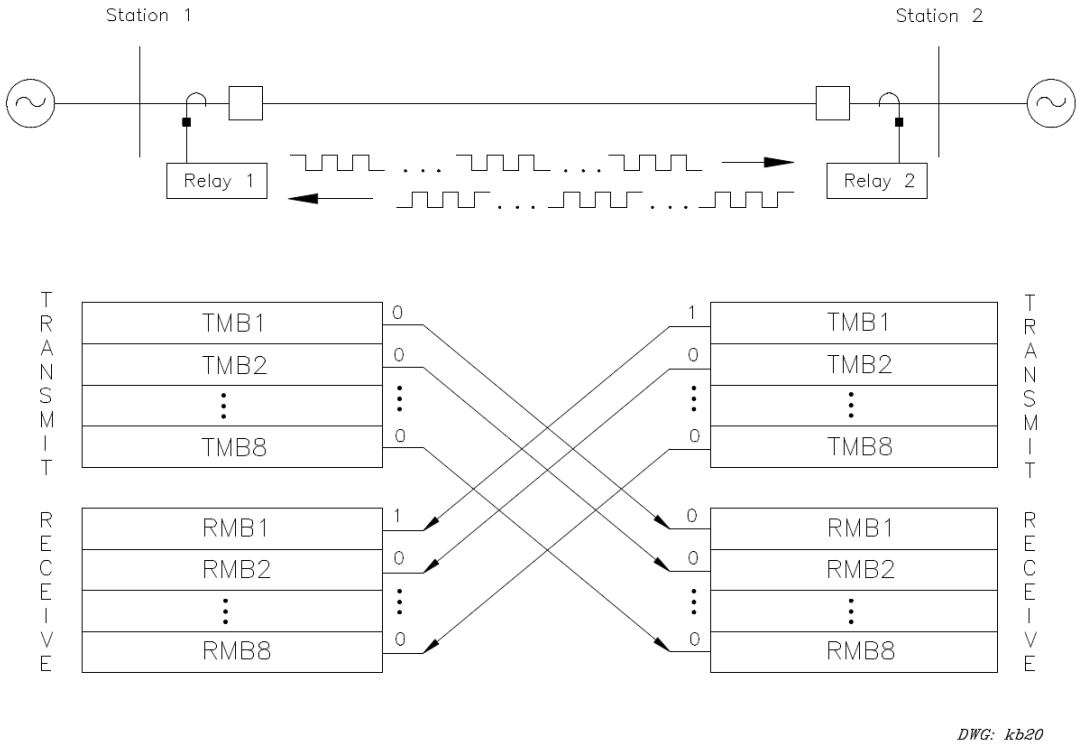


Figura 6: Comunicação Lógica Relé-a-Relé

Esta nova abordagem produz o equivalente a oito canais de comunicação de relés tradicionais entre terminais de relé, aumentando significativamente a funcionalidade e a economia do meio de comunicação. Esta nova abordagem também elimina a necessidade de equipamento de comunicação tradicional oneroso, que é substituído por dispositivos de interface de canal muito mais econômico. As considerações para escolha do meio de comunicação e os dispositivos de interface de canal correspondentes, são discutidos mais tarde neste trabalho.

Segurança e confiabilidade do canal de comunicação são importantes aspectos em esquemas de comunicação tradicionais e eles são igualmente importantes com o novo esquema de comunicação lógica relé-a-relé. Nos esquemas tradicionais, o equipamento de comunicação realiza as verificações de integridade de sinal necessárias antes de entregar a mensagem ao sistema de relé. No novo esquema de comunicação lógica relé-a-relé, o relé assume a responsabilidade pela segurança da mensagem digital.

Segurança da Mensagem Digital

Cada mensagem digital de comunicação lógica relé-a-relé enviada de um relé para outro consiste de dois bytes, onde cada byte contém oito bits de dados. Cada byte da mensagem carrega parte dos oito bits de estado lógico do relé representando o programável estado lógico TMB (Mirrored Bits). A figura 7 mostra a posição relativa do estado de cada bit em cada estrutura de mensagem. O estado de cada bit é representado como um lógico 0 ou 1 na mensagem digital.

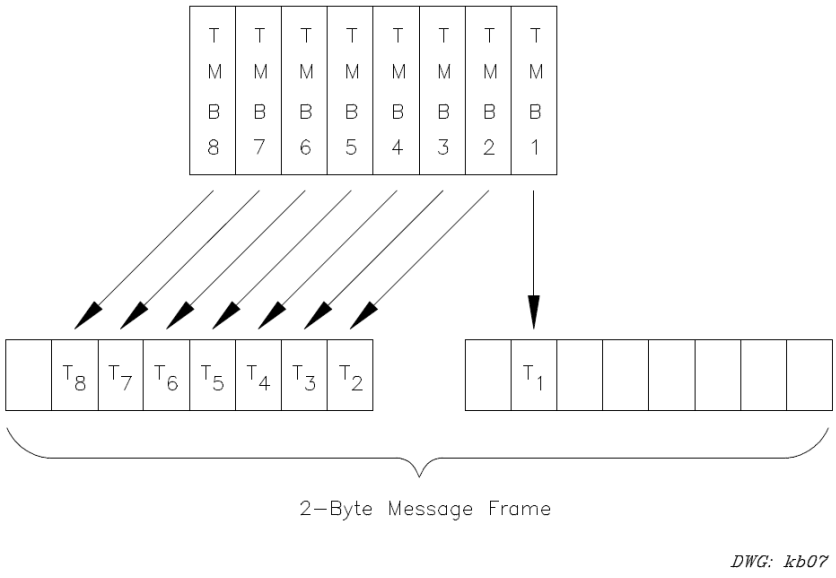


Figura 7: Bits de Estado Lógico de Relé na Estrutura da Mensagem Digital

Medidas de segurança múltiplas são utilizadas para garantir que os oito elementos de estado lógico do relé estão corretamente comunicados de um relé ao outro. Cada byte da mensagem de 2 bytes tem um byte-flag de 1-bit para identificar a seqüência de byte correta. O segundo byte da mensagem inclui uma tabela de verificação de redundância cíclica de 6-bits (Cyclic Redundancy Check - CRC) calculada dos estados dos oito bits de estado lógico do relé.

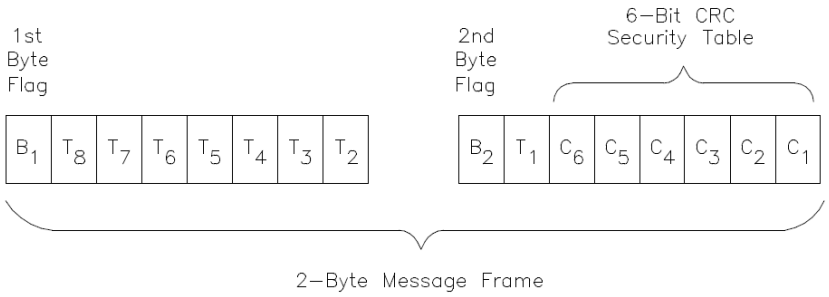


Figura 8: Byte Flag e Bits de Segurança CRC na Estrutura da Mensagem

Cada byte da mensagem assíncrona é precedida por um bit de partida e seguida por até três bits, que podem incluir um ou dois bits de parada e um bit de paridade como mostrado na Figura 9.

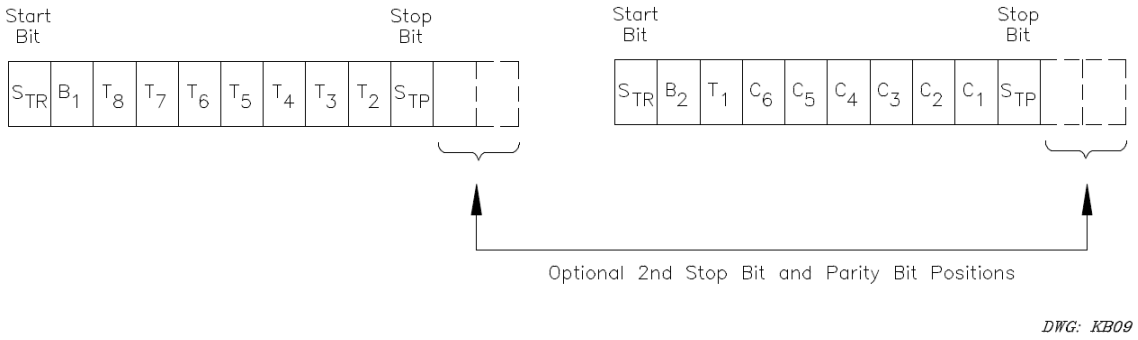


Figura 9: Bits de Estrutura de Mensagem Assíncrona

O relé verifica cada mensagem para ter certeza que os byte flags estão na ordem correta, calcula um valor CRC de uma mensagem recebida e verifica que ele confere com o CRC recebido, verifica a estrutura da mensagem quanto aos bits de partida, de parada e de paridade apropriados e realiza um teste de tempo para garantir que uma mensagem é recebida para cada mensagem enviada. Se alguma destas verificações falha, a mensagem errônea é rejeitada. Por segurança adicional, várias mensagens boas tem que ser recebidas antes que o relé novamente comece a aceitar mensagens e processe os bits de estado lógico.

Controle de Segurança e Confiabilidade

Porque a integridade da mensagem é verificada no relé, um controle apropriado pode ser aplicado para aceitar, rejeitar e temporizar alterações de estado lógico recebidas. Isto permite que você determine o nível de segurança e confiabilidade necessária a sua aplicação particular. Por exemplo, aplicações de disparo direto podem indicar um nível de segurança maior do que aplicações de disparo permissivo. Você pode adicionar segurança para uma aplicação de duas formas:

Introduza um pequeno retardo de tempo de atuação na saída do bit de estado lógico recebido. Este pequeno retardo de tempo de atuação precisa de mais do que uma mensagem de disparo direto para manter a saída de disparo iniciada. E, como mostrado na Figura 10, supervisione a saída de disparo com um bit de segurança de mensagem de relé para garantir que nenhuma saída ocorra a menos que o relé continue a receber mensagens boas.

