

Comparando a Confiabilidade de Topologias de Redes Ethernet nas Redes de Supervisão e Controle de Subestações

Gary W. Scheer e David J. Dolezilek
Schweitzer Engineering Laboratories, Inc.

Apresentado na
UTC Telecom 2002
Las Vegas, Nevada
23–26 de junho de 2002

Originalmente apresentado na
2nd Annual Western Power Delivery Automation Conference, abril de 2000

Traduzido para o português em agosto de 2017

COMPARANDO A CONFIABILIDADE DE TOPOLOGIAS DE REDES ETHERNET NAS REDES DE SUPERVISÃO E CONTROLE DE SUBESTAÇÕES

Gary W. Scheer and David J. Dolezilek
Schweitzer Engineering Laboratories, Inc.
Pullman, WA USA

INTRODUÇÃO

As concessionárias de energia elétrica têm implantado redes Ethernet em algumas subestações. A impressão que se tem é de que logo um número maior de redes de subestação irá adotar a Ethernet. No entanto, muitos dispositivos Ethernet, software, ferramentas e experts existem como resultante da Internet e das redes locais Ethernet (LANs) nos escritórios e fábricas. Concessionárias de energia elétrica, o Instituto de Pesquisas em Energia Elétrica (EPRI) e os fabricantes de equipamentos estão trabalhando conjuntamente para definir e implantar a Arquitetura de Comunicações das Concessionárias (UCA). A padronização formal da UCA encontra-se em andamento. Os fabricantes de Dispositivos Eletrônicos Inteligentes (IED) estão disponibilizando mais equipamentos que podem ser conectados a uma rede Ethernet.

Este trabalho avalia a confiabilidade das topologias Ethernet de conexão de subestações para a conexão de dispositivos. Redes baseadas nessas topologias são aplicadas para atender às demandas de instrumentação e controle (I&C) de uma subestação.

A confiabilidade é um critério para a comparação de sistemas Ethernet; outros critérios comparativos incluem:

- custo do equipamento, instalação e comissionamento
- taxas efetivas de transferência de dados
- facilidade e custo de manutenção
- facilidade e custo de expansão
- flexibilidade para uso do melhor IED para cada trabalho sem limitações indevidas por questões da rede
- facilidade e custo da incorporação dos dispositivos e projetos existentes ao incorporar uma rede numa instalação já existente.

Observe que esses critérios não são totalmente independentes; por exemplo, a confiabilidade é um fator importante no custo de manutenção.

HISTÓRICO E COMPONENTES DA ETHERNET

Representação de Redes

Muitas vezes as redes são ilustradas como uma linha única, com interseção de várias linhas curtas conectadas a cada dispositivo. As redes Ethernet mais modernas na realidade incluem muito mais componentes e conexões do que se pode visualizar por esta abstração. O projetista precisa compreender e documentar todos os componentes e interconexões da Ethernet para analisar a confiabilidade do sistema e para projetar, fornecer, instalar e manter a rede.

Hubs

Um HUB é um dispositivo relativamente simples com portas múltiplas, que retransmite todos os dados que recebe em cada porta para todas as outras portas. Ele opera na camada Física do modelo de rede OSI, de modo que não usa qualquer dos dados para determinar as ações de roteamento. Os Hubs Ethernet têm um MTBF médio de 118,9 anos.

Chaves

Uma chave é um dispositivo multiplexador inteligente que monitora os dados recebidos em uma porta para determinar a sua disposição. Uma chave opera na camada de Link de Dados do modelo da rede OSI. Se um pacote de dados está incompleto ou é indecifrável, a chave o ignora e não retransmite esse pacote. Se um pacote de dados está intacto, a chave o retransmite a outra porta, baseado no dado de endereçamento incluído no pacote e os endereços associados a cada porta da chave. As chaves Ethernet possuem um MTBF médio de 11,5 anos.

Roteadores

Um roteador é um dispositivo multiplexador inteligente utilizado para conectar duas redes, uma na outra. Ele pode ser um dispositivo complexo, com muitas funções. Ele opera na camada de Rede do modelo OSI. Um roteador é programado para ignorar tráfego intra-segmento e para rotear o tráfego inter-segmento para o segmento de destinação apropriado. Os roteadores Ethernet possuem um MTBF médio de 9,5 anos, porém por preço 25 vezes maior, eles são disponíveis com um MTBF de 35 anos.

Interfaces IED Ethernet

Uma interface IED Ethernet é um dispositivo inteligente que conecta um IED a uma rede Ethernet. Cada dispositivo conectado à Ethernet precisa ter uma interface Ethernet que inclui tecnologia de transceptor para casar a velocidade e a mídia da rede. Cada dispositivo ou interface também precisa usar tempo significativo de processamento para comunicar usando as pilhas (stacks) de interface que são populares atualmente. Muitos IEDs contêm processadores com capacidade de computação, apropriadamente adequados à sua finalidade primária. Para atender à performance exigida para conexões Ethernet de alta velocidade, a interface usualmente dispõe de considerável poder de processamento. As interfaces Ethernet têm um MTBF típico de 19,2 anos.

Servidores

Um servidor coleta dados de todos os dispositivos locais e cria uma base de dados da Subestação. Frequentemente, um pacote gráfico de interface homem-máquina local utiliza dados dessa base de dados. Os servidores funcionam na camada de Aplicativo do modelo OSI. Se os servidores Ethernet forem baseados em computadores pessoais industriais, eles terão um MTBF de 14,3 anos.

Mídia

A maioria das redes Ethernet emprega uma das seguintes mídias.

- BaseT: conexões especializadas de cabo de par torcido de cobre
- BaseF: cabo de fibra ótica.

Um indicador de taxa de dados de 10 para 10, ou 100 para 100 megabits por segundo comumente precede a designação da mídia. Os engenheiros frequentemente selecionam cabo de fibra ótica para comunicações do sistema de supervisão e controle da subestação porque o mesmo:

- isola o equipamento de elevações de potencial de terra perigosas e danosas
- é imune a interferência de radiofrequência e de outras interferências eletromagnéticas
- elimina erros de dados causados por problemas de malha de terra de comunicação
- permite trajetos de sinais mais longos do que as conexões de cobre

As conexões de cobre algumas vezes são selecionadas para os pontos onde os itens acima não se aplicam. Isso geralmente é porque:

- cobre custa mais barato do que a fibra
- o equipamento conectado por cobre custa menos do que o equipamento conectado por fibra
- um número menor de ferramentas especiais são necessárias para terminações de cobre

Tempestades de Dados de Transmissão

Se o controle de mediação para a transmissão de dados falhar, nenhum dos dispositivos de um barramento poderá se comunicar. Uma interface de comunicações de IED pode falhar em um modo que corrompe a rede. O fenômeno da Ethernet chamado “tempestade de dados de transmissão” ocorre se a interface da rede Ethernet falhar e continuamente transmitir as mensagens, corrompendo as comunicações com qualquer dos recipientes de dados. Chaves e roteadores podem evitar que uma tempestade de dados transmitidos influencie a comunicação nos outros segmentos, porém nenhum dado poderá ser recuperado dos segmentos defeituosos. Os HUBs compartilhados passam a “tempestade de dados” adiante e impactam outros segmentos conectados.

INDISPONIBILIDADE DE DISPOSITIVO E SUMÁRIO DA ÁRVORE DE FALHAS

Uma explicação de indisponibilidade de dispositivo e construção da árvore de falhas é incluída na referência [1]. A Referência [2] é um manual que trata desses assuntos. A nível de sumário:

- MTTR é um tempo médio para detectar e reparar uma falha; 48 horas para os dispositivos destes exemplos
- MTTF é o tempo médio de ocorrência de uma falha
- MTBF é o tempo médio entre falhas, definido como a soma de MTTR e MTTF. Para os dispositivos discutidos neste artigo, MTTF é muito maior do que MTTR, de maneira que nós colocamos MTBF como aproximadamente igual a MTTF.
- Indisponibilidade é a probabilidade de que um dispositivo não estará disponível para executar funções vitais para operação do sistema, e é a relação entre MTTR e MTBF.

Tabela 1: Indisponibilidades aproximadas dos diversos componentes

Componente	Indisponibilidade (multiplicar por 10⁻⁶)
Processador de Comunicações da Subestação	30
Hub Ethernet	46
Relé de Proteção / Hardware do IED	55
Interface da Rede do IED	285
Equipamento de Supervisão / IED	320
PC Industrial (usado como um servidor)	385
Gateway SCADA	385
Chave Ethernet	477
Roteador Ethernet	577

Nota: Os componentes de maior disponibilidade possuem os menores números de indisponibilidade.

Quando você conhece a indisponibilidade de cada componente de um sistema, as árvores de falhas são úteis para prever a indisponibilidade do sistema global. Use portas OR para somar as indisponibilidades quando a falha de qualquer dos dispositivos causa uma falha de sistema e portas AND para calcular o produto das indisponibilidades quando todas as falhas têm de ocorrer para o sistema falhar.

COMPARAÇÕES DE TOPOLOGIA PARA AQUISIÇÃO E CONTROLE DE DADOS

Introdução

As seguintes análises são baseadas em uma subestação real de 138/69 kV, com 29 disjuntores. Relés de proteção principal e de retaguarda completos foram incluídos em um upgrade da subestação, totalizando 84 relés de proteção. Para esses exemplos, cada relé é equipado com uma interface Ethernet. Dois processadores de comunicações são incluídos como portas EIA-232 serial para Ethernet, para 23 dispositivos de supervisão de equipamento que não são disponíveis com capacidade Ethernet. Um servidor baseado em um computador industrial é incluído para proporcionar IHM e outros clientes de dados. Um roteador proporciona uma conexão entre a LAN da subestação e uma rede de âmbito do sistema (WAN).

A análise de disponibilidade se foca nas diferenças entre os sistemas. Referências [1] e [3] descrevem itens adicionais que impactam a disponibilidade global da instrumentação e controle. Especificamente, neste artigo não incluímos os impactos da bateria da subestação, transformadores de instrumentação e erros de escavação de cabos de fibra ótica, porque eles representam riscos comparáveis em todos os sistemas. O impacto das falhas de software nos servidores não foi incluído, em parte, porque os sistemas compartilham exposição similar e em parte porque é difícil quantificar taxas de falhas em software.

As cinco seções seguintes resumem a análise para cada uma das cinco LANs.

LAN de HUB Compartilhado

Uma LAN de subestação Ethernet usando HUBs compartilhados é mostrada na Figura 1. As caixas sem texto são IEDs. As caixas marcadas “GW” são portas para os IEDs de supervisão dos equipamentos da subestação.

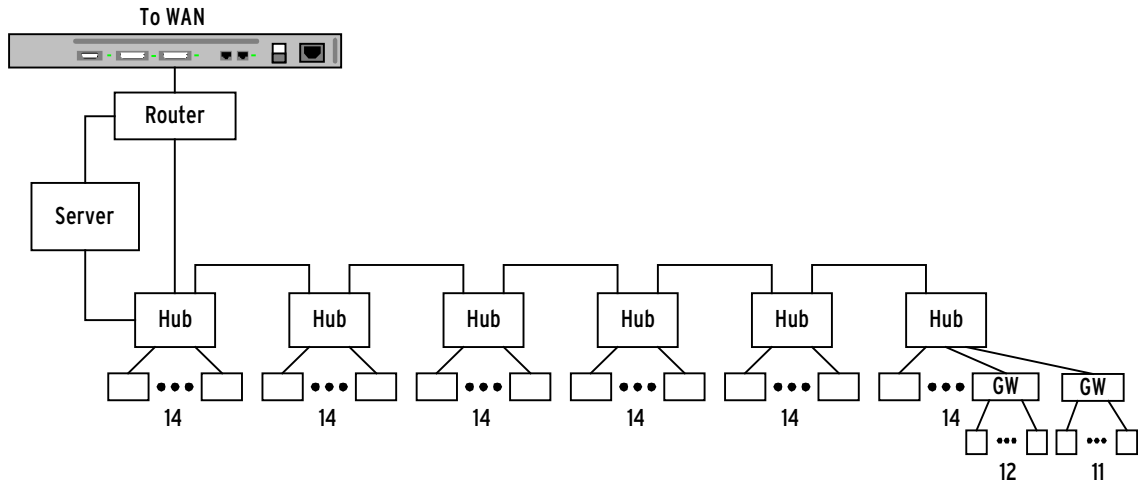


Figura 1: Diagrama de blocos de LAN de HUB Compartilhado

A árvore de falhas mostrada na Figura 2 ilustra a análise de indisponibilidade do sistema. O evento superior da árvore indica que a indisponibilidade computada é a probabilidade de que um cliente acessando o servidor ou a WAN não teria condição de recuperar todos os dados da linha ou seria impedido de controlar qualquer disjuntor.