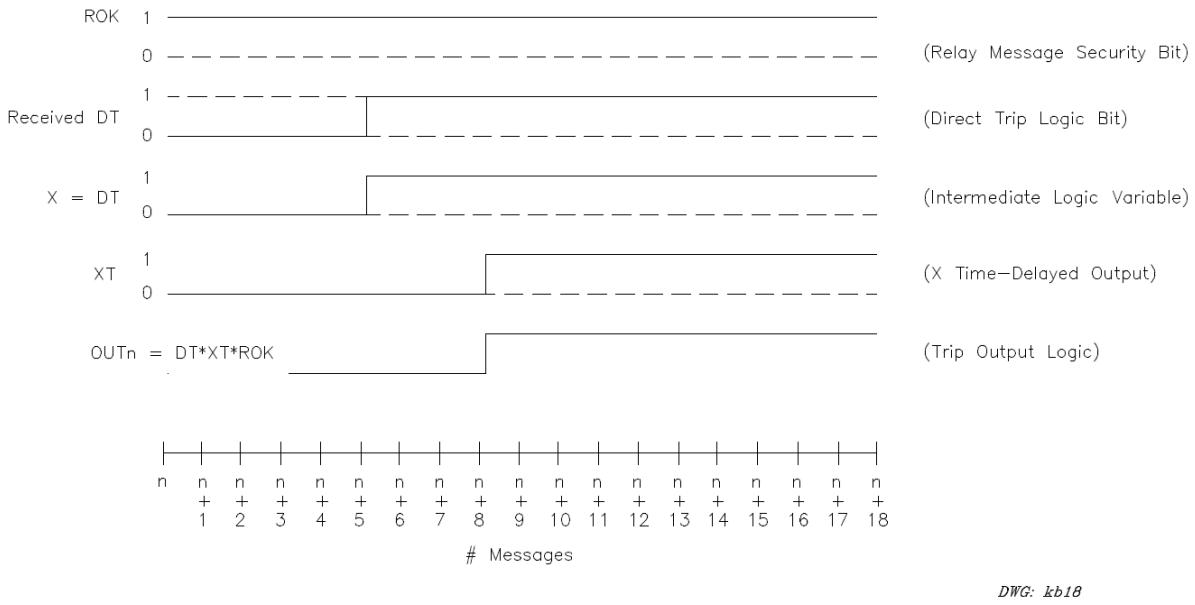


Figura 10: Técnica Lógica de Relé para Aplicações de Esquemas de Teleproteção de Alta Segurança

Ajuste dois ou mais bits de estado lógico transmitidos com a mesma inicial e ajuste os bits de estado lógico receptores correspondentes com saídas diferentes. Então forme um E (*) com os bits de estado lógico receptores juntos para formar a saída como mostrado na tabela abaixo:

Relé 1	Relé 2
TMB1 = 3PT	RMB1 = DT
TMB2 = 3PT	RMB2 = LP1
	OUT1 = DT *LP1

A confiabilidade é melhorada permitindo-se ação mesmo quando mensagens ruins ocasionais são recebidas, como é tipicamente feito com esquemas de disparo permissivo onde você espera que uma falta na linha pode afetar indevidamente o canal de comunicação. Você pode permitir disparo se mensagens ruins ocorrerem coincidentemente com detecção de falta utilizando a lógica de relé mostrada na Figura 11. Com esta lógica, a saída de relé receptor é permitida operar se o elemento de distância por sobrealcance de Zona 2, de fase (M2P) ou de terra (Z2G), operam no mesmo instante que o canal de comunicação se perde. Uma saída temporizada (YT) é utilizada para limitar a duração do disparo permitido.

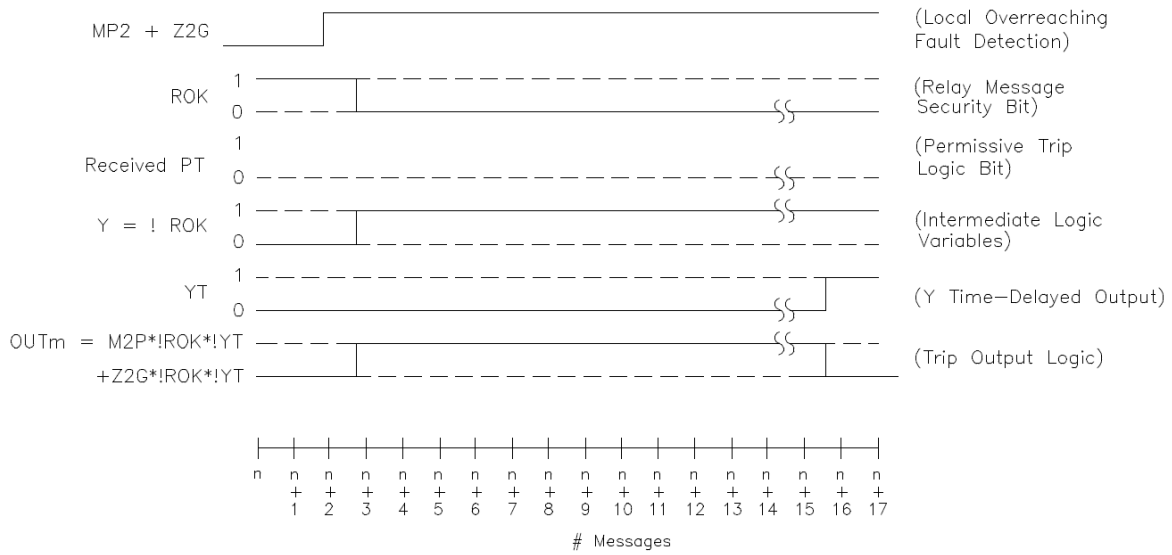


Figura 11: Técnica Lógica de Relé para Confiáveis Aplicações de Esquemas de Teleproteção

Desempenho da Comunicação Lógica Relé-a-Relé

O desempenho da nova técnica de comunicação lógica relé-a-relé se compara favoravelmente com esquemas de comunicação tradicionais, apesar de que alguns parâmetros poderem não ser diretamente comparáveis. Velocidade, que é uma medida do tempo que se leva para ativar um elemento no relé receptor após o início da alteração de estado lógico no relé transmissor, pode ser o aspecto mais comparável. Em termos gerais, o tempo de operação nominal ponto-a-ponto é 6,3 milisegundos na taxa de comunicação de 9.600 ou 19.200 bits por segundo. Este tempo de operação ponto-a- ponto não inclui os tempos de propagação e de interface de canal, que serão afetados pela escolha do canal de comunicação, como será discutido mais tarde neste trabalho.

Em comparação, equipamento típico de tom de áudio tem um tempo de operação ponto-a-ponto de 8 a 12 mseg, dependendo da largura da banda. Isto não inclui o tempo de operação dos contatos de saída do relé de inicialização e o tempo de processamento da entrada de controle no relé receptor, que pode somar vários milisegundos. O tempo de propagação do canal afetará também indevidamente a velocidade de operação global.

	Comunicação Analógica Tradicional	**Comunicação Digital Relé-a-Relé**
Tempo do contato de saída do relé	3,5 mseg	Nenhum
Tempo de operação ponto-a-ponto	8 – 12 mseg[1]	4,2 – 6,3 mseg[2]
Tempo de processamento da entrada de controle do relé	2,1 mseg	2,1 mseg
	13,6 – 17,6 mseg	6,3 – 8,4 mseg

1) 8 mseg para banda larga, 12 mseg para banda estreita
2) 9.600 baud

Figura 12: Comparação de Velocidade: Tradicional Versus Lógica Digital Relé-a-Relé

Segurança e confiabilidade da nova técnica de comunicação lógica relé-a-relé são muito mais difíceis de relacionar aos esquemas de comunicação tradicionais. Esquemas tradicionais utilizando sinais de comunicação analógicos medem o desempenho do canal em termos da relação sinal/ruído (SNR). Potência de saída do transmissor analógico e a sensibilidade da entrada do receptor são medidas em decibéis (db). O receptor tem que distinguir entre sinal bom e ruído indesejado. A habilidade para fazer esta distinção depende fortemente do projeto do receptor, que está fora do escopo deste trabalho. Para a maior parte, a segurança e a confiabilidade de esquemas de comunicação analógicos tradicionais não são um assunto importante.

Em comunicação digital, o desempenho do canal é medido em Razão de Erro do Bit (BER), expresso em número de erros de bit por número de bits transmitidos. Um erro de bit é um bit invertido, onde um bit transmitido como um lógico "1" é recebido como um lógico "0", ou vice-versa. Não é raro para canais de comunicação digital ter uma 109 BER, que significa que, na média, existe 1 erro de bit ou 1 bit invertido para cada um bilhão de bits transmitidos.

Como discutido anteriormente, o novo esquema de comunicação lógica relé-a-relé aplica verificações de segurança de mensagem múltiplas, incluindo uma verificação de redundância cíclica de 6 bits (6-bit Cyclic Redundancy Check - CRC), para verificar erros de bit. O polinômio geral para um 6-bit CRC é:

$$g(x) = x^6 + x^5 + x = 1 \qquad \text{Equação 1}$$

Os 6 bits CRC detectarão todas as possíveis combinações de um, dois ou três bits invertidos na mesma mensagem. Algumas combinações de quatro ou mais bits invertidos na mesma mensagem podem ir sem serem detectadas. Por esta razão, é importante entender a probabilidade desses erros não detectados. A probabilidade de uma mensagem ruim ficar não detectada pode ser analisada utilizando-se técnicas de probabilidade estatística. Análise de probabilidade para segurança e confiabilidade de canal está incluída nos Apêndices A e B. Os resultados claramente mostram que segurança de canal de comunicação lógica relé-a-relé é aproximadamente unitária (1,0) sobre uma grande faixa de Razão de Erro de Bit (BER). Da mesma forma, confiabilidade de canal de comunicação se aproxima da unidade para BER menor do que 10^{-4}, que é um BER relativamente alto, indicativo de um canal de comunicação pobre.

APLICAÇÕES DE ESQUEMAS DE TELEPROTEÇÃO APRIMORADOS COM COMUNICAÇÃO LÓGICA RELÉ-A-RELÉ

Aplicações de esquemas de teleproteção tradicionais transmitem um bit de estado lógico entre terminais de relés. A nova técnica de comunicação lógica relé-a-relé, com a habilidade para transferir até oito bits de estado lógico em uma mensagem, expande enormemente a capacidade do esquema de teleproteção para realizar outras funções. Para efeito de comparação, nós examinamos um típico esquema de transferência de disparo por sobrealcance permissivo para ver o quão fácil este esquema é aprimorado para completar outras funções.

Esquema Básico de Transferência de Disparo por Sobrealcance Permissivo

No esquema básico de teleproteção com transferência de disparo por sobrealcance permissivo, o elemento de sobrealcance Zona 2 comanda a lógica de disparo permissivo para o terminal remoto, permitindo ao relé remoto disparar seu disjuntor se ele vê uma falta na direção direta. O esquema também comanda a lógica de disparo permissivo se o disjuntor local está aberto (!52AA1 = NOT 52A).

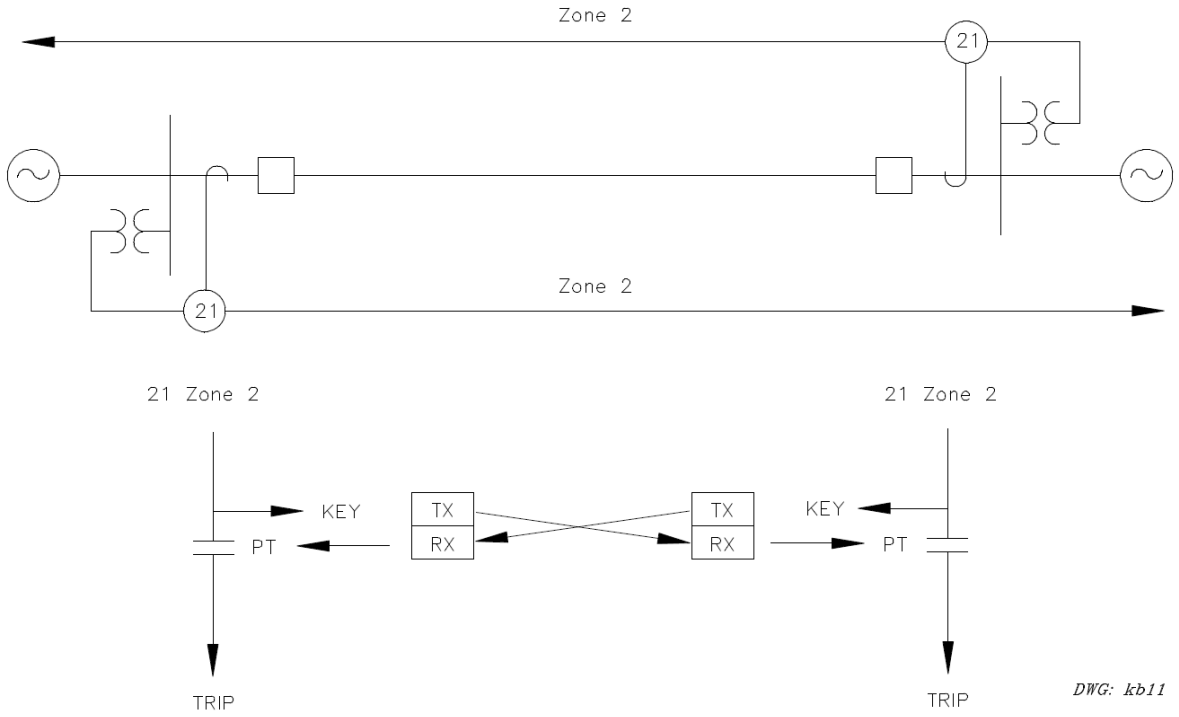


Figura 13: Esquema Básico de Teleproteção com Transferência de Disparo por Sobrealcance Permissivo

Esta lógica básica é implementada com a comunicação lógica relé-a-relé utilizando-se os parâmetro de estado lógico transmitidos e recebidos mostrados na Tabela 1. Todos os outros elementos de estado lógicos relé-a-relé TMB2 a TMB8 e RMB2 a RMB8, não são parametrizados (na).

Tabela 1: Ajustes da Comunicação Lógica Relé-a-Relé de Transferência de Disparo por Sobrealcance Permissivo

Relay 1	**Relay 2**
Transmit Logic	**Transmit Logic**
7TMB1 = **KEY + !52AA1**	TMB1 = **KEY + !52AA1**
TMB2 … 8 = na	TMB2 … 8 = na
Receive Logic	**Receive Logic**
RMB1 = **PT**	RMB1 = **PT**
RMB2 … 8 = na	RMB2 … 8 = na
Partial Output Logic	**Partial Output Logic**
OUT1 = **3PT**	OUT1 = **3PT**

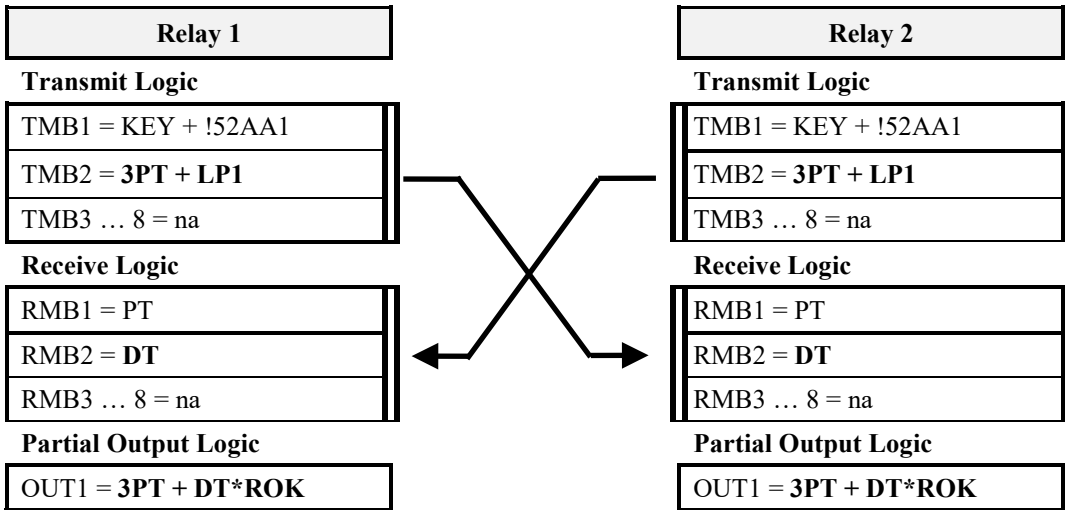
Ajustar o bit TMB1 como KEY é equivalente a se conectar o contato de saída do relé de sobrealcance Zona 2 na entrada de chaveamento num dispositivo de comunicação. Da mesma forma, ajustar RMB1 como PT é equivalente a conectar o contato de saída do dispositivo de comunicação em uma entrada de disparo permissivo no esquema do relé. Neste exemplo, o contato de saída do relé OUT1 é conectado para disparar o disjuntor local quando a lógica de disparo tripolar do relé (3PT) atua.

POTT Mais Transferência de Disparo Direto

A lógica do esquema básico POTT é facilmente aprimorada utilizando-se comunicação lógica relé-a-relé. Por exemplo, para garantir que o disjuntor do terminal de linha remoto dispare quando o relé local dispara o disjuntor local, você pode estabelecer um canal de transferência de disparo direto utilizando-se um outro bit de comunicação lógico transmitido e recebido. Para completar isto, simplesmente ajuste TMB2 = 3PT para ativar TMB2 quando a lógica de disparo tripolar do relé local atua e ajuste o associado RMB2 = DT para ativar a lógica de disparo direto quando o bit de RMB2 atua. Então programe o contato de saída de disparo do disjuntor para operar para qualquer atuação de elemento 3PT ou (+) DT. Você pode aumentar um nível de segurança a saída de transferência de disparo direto através de uma lógica E (AND) com DT e o elemento de estado de comunicação lógica relé-a-relé, ROK. Enquanto as mensagens continuam a passar todas as verificações de segurança, ROK permanece atuado. Quando uma mensagem ruim é detectada, esta mensagem é rejeitada e ROK desatua.

Da mesma forma, se incrementa funções de transferência de disparo direto para operações de relés de transformadores, barras ou de falha de disjuntor simplesmente através de uma lógica OU (OR) com suas respectivas entradas de relé (LP1 mostrada neste exemplo) e o elemento 3PT no ajuste TMB2.

Tabela 2: POTT mais Lógica de Esquema de Teleproteção por Transferência de Disparo Direto



POTT mais DT mais Bloqueio de Religamento Remoto

Um outro aprimoramento de esquema de teleproteção que é fácil de se realizar com comunicação lógica relé-a-relé é o bloqueio de religamento remoto. Após disparar ambos terminais da linha por uma falta, o religamento automático é utilizado para fechar ambos disjuntores da linha. Por escalonamento dos tempos de religamento, você pode utilizar a lógica relé-a-relé para bloquear remotamente a operação de religamento do segundo terminal se o primeiro terminal fecha sob uma falta. Essa lógica utiliza o elemento lógico de fechamento sob falta do relé, SOTFE, em combinação com o elemento de disparo tripolar, 3PT, para ativar um dos bits lógicos transmissores do relé (TMB3 nesse exemplo). Isto, no retorno, ativa o bit lógico receptor associado, RMB3, no relé remoto, que é parametrizado para um elemento de entrada programável, LP2.

O elemento de entrada programável, LP2, é então utilizado para bloquear o religamento—internamente se a lógica de religamento for programada no relé ou externamente, através de um contato de saída, se um relé de religamento separado for utilizado.