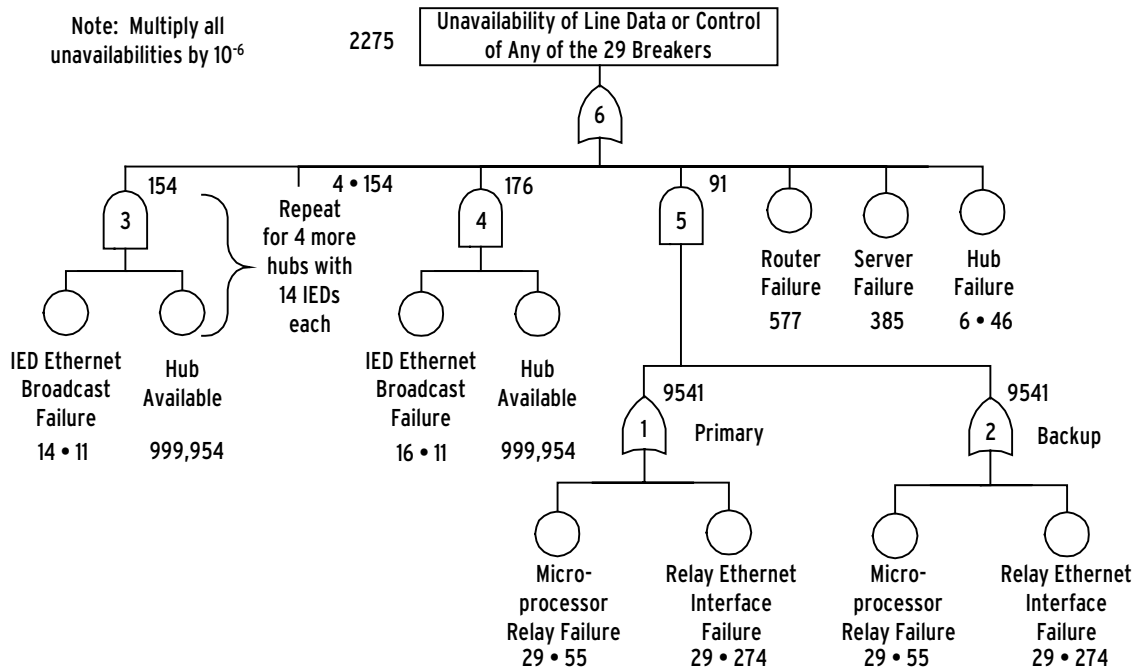


Figura 2: Árvore de Falhas do HUB Compartilhado

O sistema inclui sistemas de relés principais e de retaguarda. Os dispositivos em ambos os sistemas principal e de retaguarda teriam de falhar dentro do mesmo período de tempo para impedir o controle ou supervisão de um disjuntor, de modo que as suas indisponibilidades são combinadas com uma porta AND (Porta 5).

Este sistema usa HUBs compartilhados simples, de modo que qualquer dispositivo Ethernet pode causar uma tempestade de dados de transmissão que inibe toda a rede. Para permitir separação entre as falhas que impactam um dispositivo e a falha de transmissão que impacta toda a rede, é apropriado tratar a indisponibilidade da interface Ethernet IED como duas falhas: 1) as falhas demodo de não-transmissão com uma indisponibilidade de 275×10^{-6} , e 2) a indisponibilidade associada às transmissões que impactam a rede, 11×10^{-6} , para a indisponibilidade total de dispositivo de 285×10^{-6} .

Começando com as entradas para a Porta 1 da árvore de falhas, há 29 relés microprocessados principais, com uma indisponibilidade combinada de $(29)(55 \times 10^{-6}) = 1595 \times 10^{-6}$. Há 29 interfaces Ethernet, com uma indisponibilidade de falha de não transmissão combinada de $(29)(274 \times 10^{-6}) = 7946 \times 10^{-6}$. A indisponibilidade combinada dos relés principais e suas interfaces é a soma dessas entradas, ou 9541×10^{-6} .

O sistema de proteção de retaguarda é idêntico ao sistema principal, de modo que ele apresenta uma indisponibilidade idêntica. Tendo em vista que ambos precisam falhar para que o sistema fique indisponível, eles são entradas para uma porta AND (Porta 5). A indisponibilidade prevista para o sistema combinado é o produto de suas indisponibilidades: $(9541 \times 10^{-6})(9541 \times 10^{-6}) = 91 \times 10^{-6}$.

As falhas de transmissão da interface Ethernet IED afetam a rede se o HUB associado está disponível e funcional. Disponibilidade do HUB = $1 - (\text{indisponibilidade do HUB})$ ou $1 - (46 \times 10^{-6}) = 0,999954$. Há seis HUBs com um total de 86 conexões de rede de IED. Essas incluem os 58 relés no sistema principal e de retaguarda envolvido na monitoração da linha ou controle do disjuntor, mais 26 relés e duas portas para os dispositivos de monitoração de equipamento. O sistema usa 5 HUBs com 14 IEDs cada um (Porta 3) e um HUB com 16 IEDs (Porta 4). A indisponibilidade combinada devida a falhas de transmissão da rede é de: $(5)(14)(11 \times 10^{-6})(0,999954) + (16)(11 \times 10^{-6})(0,999954) = 946 \times 10^{-6}$.

Qualquer dos seguintes eventos da Tabela 2 ocasiona o evento superior, de modo que as suas indisponibilidades são somada na porta OR superior (Porta 6).

Tabela 2: Análise da Árvore de Falhas do HUB Compartilhado

Causa do Evento Superior	Indisponibilidade (multiplicar por 10^{-6})
Falha dos Sistemas de Proteção Principal e de Retaguarda	91
Tempestade de dados de transmissão	946
Um dos seis HUBs falha: $(6)(46 \times 10^{-6})$	276
Roteador Falha	577
Servidor Falha	385
Indisponibilidade Prevista Combinada	2275
Disponibilidade do Evento Superior: $1 - (2275 \times 10^{-6})$	99,7725%

LAN Chaveada

Uma LAN de subestação Ethernet utilizando chaves possui um diagrama de blocos similar à Figura 1, exceto que todos os HUBs são substituídos por chaves. A árvore de falha para o sistema baseado em chaves é mostrada na Figura 3, e possui menos portas do que o sistema de HUB compartilhado. Isso é porque as tempestades de dados transmitidos são bloqueadas

pela chave e impactam apenas a interface Ethernet que estiver com o problema. Nesta análise, cada interface Ethernet possui uma indisponibilidade de 285×10^{-6} . A indisponibilidade combinada dos sistemas LAN Chaveados é 3921×10^{-6} . A disponibilidade é $1 - 3921 \times 10^{-6} = 99,6079\%$.

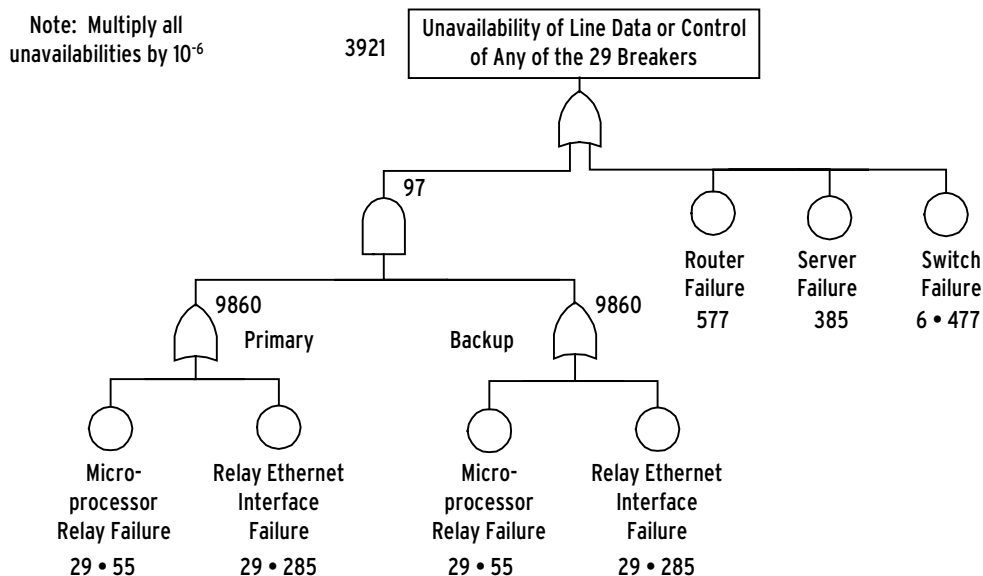


Figura 3: Árvore de Falhas da Chave

LAN de “Hub” Compartilhado Redundante

Uma maneira de incrementar a disponibilidade é proporcionar redes redundantes. Então, ao invés de uma única falha ocasionar o evento superior, duas falhas têm que ocorrer para causar a falha do sistema inteiro. O diagrama de blocos de uma LAN de HUB Compartilhado Redundante é mostrado na Figura 4. A árvore de falhas correspondente é mostrada na Figura 5. Para o sistema de proteção principal ou de retaguarda, a indisponibilidade combinada é a soma das indisponibilidades dos 29 relés principais e as falhas de tempestade de dados de não transmissão de qualquer de suas 29 interfaces $(29) (55 + 274) \times 10^{-6}$. Para a rede, cada um dos sistemas principal e de retaguarda está sujeito à falha de qualquer dos 6 HUBs, e à falha de tempestade de dados de transmissão de qualquer dos 86 dispositivos. As redes primária e de retaguarda possuem cada uma indisponibilidade de $12,22 \times 10^{-6}$. A indisponibilidade combinada é 1055×10^{-6} . A disponibilidade é $99,8945\%$, consideravelmente maior que a topologia HUB Compartilhado ou LAN Chaveada.