Tabela 3: POTT mais DT mais Lógica de Esquema de Teleproteção de Bloqueio de Religamento (RB)

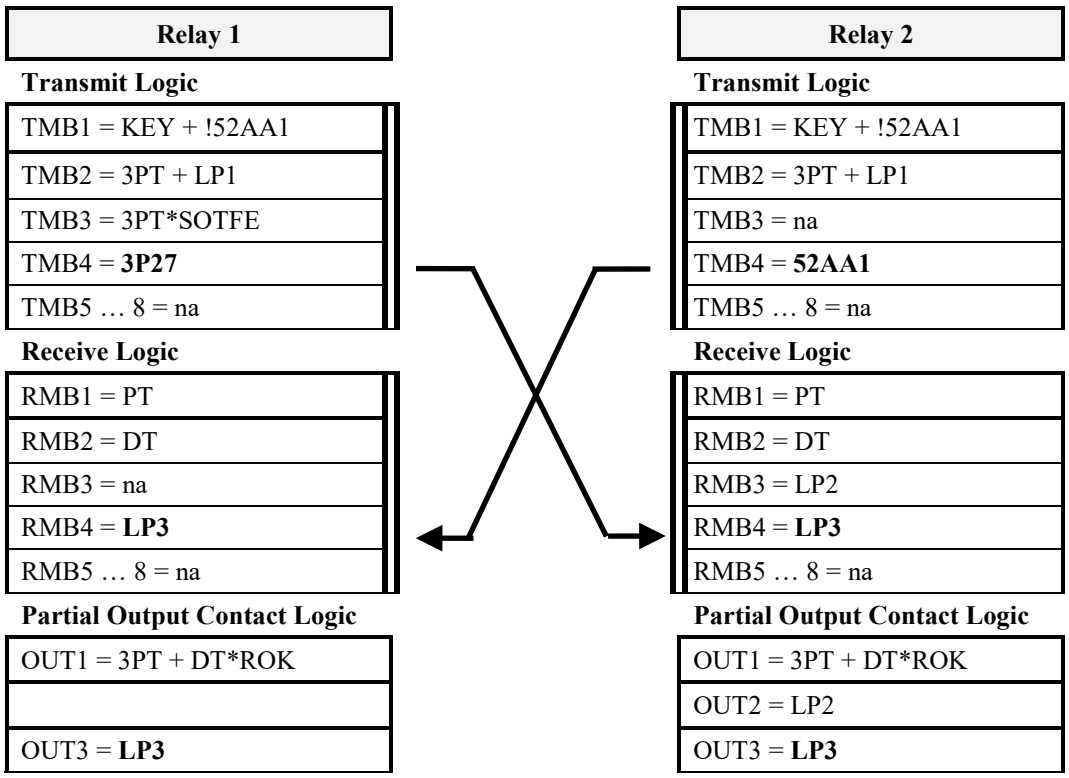
Relay 1	Relay 2
Transmit Logic	**Transmit Logic**
TMB1 = KEY + !52AA1	TMB1 = KEY + !52AA1
TMB2 = 3PT + LP1	TMB2 = 3PT + LP1
TMB3 = **3PT*SOTFE**	TMB3 = na
TMB4 … 8 = na	TMB4 … 8 = na
Receive Logic	**Receive Logic**
RMB1 = PT	RMB1 = PT
RMB2 = DT	RMB2 = DT
RMB3 = na	RMB3 = **LP2**
RMB4 … 8 = na	RMB4 … 8 = na
Partial Output Contact Logic	**Partial Output Contact Logic**
OUT1 = 3PT + DT*ROK	OUT1 = 3PT + DT*ROK
	OUT2 = **LP2**

Monitoramento Remoto

É freqüentemente desejável se monitorar remotamente o estado de um dispositivo, tal como um disjuntor de linha, ou uma condição, tal como subtensão de barra, no terminal remoto de linha. Isso tem aplicações para proteção, controle ou monitoramento e é facilmente realizada com comunicação lógica relé-a-relé. Simplesmente programe o bit lógico transmissor com o elemento de relé apropriado, seja interno ou externo e atribua ao bit lógico receptor no relé remoto com uma entrada lógica. Utilize a entrada lógica atribuída em uma equação de controle interna ou ajuste um contato de saída para seguir a entrada remota, como mostrado nesse exemplo.

Neste exemplo, nós utilizamos o Relé 1 para monitorar remotamente o estado do disjuntor 52a no terminal de linha do Relé 2 e na outra direção, nós utilizamos o Relé 2 para monitorar remotamente o estado da tensão da barra no terminal de linha do Relé 1. O estado do disjuntor 52a é representado por uma entrada de controle do contato do disjuntor 52a representada por um elemento de relé interno 52AA1, no Relé 2, e o estado da tensão de barra é representado por um elemento de subtensão trifásica, 3P27, no Relé 1.

Tabela 4: POTT mais DT mais RB mais Monitoramento Remoto (RM)



Relay 1	Relay 2
Transmit Logic	**Transmit Logic**
TMB1 = KEY + !52AA1	TMB1 = KEY + !52AA1
TMB2 = 3PT + LP1	TMB2 = 3PT + LP1
TMB3 = 3PT*SOTFE	TMB3 = na
TMB4 = **3P27**	TMB4 = **52AA1**
TMB5 … 8 = na	TMB5 … 8 = na
Receive Logic	**Receive Logic**
RMB1 = PT	RMB1 = PT
RMB2 = DT	RMB2 = DT
RMB3 = na	RMB3 = LP2
RMB4 = **LP3**	RMB4 = **LP3**
RMB5 … 8 = na	RMB5 … 8 = na
Partial Output Contact Logic	**Partial Output Contact Logic**
OUT1 = 3PT + DT*ROK	OUT1 = 3PT + DT*ROK
	OUT2 = LP2
OUT3 = **LP3**	OUT3 = **LP3**

Alteração Remota de Ajuste

Conecte um contato de uma chave de controle ou um contato de controle de uma RTU SCADA, em uma entrada de controle de um relé em um terminal de linha e programe a entrada para alterar os ajustes nos relés local e remoto ao mesmo tempo. Da mesma forma, utilize um elemento interno de relé ou um contato de dispositivo da subestação, para alterar automaticamente os ajustes de relé local e remoto para criar um esquema de relé adaptativo. A tabela 5 mostra um exemplo onde TMB5 é ajustado para seguir um bit programável, LP4, que é parametrizado para monitorar uma entrada de controle de relé. Quando LP4 ativa, o elemento lógico local TMB5 ativa o elemento lógico remoto RMB5, que é programado como uma entrada de chave seletora de ajuste, SS1. Quando esse elemento ativa, o relé altera o grupo de ajustes baseado em uma tabela de posição da chave seletora predeterminada.

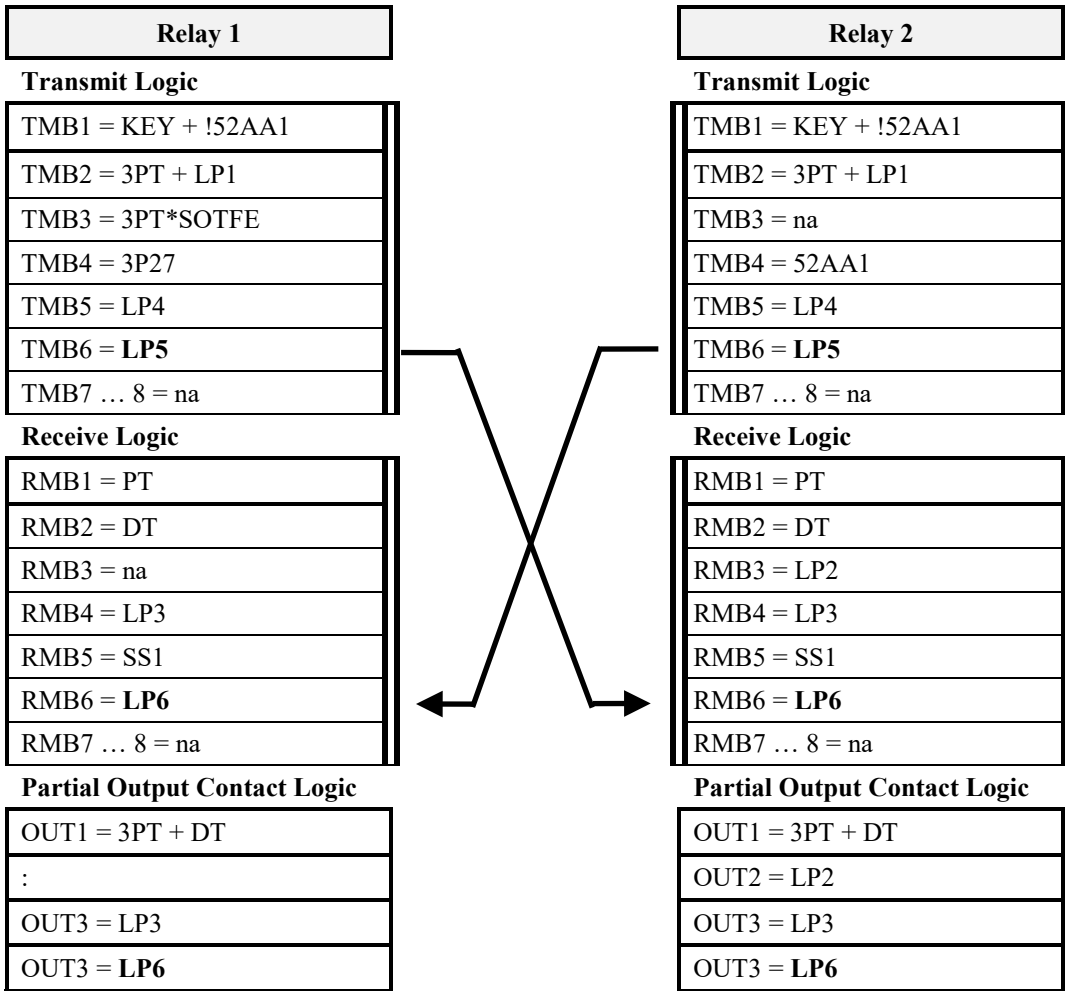
Tabela 5: POTT mais DT mais RB mais RM mais Alteração de Ajuste Remoto (RSC)

Relay 1	Relay 2
Transmit Logic	**Transmit Logic**
TMB1 = KEY + !52AA1	TMB1 = KEY + !52AA1
TMB2 = 3PT + LP1	TMB2 = 3PT + LP1
TMB3 = 3PT*SOTFE	TMB3 = na
TMB4 = 3P27	TMB4 = 52AA1
TMB5 = **LP4**	TMB5 = **LP4**
TMB6 … 8 = na	TMB6 … 8 = na
Receive Logic	**Receive Logic**
RMB1 = PT	RMB1 = PT
RMB2 = DT	RMB2 = DT
RMB3 = na	RMB3 = LP2
RMB4 = LP3	RMB4 = LP3
RMB5 = **SS1**	RMB5 = **SS1**
RMB6 … 8 = na	RMB6 … 8 = na
Partial Output Contact Logic	**Partial Output Contact Logic**
OUT1 = 3PT + DT*ROK	OUT1 = 3PT + DT*ROK
	OUT2 = LP2
OUT3 = LP3	OUT3 = LP3

Controle Remoto

Assim como nós utilizamos a nova lógica relé-a-relé para alterar remotamente ajustes de relé no exemplo anterior, a mesma técnica é utilizada para controlar remotamente um dispositivo no terminal oposto da linha e subestação. Um contato de chave de controle, contato de controle RTU SCADA, contato de controle de dispositivo é conectado a uma entrada de controle do relé, atribuída como LP5 nesse exemplo, que é programada para ativar um bit de estado lógico transmissor, TMB6. TMB6, de volta, ativa a entrada de estado lógico receptor remoto, RMB6. A entrada de estado lógico RMB6 é parametrizada para ativar o elemento de entrada programável LP6, que, de volta, é programado para operar o contato de saída OUT3 quando a entrada de controle remoto é ativada. O contato de saída do relé é conectado para controlar um dispositivo da subestação, tal como um disjuntor

Tabela 6: POTT mais DT mais RB mais RM mais RSC mais Controle Remoto (RC)



Resumo

Para resumir nosso exemplo, nós temos realizado várias funções de esquema de teleproteção típicas com um canal de comunicação conectado diretamente entre relés de cada terminal da linha como mostrado na Figura 14, abaixo. De fato, nós temos elementos de estado lógico relé-a-relé sobressalentes disponíveis para outras funções, ou esses elementos sobressalentes podem ser utilizados para aumentar a segurança das funções de disparo direto, como discutido anteriormente.