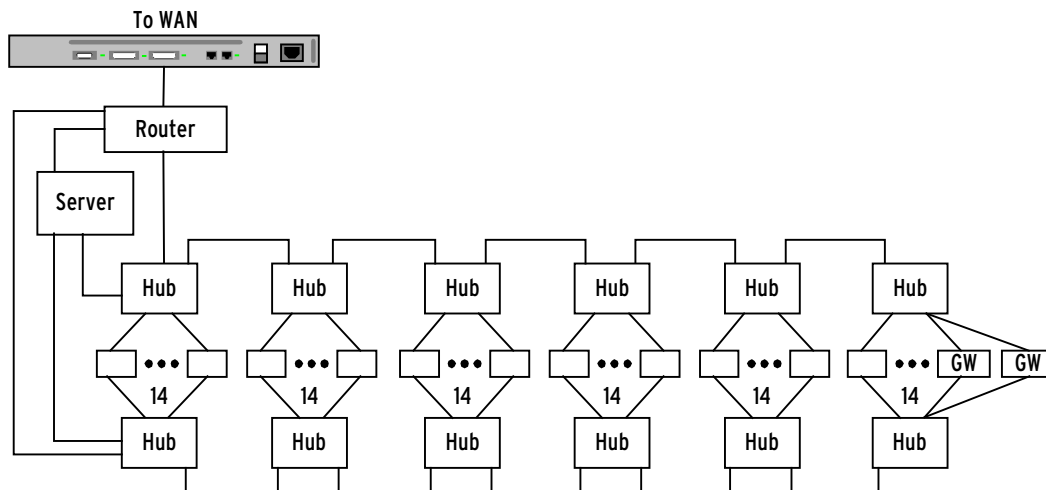


Figura 4: Diagrama de Blocos do HUB Compartilhado Redundante

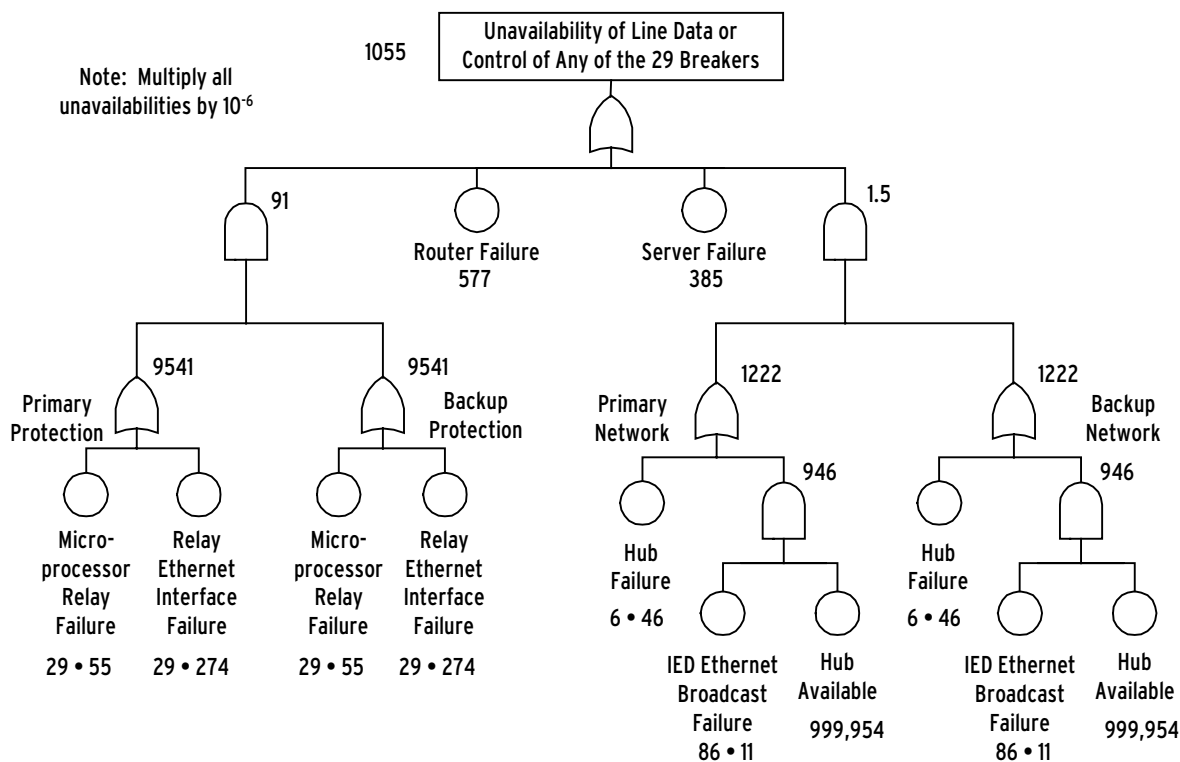


Figura 5: Árvore de Falhas do HUB Compartilhado Redundante

LAN Chaveada Redundante

O diagrama de blocos para uma subestação com LANs chaveadas redundantes é similar à Figura 4, exceto que todos os HUBs são substituídos por chaves. Nesta análise, cada interface Ethernet apresenta uma indisponibilidade de 285×10^{-6} . A indisponibilidade combinada da proteção principal e de retaguarda é de 97×10^{-6} , como no caso chaveado não redundante. As redes principal e de retaguarda têm, cada uma, seis chaves, (6×10^{-6}). A indisponibilidade combinada da rede é $(2862 \times 10^{-6})^2$, ou $8,19 \times 10^{-6}$. A indisponibilidade global da LAN Chaveada Redundante é de 1067×10^{-6} , a soma das indisponibilidades da rede de proteção, servidor e roteador. A disponibilidade é de 99,8932%, ligeiramente menor do que a da topologia LAN de HUB Compartilhado Redundante.

Servidores, Roteadores e LAN Chaveada Redundantes

Ao invés de replicar a rede inteira, um projetista pode dividir a rede de comunicações em redes principal e de retaguarda, conectadas em seus respectivos sistemas de proteção principal e de retaguarda. Figura 6 ilustra sistemas de comunicações e proteção totalmente redundantes. Os únicos componentes não redundantes estão no subsistema de supervisão de equipamentos. A árvore de falhas para este sistema é mostrada na Figura 7. Os sistemas principal e de retaguarda possuem, cada um, uma indisponibilidade de 12.253×10^{-6} . A indisponibilidade combinada do sistema é de 150×10^{-6} . A disponibilidade é de 99,9850%.

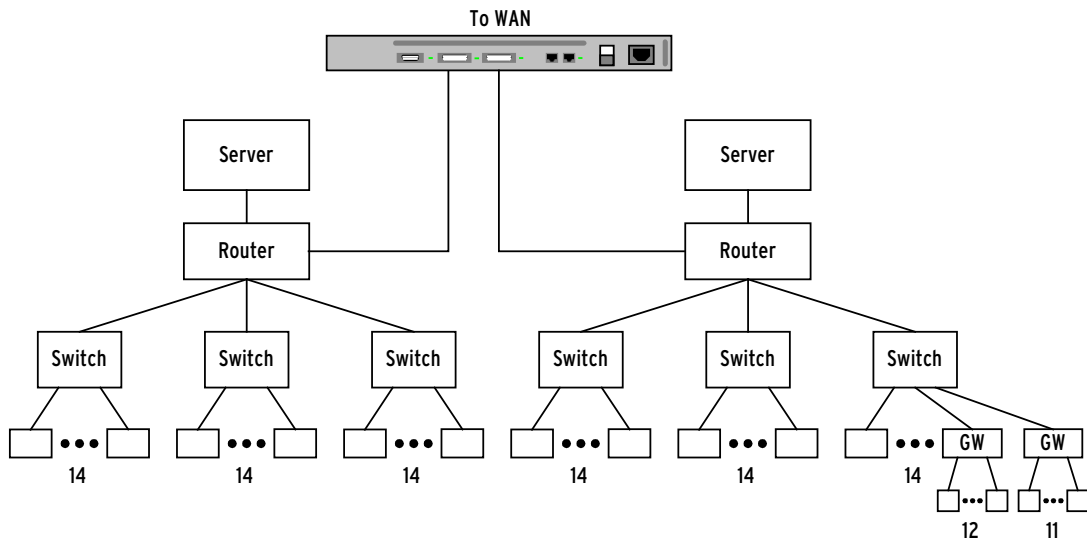


Figura 6: Diagrama de Blocos de Servidores, Roteadores e LAN Chaveada Redundantes

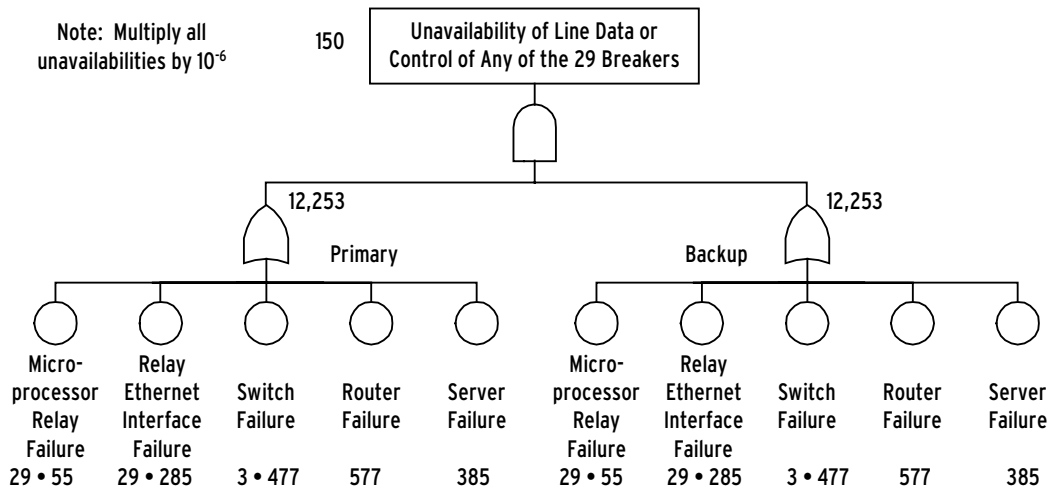


Figura 7: Árvore de Falhas de Servidores, Roteadores e Chaves Redundantes

Comparação de Disponibilidade

Tabela 3 resume as disponibilidades de topologia de conexão discutidas. A previsão de horas anuais fora de serviço é a indisponibilidade vezes o número de horas em um ano.

Tabela 3: Disponibilidades dos Sistemas para Recuperar todos os Dados de Linha e Operar Qualquer Disjuntor

LAN Ethernet	Disponibilidade %	Previsão de nº de horas anuais fora de serviço
Chaves	99,6079	34,3
HUBs Compartilhados	99,7725	19,9
Chaves Redundantes	99,8932	9,3
HUBs Compartilhados Redundantes	99,8945	9,2
Servidores, Roteadores, Chaves Redundantes	99,9850	1,3

A susceptibilidade dos HUBs compartilhados à tempestades de dados poderia levar à se suspeitar de que um sistema baseado em HUBs poderia apresentar uma disponibilidade pior do que um sistema chaveado. No entanto, nos exemplos, o sistema baseado em HUBs é mais disponível, devido à MTBF mais longa do HUB simples em comparação com a chave, que é mais complexa. Os sistemas de HUB redundante e chave redundantes são mais representativos das instalações efetivas e apresentam disponibilidades melhores do que os respectivos sistemas não redundantes. O sistema totalmente separado com servidores, roteadores e chaves redundantes apresenta a melhor disponibilidade entre todos esses sistemas.

Comparação de Custos

Os custos são dados nesta seção para ajudar a identificar as comparações de custos contra disponibilidade para as LANs. Tabela 4 resume os custos aproximados dos componentes Ethernet de cada LAN, em ordem decrescente de custo de equipamento. Os preços médios de equipamento para interfaces de IED, cabos de fibra ótica, HUBs, chaves, roteadores e servidores estão incluídos nos custos do equipamento. Os custos de manutenção são resumidos na última coluna da Tabela 4 e incluem mão de obra e custos de materiais sem garantia, para todas as falhas de equipamento previsíveis dentro de 10 anos.

Tabela 4: Custos Típicos de Equipamentos e Manutenção das LANs Ethernet

LAN Ethernet	Custo Inicial do Equipamento (\$)	Custo de Manutenção em Dez Anos (\$)
Chaves Redundantes	156.000	173.000
Chaves	123.000	147.000
“Hubs” Compartilhados Redundantes	121.000	129.000
Servidores, Roteadores, Chaves Redundantes	116.000	156.000
“Hubs” Compartilhados	106.000	127.000

SENSIBILIDADE AO BAIXO MTBF DOS DISPOSITIVOS DE REDE DISPONÍVEIS

As comparações acima calculam a indisponibilidade utilizando MTBF médios para dispositivos fabricados e implantados hoje. Crescentes aplicações de Ethernet nos ambientes industriais e de concessionárias de energia elétrica podem criar demanda para dispositivos Ethernet que são projetados para Tempos Médios Antes da Falha (MTBF) mais longos. Se indisponibilidades comparáveis a relés de proteção forem obtidas para interfaces e chaves, então nós poderemos comparar as mesmas topologias usando uma indisponibilidade de 55×10^{-6} , ao invés dos valores da Tabela 1. Se esses HUBs, chaves e roteadores teóricos existissem, as disponibilidades previstas das redes que os utilizam seriam os valores resumidos na Tabela 5. Os sistemas são mostrados em ordem crescente de valor de disponibilidade.

Tabela 5: Disponibilidades de Sistemas utilizando Componentes Futuros de Alto MTBF para Recuperar Todos os Dados da Linha e Operar Qualquer Disjuntor

LAN Ethernet com Dispositivos Teóricos de Alta MTBF	Disponibilidade %	Previsão de nº de horas anuais fora de serviço
HUBs compartilhados	99,8330	14,6
Chaves	99,9220	6,84
HUB compartilhado redundante	99,9550	3,93
Chaves Redundantes	99,9550	3,94
Servidores, Roteadores, Chaves Redundantes	99,9986	0,126

ANÁLISES COM OUTROS EVENTOS SUPERIORES

As análises acima focalizam a disponibilidade dos sistemas para recuperar todos os dados de linha e operar todos os disjuntores. Este evento superior corresponde à visão de disponibilidade de sistema que é freqüentemente aplicada aos sistemas SCADA.

Análises usando outros eventos superiores revelam diferentes facetas de disponibilidade do sistema. Por exemplo, um evento superior de “Impossível Controlar Disjuntor Número 7 ou Recuperar Dados de Linha da Linha 7” teriam apenas impactos do sistema sobre as comunicações com um relé específico. A análise nesta base geraria uma melhor disponibilidade para topologias independentes do que para topologias compartilhadas.

COMPARAÇÕES DE TOPOLOGIA PARA COMUNICAÇÕES RELÉ COM RELÉ

Outro evento importante é “Impossível Comunicar Dados de Proteção Relé com Relé.” Use este evento superior para comparar a utilização de um link Ethernet com a utilização de links diretos para comunicações relé com relé. Considere somente os componentes e conexões que impactam o trajeto de comunicações entre dois relés em diferentes segmentos de cada LAN Ethernet previamente analisada.