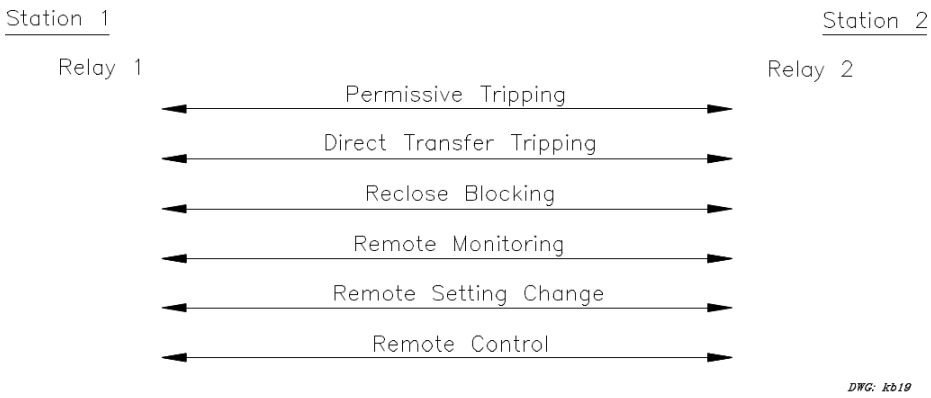


Figura 14: Resumo do Exemplo de Comunicação Lógica Relé-a-Relé

CONSIDERAÇÕES SOBRE CANAL DE COMUNICAÇÃO PARA A LÓGICA RELÉ-A-RELÉ

Comunicação Digital Direta via Cabo de Fibra-Ótica

A Comunicação lógica digital direta relé-a-relé via fibra direta supera os problemas de aumento de potencial de terra e problemas de interferência encontrados com cabos metálicos. Um transdutor de fibra-ótica é utilizado em cada terminal de relé para converter o sinal EIA-232 do relé em um sinal ótico que pode ser transmitido pelo cabo de fibra-ótica. Cabos de fibra-ótica e tecnologias de transdutores multimodo atuais suportam transmissão de sinal ótico até dois ou três milhas (3 a 5 quilômetros). Transmissão de distâncias mais longas, de várias milhas até mais de 50 milhas, é alcançada utilizando-se cabos e transdutores óticos monomodo. Os custos atuais dos transdutores de fibra-ótica variam de poucas dezenas de dólares para cada transdutor multimodo a cerca de mil dólares ou mais para cada transdutor monomodo.

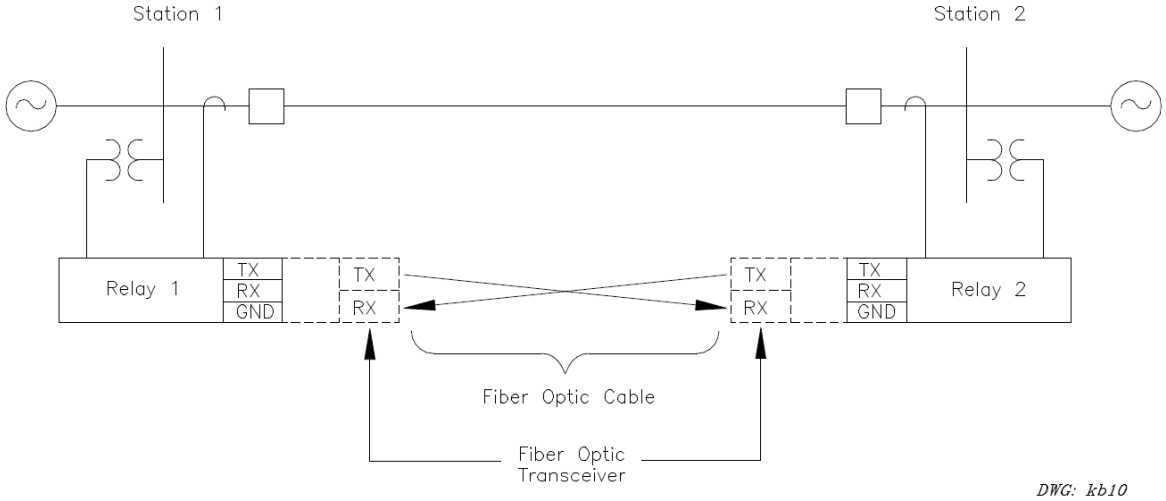


Figura 15: Comunicação Digital Direta via Cabo de Fibra-Ótica Direto

Comunicação por cabo de fibra-ótica direto é o mais simples e o mais claro meio de comunicação lógica relé-a-relé. É virtualmente imune a interferência elétrica e tipicamente tem uma taxa de erro de bit menor do que 10^{-9}. O retardo de tempo de dados nos transdutores de fibra-ótica e cabos óticos é tipicamente medido nas dezenas de microsegundos ou menos, que é desprezível comparado com a taxa de transferência de dados entre relés.

Comunicação Digital via Multiplexadores de Comunicação do Sistema

Multiplexadores de comunicação fazem a interface de canais de comunicação individuais com um sistema de comunicação que podem conduzir muitos canais de comunicação. O meio do sistema de comunicação pode ser constituído de fibras-óticas e/ou microondas. A topologia do sistema usualmente tem vários nós de comunicação, onde canais são inseridos ou retirados e podem estar ligados para permitir caminhos alternativos se um segmento do sistema falha ou é colocado fora de serviço para manutenção.

A comunicação lógica relé-a-relé é interligada ao multiplexador do sistema de comunicação através de um cartão EIA-232 inserido no rack do multiplexador como mostrado na Figura 16. A porta de comunicação serial do relé é conectada ao cartão de interface EIA-232 do multiplexador com um cabo metálico blindado ou um cabo de fibra- ótica com transdutor de fibra-ótica. A comunicação de fibra-ótica é recomendada entre o relé e o multiplexador para eliminar qualquer efeito de interferência elétrica do ambiente da subestação.

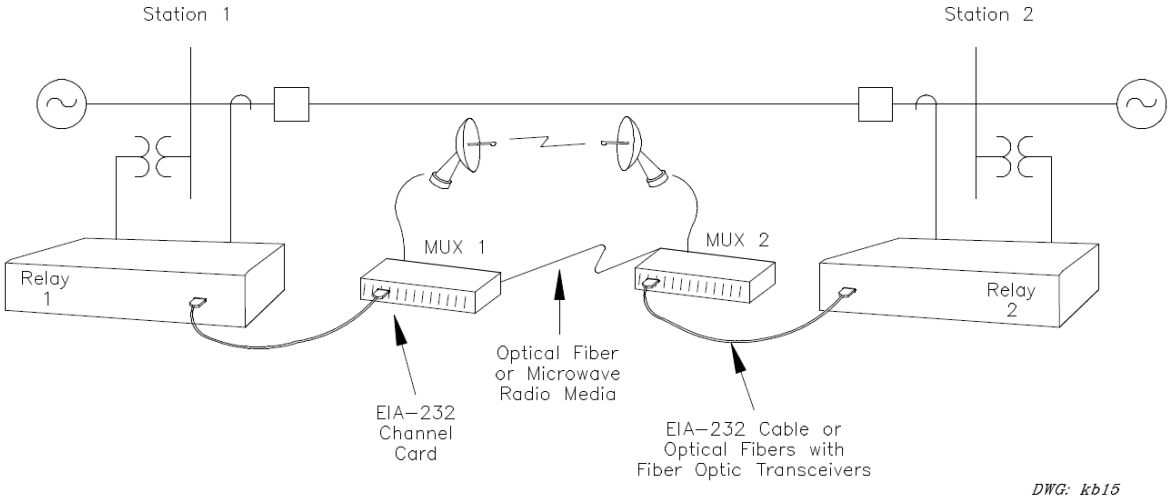


Figura 16: Comunicação Digital via Multiplexadores do Sistema de Comunicação

Administração do sistema, tal como endereçamento e sincronismo são conduzidos no multiplexador do sistema. Alguns multiplexadores de sistema também realizam verificação de erro. Se perde-se o canal devido a falha ou erro de dados, os multiplexadores de sistema tem que "re-sincronizar" o caminho de comunicação de sinal antes que o canal seja recuperado. Este tempo de re-sincronismo depende do tipo do equipamento multiplexador e da técnica de 'chaveamento" utilizada. As técnicas de chaveamento mais simples precisam somente de uns poucos milisegundos para re- sincronizar, enquanto aqueles com sinais de concordância mais complexos podem levar até 60 milisegundos para re-sincronizar.

Multiplexadores de sistema que realizam detecção de erro podem causar retardos de tempo nos dados que afetam o tempo de resposta lógica do relé ponta-a-ponta. Verifique com o fabricante do equipamento de comunicação informações sobre retardos de tempo de dados.

Comunicação Digital via Rádio Digital Ponto-a-Ponto

Rádio digital ponto-a-ponto fornece comunicação única entre duas áreas. Rádios são disponíveis para operar na banda de freqüência de 900 MHz com relativamente baixa potência nominal que podem não requerer licenciamento especial, e tem uma faixa de operação de cerca de 20 a 30 milhas, de linha de campo. Os rádios incluem um transdutor EIA-232 para interligar com a porta de comunicação serial EIA-232 do relé em taxas de até 9.600 baud.