Para a LAN de HUB Compartilhado, os sistemas de proteção principal e de retaguarda incluem, cada um, os dois relés e as suas interfaces Ethernet. As falhas relativas à não transmissão das interfaces com os relés de campo geram uma indisponibilidade de 658×10^{-6} para a proteção primária ou de retaguarda. A indisponibilidade combinada é de $0,433 \times 10^{-6}$. Adicione as indisponibilidades de 6 HUBs e 86 falhas de transmissão para uma indisponibilidade de 1222×10^{-6} . A disponibilidade é de 99,8778%.

Para a LAN Chaveada, os sistemas de proteção principal e de retaguarda incluem, cada um, os dois relés e as suas interfaces Ethernet, para uma indisponibilidade de 680×10^{-6} . A indisponibilidade combinada é de $0,462 \times 10^{-6}$. Adicione as indisponibilidades de 6 chaves para uma indisponibilidade de sistema de 2862×10^{-6} . A disponibilidade é de 99,7138%.

Para a LAN de HUB Redundante, os itens impactantes da disponibilidade “peer-to-peer” nos sistemas de proteção principal ou de retaguarda são dois relés ($2 \times 55 \times 10^{-6}$) e as falhas não de transmissão de suas interfaces Ethernet ($2 \times 273 \times 10^{-6}$). A indisponibilidade combinada dos sistemas de proteção é de $0,430 \times 10^{-6}$. As redes primária e de retaguarda possuem, cada uma, 6 HUBs ($6 \times 46 \times 10^{-6}$) e falhas de transmissão para 86 IEDs ($0,9999 \times 86 \times 11 \times 10^{-6}$), para uma indisponibilidade de 1222×10^{-6} . A indisponibilidade combinada das redes primária e de retaguarda é de $1,49 \times 10^{-6}$. A indisponibilidade total combinada é de $1,92 \times 10^{-6}$. A disponibilidade é de 99,9998%.

Para a LAN Chaveada Redundante, os sistemas principal e de retaguarda incluem, cada um, os dois relés ($2 \times 55 \times 10^{-6}$) e suas interfaces Ethernet ($2 \times 285 \times 10^{-6}$), para uma indisponibilidade de 680×10^{-6} . A indisponibilidade combinada é de $0,462 \times 10^{-6}$. As redes primária e de retaguarda possuem, cada uma, 6 chaves ($6 \times 477 \times 10^{-6}$) e uma indisponibilidade combinada de $8,19 \times 10^{-6}$. A indisponibilidade combinada total é de $8,65 \times 10^{-6}$. A disponibilidade é de 99,9991%.

Para os Servidores, Roteadores e Chaves LAN Redundantes, os itens impactantes da disponibilidade relé a relé nos sistemas principal e de retaguarda são dois relés ($2 \times 55 \times 10^{-6}$), suas interfaces Ethernet ($2 \times 285 \times 10^{-6}$), duas chaves ($2 \times 477 \times 10^{-6}$) e um roteador (577×10^{-6}). O sistema principal ou de retaguarda possui uma indisponibilidade de 2211×10^{-6} , para uma indisponibilidade combinada de $4,89 \times 10^{-6}$. A disponibilidade é de 99,9995%.

Para uma conexão direta relé-relé, o sistema principal ou de retaguarda inclui dois relés ($2 \times 55 \times 10^{-6}$) e duas interfaces de fibra dedicadas ($2 \times 10 \times 10^{-6}$), para uma indisponibilidade líquida de 130×10^{-6} . A indisponibilidade combinada dos sistemas principal, mais retaguarda, é de $0,0169 \times 10^{-6}$. A disponibilidade é de 99,9999%.

Tabela 6 resume as indisponibilidades e disponibilidades das redes e dos links diretos para comunicações relé a relé dentro de uma subestação, dispostos em ordem decrescente de disponibilidade.

Tabela 6: Comunicações Relé a Relé em uma Subestação

Rede	Disponibilidade %	Previsão de nº de horas anuais fora de serviço
Chaves	99,7138	25
“Hubs” Compartilhados	99,8778	10,7
Chaves Redundantes	99,9991	0,07
Servidores, Roteadores, Chaves Redundantes	99,9995	0,04
“Hubs” Compartilhados Redundantes	99,9998	0,01
Direta	99,9999	0,00014

O enfoque deste trabalho é sobre as aplicações Ethernet dentro das subestações. Veja o Apêndice para as diretrizes referentes à análise de comunicações de relés entre subestações.

CONCLUSÕES

Das cinco LANs analisadas, a topologia com redes redundantes e independentes é a mais disponível para operar qualquer disjuntor ou recuperar todos os dados da linha de potência. Esta topologia é a segunda mais baixa, entre as cinco, em termos de custos de equipamento. Se esta topologia tornar-se largamente aceita para automação de subestações, isso poderia reduzir ainda mais o custo e a indisponibilidade de interfaces IEDs, porque ela não utiliza a função standby-failover das interfaces.

Se os fabricantes de equipamentos Ethernet oferecerem dispositivos com Tempos Médios Antes da Falha (MTBF) muito melhores do que os dispositivos existentes, então a mesma topologia com redes redundantes e independentes ainda continuará sendo a mais disponíveis para os casos gerais de instrumentação e controle. A classificação de redes que utilizam chaves irá suplantar a classificação das redes com HUBs compartilhados. Todos os sistemas que utilizam dispositivos com MTTF mais altos são mais disponíveis do que os sistemas existentes. Se a Ethernet vai ser utilizada em sistemas industriais e em subestações, recomendamos que os fabricantes de IEDs projetem e forneçam componentes Ethernet com MTTF mais elevados.

Para comunicações relé com relé, comunicações diretas externas à LAN são muito mais disponíveis do que qualquer das LANs. Isso é devido ao número de dispositivos envolvidos na LAN e a relativa complexidade dos dispositivos. Se uma LAN é utilizada para dados de proteção relé-relé, a LAN de HUBs Redundantes Compartilhados apresenta melhor disponibilidade.

Se a Ethernet é utilizada para I&C da subestação, recomendamos a topologia de Servidores Redundantes, Roteadores e Chaves. Para comunicações de proteção relé a relé, recomendamos conexões diretas com fibra, separadas da rede.

SUMÁRIO DO PROCESSO

É importante identificar e caracterizar todos os dispositivos em uma rede e as suas interconexões para analisar a confiabilidade das redes.