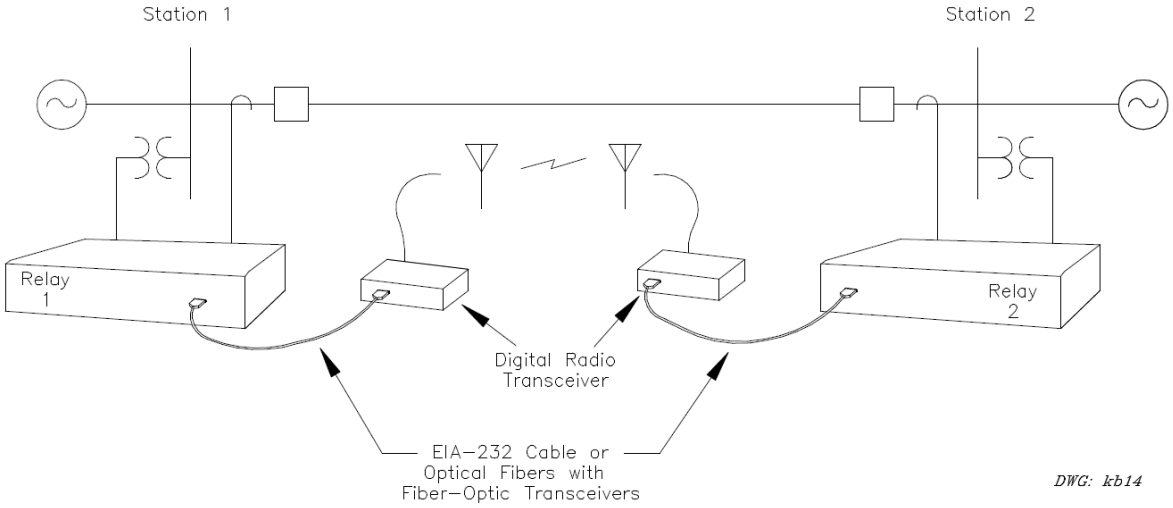


Figura 17: Comunicação Digital via Rádio Digital Ponto-a-Ponto

Rádios sem detecção de erro embutido trabalham melhor com comunicação lógica relé- a-relé porque eles adicionam somente dois ou três milisegundos ao retardo de tempo global de comunicação de dados relé-a-relé. Aqueles rádios que tem detecção de erro embutido podem introduzir retardos de tempo de 60 milisegundos ou mais. Porque velocidade é um aspecto muito crítico da maioria dos esquemas de teleproteção, certifique-se de verificar as especificações do rádio cuidadosamente em relação às características de retardo de tempo do sistema de rádio.

Comunicação Digital via Canal de Comunicação Digital Compartilhada

Nota Editorial: **Esta aplicação não é mais recomendada pela Schweitzer Engineering Laboratories, Inc., favor contatar a fábrica para mais detalhes.**

Uma outra alternativa de comunicação relé-a-relé é compartilhar um canal de comunicação digital dedicado de um provedor de serviços local (companhia telefônica). O canal de comunicação digital dedicado é tipicamente fornecido na forma de um circuito de comunicação metálico a quatro fios da unidade central mais próxima, similar a um canal de comunicação analógico. O canal de comunicação digital, referido como um canal DS0, tem capacidade de comunicação de 56 kilobits por segundo, que é mais do que suficiente para a taxa de comunicação serial de 9.600 ou 19.200 baud no relé.

A porta de comunicação serial do relé é interligada com o canal de comunicação digital compartilhado através de um dispositivo digital de acesso de serviço chamado Unidade de Serviço de Canal/Unidade de Serviço de Dados (Channel Service Unit/Data Service Unit - CSU/DSU) na América do Norte ou Unidade Terminal de Linha (Line Terminating Unit - LTU) na Europa.

Os dispositivos digitais de acesso de serviço realizam duas funções. A interface digital ao equipamento do cliente (EIA-232 neste caso) é realizada pela parte DSU da unidade, e a interface ao circuito de transmissão digital , incluindo condicionamento e equalização da linha, é realizada pela parte CSU da unidade.

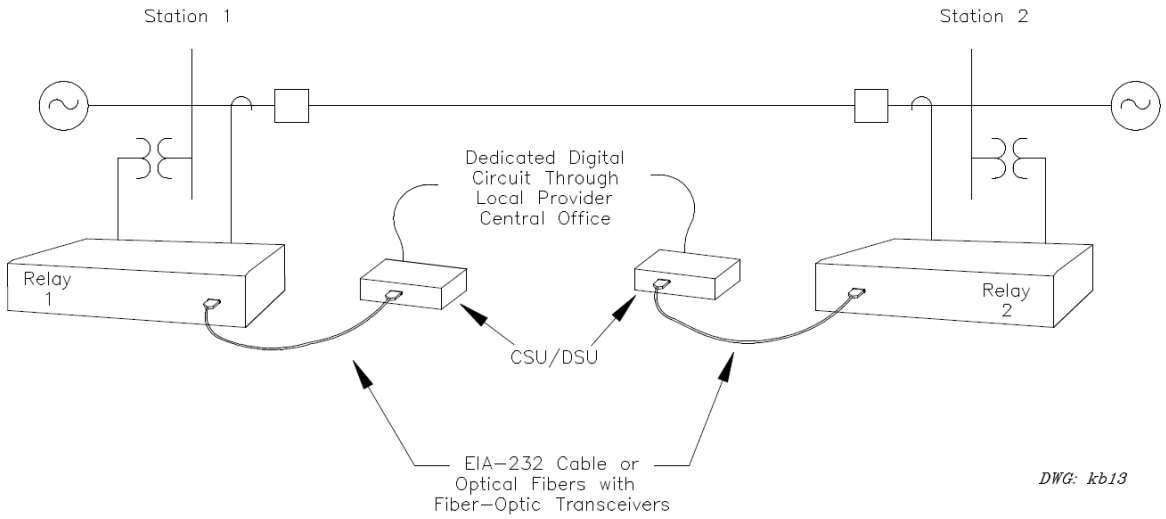


Figura 18: Comunicação Digital via um Canal de Comunicação Digital Compartilhado

O retardo de tempo de dados através do CSU/DSU e o circuito digital compartilhado é insignificante, uma vez que não existe detecção/correção de erro realizada fora do relé. Verifique com seu vendedor do CSU/DSU e do provedor de serviços do circuito digital sobre as característica de retardo de tempo de dados.

O circuito digital dedicado, compartilhado do provedor de serviços local, é roteado através de pelo menos uma unidade central. Se as subestações são localizadas em territórios de unidades centrais diferentes, o circuito será roteado através de múltiplas unidades centrais e neste caso o provedor de serviços pode multiplexar o circuito em um sistema de comunicação. Como discutido anteriormente, chaveamento de caminhos em sistemas podem momentaneamente interromper a comunicação. Verifique com seu provedor de serviços local sobre retardos de tempo de dados e chaveamento de circuitos.

Comunicação Digital via Canais de Comunicação Analógicos

Nota Editorial: **Esta aplicação não é mais recomendada pela Schweitzer Engineering Laboratories, Inc., favor contatar a fábrica para mais detalhes.**

Circuitos de comunicação analógicos compartilhados são comumente utilizados para esquemas de teleproteção tradicionais. Eles podem também ser aplicados no novo esquema de comunicação lógico relé-a-relé simplesmente conectando-se a porta de comunicação serial selecionada em cada relé ao circuito de comunicação analógico via um modem de linha compartilhada. O canal de comunicação analógico dedicado é tipicamente fornecido na forma de um circuito de comunicação metálico a quatro fios da unidade central mais próxima do provedor de serviços. O modem de linha compartilhada, muito semelhante ao CSU/DSU para os circuitos digitais compartilhados, se interliga com a porta serial EIA-232 do relé e fornece condicionamento e equalização de linha na interface com o circuito de comunicação analógico.

De forma diferente do modem discado, o modem de linha compartilhado é conectado todo o tempo, escutando um sinal carrier que indica que o modem remoto está operacional. Transferência de dados podem ocorrer tão logo ambos os modems estejam prontos (“off-hook”) e uma conexão de dados seja estabelecida.

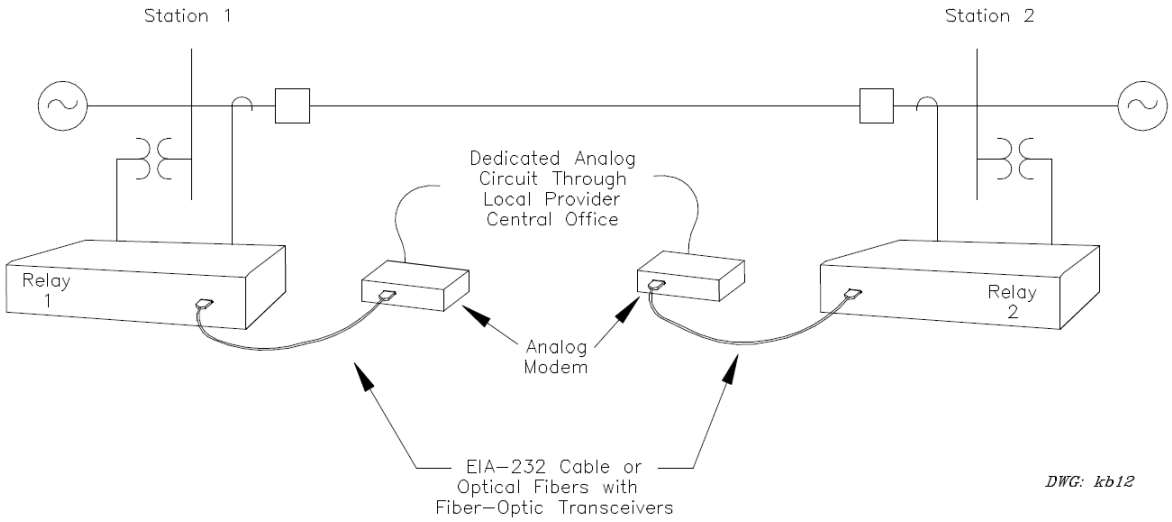


Figura 19: Comunicação Digital via um Canal de Comunicação Analógico Compartilhado

Circuitos analógicos de graduação de voz típicos tem uma largura de banda de freqüência de cerca de 300 a 3.000 Hz. Em um sistema de comunicação duplo completo, cerca de metade da largura de banda é utilizada para comunicação em cada direção. Com um relacionamento um-a-um entre largura de banda e taxa de envio, essa largura de banda limitada permite que os modems analógicos transmitam em taxas de comunicação até 1.200 baud sem compressão de dados.

Acima de 1.200 baud, modems tem que aplicar alguma forma de compressão de dados. Enquanto a compressão de dados melhora o envio global de dados dos modems, ela faz o modem ficar mais sensível a ruídos de canal e introduz retardos de tempo de dados no sinal transmitido. Sensibilidade aumentada a ruído de canal indica que o modem incorpora detecção de erro de dados, e alguns modems “espertos” incorporam correção de erros. Tudo isso requer armazenamento prévio de dados, que no final aumenta o retardo de tempo de dados. Devido a ênfase no envio de dados no mercado de comunicação de hoje, é difícil achar modems que não tem recursos “espertos” que aumentam o retardo de tempo de dados.

Consequentemente, a comunicação lógica relé-a-relé via comunicação analógica tende a incutir um retardo de tempo de dados maior do que canais de comunicação digitais.

Comunicação Digital Direta via Cabo Metálico

Comunicação lógica digital direta relé-a-relé via cabo metálico encontra as mesmas armadilhas de nosso canal ideal de teleproteção conectado direto discutido anteriormente. Aumento de potencial de terra e tensões e correntes induzidas fazem da conexão metálica direta entre relés susceptível a interferências elétricas que criam um perigo pessoal. É, portanto, não recomendado para aplicações de esquemas de teleproteção.

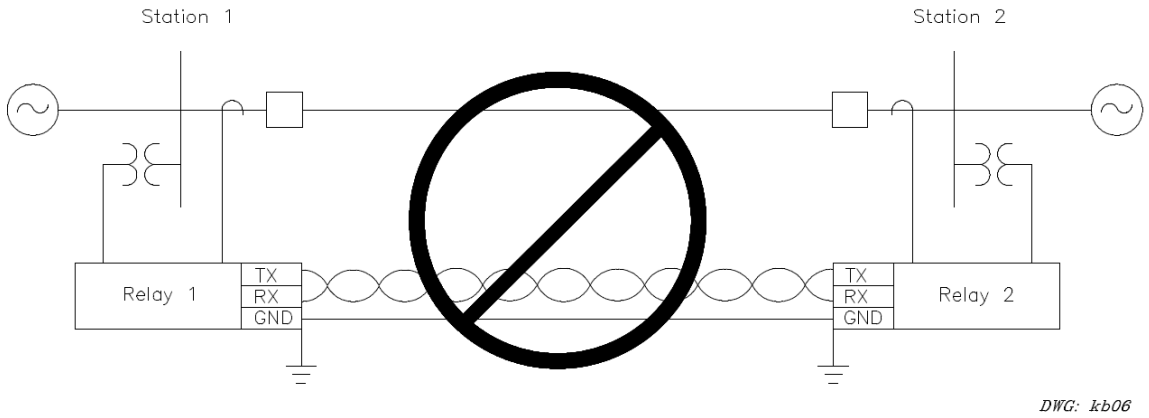


Figura 20: Comunicação Digital Direta via Cabo Metálico – Não Recomendado para Esquemas de Teleproteção

CONCLUSÃO

Neste trabalho, nós discutimos uma nova, inovativa abordagem para realizar funções de esquemas de teleproteção entre relés microprocessados em subestações diferentes. A nova abordagem se beneficia da capacidade de comunicação inerente nos relés microprocessados modernos, eliminando a necessidade de equipamento de teleproteção tradicional separado. A nova abordagem possibilita comunicação rápida, segura e confiável para até oito funções de proteção, monitoramento e controle independentes.

O trabalho também discute as considerações de canal de comunicação para comunicação lógica relé-a-relé. Essa nova abordagem de comunicação pode ser aplicada em qualquer canal de comunicação capaz de comunicar uma mensagem digital, incluindo fibra-ótica direta, fibra-ótica multiplexada e/ou rádio microondas, rádio ponto-a-ponto direto e circuitos analógicos ou digitais compartilhados

REFERÊNCIAS

1. IEC 834-1, “Performance and Testing of Teleprotection Equipment of Power Systems,” Draft 31, July 1995.
2. IEEE/PSRC, “Inter Substation Protection Using Digital Communications,” Draft #8.

APÊNDICE A: PROGRAMA MATHCAD PARA CALCULAR SEGURANÇA E CONFIABILIDADE DE CANAL DE COMUNICAÇÃO LÓGICA RELÉ-A-RELÉ

Ken Behrendt
30 de julho de 1996

CÁLCULOS DE SEGURANÇA PARA UM CANAL DIGITAL

Segurança é uma medida da probabilidade de que todas as mensagens corrompidas serão detectadas e rejeitadas, logo elas não causam uma ação indesejada. Um canal perfeitamente seguro não produz nenhuma ação indesejada. A probabilidade de que uma mensagem corrompida escape da detecção pelas verificações de segurança do relé é PK, assim a segurança do canal, PS, é 1-PK.

Calcule a probabilidade (PK) de que uma mensagem corrompida não seja detectada por um esquema de detecção de erro constituído de um CRC de 6 bits visualizando oito bits de dados e dois flag bits que identificam a seqüência correta de palavras na mensagem:

Onde:

$Z := 1...9$

$P_Z := 10^{-Z}$ P = Razão de erro do bit (BER) do canal

$CRC \equiv 6$ CRC = Número de bits CRC

$N \equiv 8$ N = Número de bits verificados pelo CRC

$K \equiv 4$ K = Número mínimo de bits onde o CRC não é 100% efetivo na detecção de erros

$$PKCR_z := \left[\frac{2}{70} \bullet (P_z)^K \bullet (1 - P_Z)^{(N-K)}\right] + \left[\frac{1}{32} \bullet (P_z)^K \bullet (1 - P_Z)^{(CRC+N-K)}\right]$$

Probabilidade de que o cálculo de bit CRC não vai detectar uma mensagem corrompida

$PKFB_Z := (1-P_Z)^2$ Probabilidade de que os flag bits não vão detectar uma mensagem corrompida.

$PK_Z := (PKFB_Z) \bullet (PKCRC_Z)$ Probabilidade combinada de que uma mensagem corrompida vai passar sem ser detectada.

$PS_Z := 1-PK_Z$ Probabilidade de que o canal seja seguro.

P_Z	PK_Z	PS_Z
$1 \bullet 10^{-1}$	$2{,}4 \bullet 10^{-6}$	0,999997599004841
$1 \bullet 10^{-2}$	$5{,}5 \bullet 10^{-10}$	0,999999999454010
$1 \bullet 10^{-3}$	0	0,999999999999941
$1 \bullet 10^{-4}$	0	1,000000000000000
$1 \bullet 10^{-5}$	0	1,000000000000000
$1 \bullet 10^{-6}$	0	1,000000000000000
$1 \bullet 10^{-7}$	0	1,000000000000000
$1 \bullet 10^{-8}$	0	1,000000000000000
$1 \bullet 10^{-9}$	0	1,000000000000000

Os resultados mostram que a combinação de CRC de 6 bits e byte flag fornece uma segurança de mensagem extremamente elevada sobre uma grande faixa.

Cálculos de Confiabilidade para um Canal Digital

Confiabilidade é uma medida da probabilidade de que uma mensagem transmitida seja recebida. Supondo que o relé detecta e rejeita cada mensagem ruim, e rejeita adicionalmente seis mensagens boas que seguem a mensagem ruim, nós podemos calcular a Taxa de Mensagem Perdida, MMR (Missing Message Rate), que é o número de mensagens rejeitadas por mensagem enviada. Este é um cálculo conservativo que assume que somente um bit corrompido ocorre dentro de cada mensagem corrompida.

A provável confiabilidade de canal, PD, que é o número de mensagens boas recebidas por mensagem enviada, é calculada pela equação: PD = 1 – MMR.

$MER_Z := P_Z \bullet 20$ — Para cada bit de erro enviado, existe uma mensagem ruim. Para cada mensagem, existem 20 bits enviados, então a Taxa de Erro de Mensagem (MER) é a Taxa de Erro de Bit (BER) * 20.

$MMR_Z := MER_Z \bullet (1 + 6)$ — Taxa de Mensagem perdida (MMR) é a Taxa de Erro de Mensagem vezes (1 + 6) porque para cada mensagem corrompida detectada, o relé rejeita a próximas seis mensagens boas.

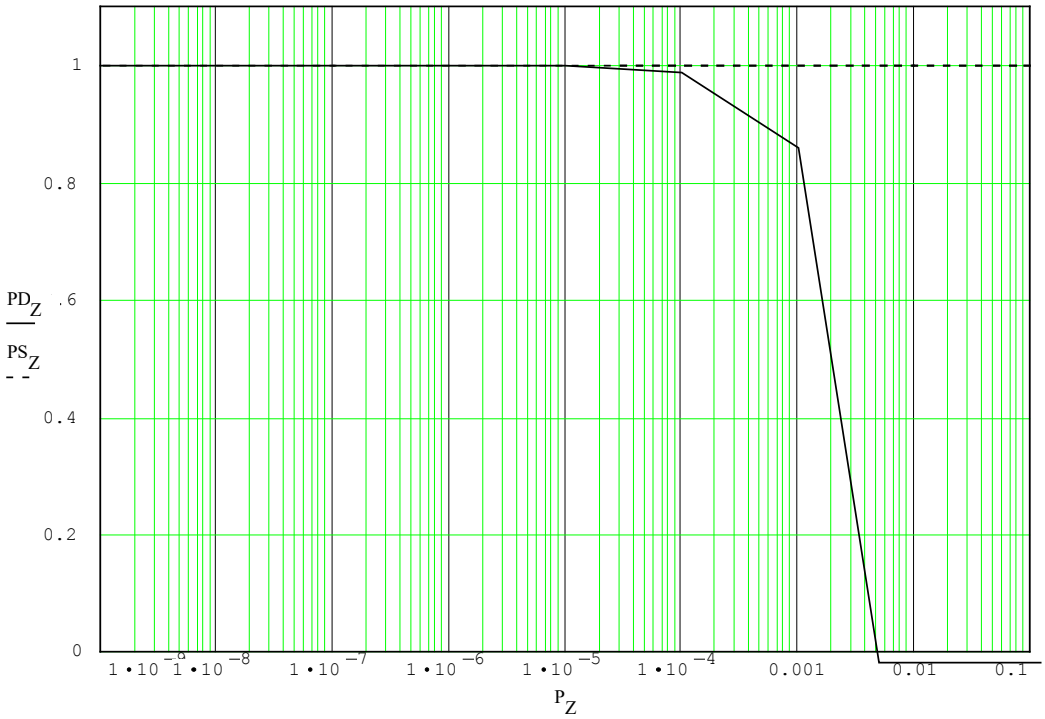
$PD_Z := 1 - MMR_Z$ — Confiabilidade é a Taxa de Transmissão de Mensagens (1) menos a Taxa de Mensagem Perdida.