Para analisar alternativas, obtenha dados de MTBF e MTTR referentes a cada componente do sistema, calcule as indisponibilidades e construa e analise árvores de falha para cada opção a ser considerada. Utilize as árvores de falha para identificar áreas que podem ser replicadas para reduzir a sua contribuição à indisponibilidade do sistema e modifique o sistema para refletir o aperfeiçoamento. Calcule o custo e determine a importância dos critérios de avaliação restantes.

Selecione os eventos superiores para as árvores de falha que produzem indisponibilidade do sistema para realizar uma tarefa bem definida ou um grupo de tarefas. Neste artigo, nós comparamos a “Disponibilidade para Recuperar Todos os Dados de Linha e Operar Qualquer Disjuntor” para cada sistema, o que é comparável às disponibilidades tipicamente consideradas nas comparações do SCADA. Além disso, comparamos as disponibilidades dos sistemas de “Comunicar Dados de Proteção Relé-Relé” dentro da subestação. Esses eventos principais abordam diretamente as aplicações Ethernet correntemente discutidas nas reuniões da indústria de energia elétrica.

APÊNDICE: DIRETRIZES PARA ANÁLISE DE CONFIABILIDADE DE COMUNICAÇÃO RELÉ- RELÉ ENTRE SUBESTAÇÕES

O enfoque deste artigo é sobre as redes Ethernet aplicadas dentro de subestações. Alguns engenheiros de concessionárias têm considerado a utilização de WAN para transmitir informação de proteção relé a relé entre subestações. Este Apêndice fornece as diretrizes para cálculo da disponibilidade estimada de comunicações relé a relé entre subestações.

Considere duas subestações idênticas à SE do exemplo utilizado nas comparações. Para cada um dos seis casos de comunicações relé-relé dentro de uma SE, considere os modos de falha adicionais da comunicação inter-estações. Se as duas subestações empregam, ambas, uma rede de HUB compartilhado, HUB compartilhado redundante ou rede chaveada redundante, então calcule a indisponibilidade em cada subestação com as seguintes modificações nos cálculos apropriados deste artigo:

- Utilize a indisponibilidade para apenas um relé e uma interface Ethernet em cada um dos sistemas de proteção principal e de retaguarda
- Adicione a indisponibilidade do roteador à indisponibilidade da subestação.

Para sistemas de roteadores, servidores e chaves redundantes em cada subestação:

- Utilize somente um relé, uma interface Ethernet e uma chave em cada um dos sistemas principal e de retaguarda.
- Observe que os roteadores já estão incluídos na análise da subestação.

A indisponibilidade global prevista é a soma das indisponibilidades das redes das duas subestações, mais a indisponibilidade dos componentes, interconexões e fibra da WAN. Analise a WAN ou WANs com uma metodologia similar a aquela empregada neste trabalho para cada LAN. Fora da subestação, adicione a indisponibilidade do cabo de fibra ótica devido a erros de escavação [2]. Em cada local adicional que impactar a performance da WAN, inclua a fonte de alimentação de energia à análise de indisponibilidade.

Para a conexão direta relé-relé entre subestações, utilize um relé e transceptor de fibra ótica no sistema principal e de retaguarda de cada SE. Fora da subestação, inclua a indisponibilidade do cabo de fibra ótica devido a erros de escavação [2]. Se as fibras estão dentro de um cabo ou vala comum, trate a indisponibilidade dos cabos de fibra ótica como um evento comum aos sistemas principal e de retaguarda. Se cabos separados de fibra ótica são instalados com rotas separadas, inclua as indisponibilidades do cabo de fibra ótica em cada um dos sistemas principal e de retaguarda.

REFERÊNCIAS

- [1] G. W. Scheer, "Answering Substation Automation Questions Through Fault Tree Analysis," Proceedings of the Fourth Annual Texas A&M Substation Automation Conference, College Station Texas, April 8-9, 1998.
- [2] N. H. Roberts, W. E. Vesely, D. F. Haasl, and F. F. Goldberg, "Fault Tree Handbook," NUREG-0492m U.S. Nuclear Regulatory Commission, Washington, DC, 1981.
- [3] G. W. Scheer, "Comparison of Fiber-Optic Star and Ring Topologies for Electric Power Substation Communications," Proceedings of the First Annual Western Power Delivery and Automation Conference, Spokane, WA, April 6-8, 1999.
- [4] D. J. Dolezilek, D. A. Klas, "Using Information From Relays to Improve Protection," Proceedings of the 25th Annual Western Protective Relay Conference, Spokane, Washington, October 13-15, 1998.

BIOGRAFIA

Gary W. Scheer recebeu seu B.S. em Engenharia Elétrica da *Montana State University* em 1977. Ele trabalhou para a *Montana Power Company* e para a subsidiária da MPC, a *Tetragenics Company*, antes de ingressar na Schweitzer Engineering Laboratories, Inc. em 1990 como engenheiro de desenvolvimento. Ele foi vice-presidente da Divisão de Pesquisas e Desenvolvimento, e da Divisão de Serviços de Engenharia e Automação da SEL. O Sr. Scheer está agora na Divisão de Marketing e Serviços de Atendimento ao Cliente como Gerente de Mercado para produtos de automação e comunicações. Sua biografia aparece no *Who's Who in America*. Ele detém duas patentes relacionadas à teleproteção. É um engenheiro profissional registrado e membro do IEEE, NSPE e ISA.

David J. Dolezilek recebeu seu B.S. em Engenharia Elétrica da *Montana State University* em 1987. Além de consultoria independente em projetos de sistemas de controle, ele trabalhou para o Estado da Califórnia, Departamento de Recursos Hídricos, e para a *Montana Power Company* antes de ingressar na Schweitzer Engineering Laboratories, Inc. em 1996 como engenheiro de projetos de integração de sistemas. Em 1997, Dolezilek tornou-se o Diretor de Vendas para os Estados Unidos e Canadá, em seguida mudou para Gerente de Engenharia de Pesquisas e Desenvolvimento no grupo de Engenharia de Automação e Comunicações da SEL. Em 2000, Dolezilek foi promovido para Gerente de Tecnologia da Automação, responsável pela pesquisa e projeto de sistemas automatizados. Ele continua a pesquisar e escrever artigos técnicos sobre projetos e implantações inovadoras de grande importância para nossa indústria, bem como a participar de grupos de trabalho e comitês técnicos. Ele é membro do IEEE, da *IEEE Reliability Society* e do Comitê Técnico 57 da *International Electrotechnical Commission* (IEC) criado para abordar a padronização global de sistemas e redes de comunicação de subestações.