P_Z	MMR_Z	PD_Z
$1 \bullet 10^{-1}$	$1{,}4 \bullet 10^{-6}$	–13,000000000
$1 \bullet 10^{-2}$	1,4	–0,4000000000
$1 \bullet 10^{-3}$	0.1	0,86000000000
$1 \bullet 10^{-4}$	$1{,}4 \bullet 10^{-2}$	0,98600000000
$1 \bullet 10^{-5}$	$1{,}4 \bullet 10^{-3}$	0,99860000000
$1 \bullet 10^{-6}$	$1{,}4 \bullet 10^{-4}$	0,99986000000
$1 \bullet 10^{-7}$	$1{,}4 \bullet 10^{-5}$	0,99998600000
$1 \bullet 10^{-8}$	$1{,}4 \bullet 10^{-6}$	0,99999860000
$1 \bullet 10^{-9}$	$1{,}4 \bullet 10^{-7}$	0,99999986000

Estes resultados indicam que a confiabilidade cai a zero (ou menos) quando cada sétima mensagem é corrompida e a confiabilidade se aproxima de 1 quando a BER do canal é menor do que 1 para 10.000 bits.

Segurança e Confiabilidade Versus Taxa de Erro de Bit

O gráfico X-Y mostra o relacionamento entre segurança de canal de comunicação lógica relé-a-relé, PS, e confiabilidade de canal, PD, sobre uma faixa de taxa de erro de bit de canal.



APÊNDICE B: PROBABILIDADE DE UM ERRO DE DETECÇÃO UTILIZANDO UM CRC DE 6 BITS

Jian Chen, Jeff Roberts, e Ken Behrendt
30 de julho de 1996

Nós podemos preparar uma mensagem para transmissão sobre um canal de comunicação digital primeiramente expressando esta mensagem como uma seqüência binária. Depois que a mensagem é convertida para uma seqüência binária, nós podemos então emiti-la para uma porta serial para transmissão de comunicação. Porque esta mensagem é uma seqüência de bits de dois estados (ou 1's ou 0's), nós temos que estar cientes da validade da mensagem recebida. Um erro de mensagem ocorre se 1 ou mais trocas de bits da mensagem (0 para 1 ou 1 para 0) durante a transmissão. É mais fácil trocar um bit do que dois ou mais bits. Isto é, quanto maior a distância forçada entre duas seqüências x e y, mais difícil é receber y quando x é transmitida.

Definição: *A distância forçada entre duas seqüências binárias, x e y, é o número de posições nas quais elas diferem.*

Por exemplo, as distâncias forçadas entre as mensagens x e y mostradas abaixo são (em ordem crescente de distância forçada):

x = 10101000
y = 11111000
01010000 - - a distância forçada é 2

x = 10101000
y = 10010000
00111000 - - a distância forçada é 3

x = 10101000
y = 01110000
11011000 - - a distância forçada é 4

Vamos agora olhar a implementação de comunicação lógica relé-a-relé.

- Campo de mensagem de 8-bits, o número de mensagens diferentes = $2^8 = 256$,
- Campo de mensagem de 6-bits, o número de possibilidades CRC diferentes = $2^6 = 64$.

Para a mensagem de 8 bits e o CRC de 6 bits, o número de mensagens com o mesmo CRC é 4 ($2^8/2^6 = 256/64 = 4$). Isto significa que quatro mensagens de 8 bits diferentes dividem o mesmo CRC. Colocando de outra forma, para cada mensagem de 8 bits enviada, existem quatro em 256 mensagens que vão gerar exatamente o mesmo CRC. Se a mensagem transmitida se troca com qualquer das três outras mensagens com o mesmo CRC, um erro de detecção ocorre (isto é, a mensagem defeituosa não é detectada pela verificação CRC).

Quão difícil é enviar uma mensagem que se troca com uma das outras três possíveis combinações de 8 bits com o mesmo CRC? Quão difícil (ou quão fácil) depende da distância excedente mínima entre as quatro mensagens com o mesmo CRC. Quanto maior a distância excedente entre as mensagens com o mesmo CRC, menor a probabilidade deste erro de detecção ocorrer.

O polinômio gerador para um CRC de 6 bits é:

$$g(x) = x^6 + x^5 + x + 1$$

e gera os códigos seguintes:

Número de Mensagen	Bits de mensagen	Bits de CRC	Distância Excedente
1	00000000	000000	mensagem enviada
2	01100101	000000	4*
3	10101111	000000	6
4	11001010	000000	4*
1	00110010	000001	mensagem enviada
2	01010111	000001	4*
3	10011101	000001	6
4	11111000	000001	4*
1	00011001	000010	mensagem enviada
2	01111100	000010	4*
3	10110110	000010	6
4	11010011	000010	4*
1	00101011	000011	mensagem enviada
	-	-	
	-	-	
	-	-	

Utilizando um CRC de 6 bits, nós vemos da tabela acima que a distância excedente mínima entre as mensagens com o mesmo CRC é quatro e o número de mensagens com o mesmo CRC é quatro.

Vamos supor que a taxa de erro de bit de canal (BER) seja p. A probabilidade de que um bit troque é p, dois bits troquem é p^2, três bits troquem é p3 e quatro bits troquem é p^4. Lembre-se que a distância excedente mínima é quatro bits. Então, a probabilidade de um erro de detecção é algum múltiplo fator de p^4. Utilizando-se um CRC de 6 bits então reduz-se a probabilidade de erro de detecção para algum múltiplo fator de p^4.

A probabilidade de um erro de detecção, P*md*, para um CRC de 6 bits é expressa na forma:

$$Pmd \approx \frac{A}{B} p^K (1-p)^{N-K} \qquad \text{Equação 1}$$

onde:

A é o número de ocorrências de distância excedente mínima por grupo de CRC comum
B é o número total de grupos CRC com a distância excedente mínima
N é o número de bits em uma mensagem transmitida verificados pelo CRC
K é o número mínimo de bits onde o CRC não é 100% efetivo
P é a taxa de erro de bit do canal

Nós utilizamos uma aproximação porque o cálculo de probabilidade total é uma série. Entretanto, o primeiro termo da série domina os resultados, assim nós usamos apenas o primeiro termo para simplificar os cálculos.

A quarta coluna na tabela acima indica que existem duas (2) de cada distância excedente de 4 mensagens em cada grupo de mesmo CRC e existe um total de 70 distâncias excedentes de 4 mensagens no campo de mensagem de 8 bits (tabela completa não mostrada). Agora nós podemos escrever a probabilidade de um erro de detecção (P*md*) como:

$$Pmd \approx \frac{2}{70} p^4 (1-p)^4 \qquad \text{Equação 2}$$

Um outro caso que pode levar a um erro de detecção é que ambas mensagem e CRC transmitido trocam durante a transmissão: a mensagem troca do grupo CRC um para grupo CRC dois e o CRC troca de CRC um para CRC dois. Considerando ambas as trocas de mensagem e CRC, nós podemos calcular a probabilidade de um erro de detecção como:

$$Pmd \approx \frac{2}{70}p^4(1-p)^4 + \frac{1}{32}p^4(1-p)^{10} \qquad \text{Equação 3}$$

EFEITO DE BYTE FLAGS NA DETECÇÃO DE ERRO

Vamos olhar agora para o efeito de byte flags na detecção de erro uma vez que existem dois flag bits na mensagem de bit espelhado transmitido (mensagem TMB). Esses flag bits agem como um filtro uma vez que o resto da mensagem não é nem considerada a não ser que os flag bits estejam corretos. Considerando os flag bits, a probabilidade de um erro de detecção se torna:

$$Pmd \approx (1-p)^2\left[\frac{2}{70}p^4(1-p)^4 + \frac{1}{32}p^4(1-p)^{10}\right] \qquad \text{Equação 4}$$

Como o valor de (1 – p) é muito próximo de 1, incluindo os flag bits não há uma melhora significativa de P*md*. Não se quer dizer que os byte flags são desnecessários porque eles são necessários para a identificação da seqüência do byte; isto é, identifica se ele é o primeiro ou segundo byte da mensagem de bit espelhado transmitido.

CÁLCULOS DE ANOS/PALAVRA DE ERRO PARA UM CRC DE 6 BITS

O que esta probabilidade nos diz? Vamos supor que nós temos um canal relativamente pobre com as seguintes características de comunicação:

- o BER é 10^{-4}, i.e., $p = 10^{-4}$ e P*md* = $5.98 \bullet 10^{-18}$ palavra de erro/palavra
- a taxa de dados é 9600 bits/seg. 960 bytes/seg, 480 palavras/seg

Desta informação, nós podemos calcular com qual freqüência nós podemos esperar que uma mensagem corrompida vai escapar da detecção pelas verificações de segurança de mensagem. A técnica de cálculo é como se segue:

$$\text{Tempo}\left(\text{palavra de}\frac{\text{erro}}{\text{seg}}\right) = \frac{10^{18}\text{palavra}}{5{,}98\text{ palavra de erro}} \bullet \frac{1\text{ seg}}{480\text{ palavra}} = 3{,}5 \bullet 10^{14}\frac{\text{seg}}{\text{palavra de erro}}$$

Que é:

$3{,}5 \bullet 10^{14}$ seg/palavra de erro = $9{,}7 \bullet 10^{10}$ horas/palavra de erro
= $4 \bullet 10^{9}$ dias/palavra de erro
= 10.958.904 anos/palavra de erro

Isto significa que uma em aproximadamente 11 milhões de anos, nós podemos esperar experimentar um erro de detecção!