

Capítulo XV

Confiabilidade de sistemas de automação de subestações

Equipe de engenharia da Schweitzer Engineering Laboratories (SEL)

Engenheiros de proteção de sistemas elétricos utilizam análise de confiabilidade para assegurar, baseado em critérios técnicos, a melhor decisão na escolha da aplicação de sistemas de supervisão, proteção e controle.

A confiabilidade em tais sistemas é importante devido aos altos impactos em custos operacionais e na satisfação de clientes causados pela falha na operação. As motivações principais de quantificar as questões de confiabilidade incluem a condução de melhor tomada de decisões sobre como melhorar o sistema de proteção, como melhorar a forma de gerir a confiança versus segurança e como obter os melhores resultados com o mínimo de dinheiro.

Confiança é a capacidade de um sistema de proteção operar corretamente. Um sistema confiável é aquele que opera quando é solicitado. Assim, um sistema de proteção que sempre atua, quando solicitado, é 100% confiável, porém, este sistema pode ocasionalmente operar quando não deve. Já um sistema que nunca opera indevidamente é 100% seguro, mas pode ocasionalmente não operar quando deveria. Assim sendo, confiança e segurança são questões de confiabilidade.

Este capítulo irá explicar os conceitos e as ferramentas de avaliação e de melhorias da

confiabilidade do sistema de proteção. O objetivo é apresentar ferramentas para projetar sistemas de proteção que ofereçam a confiabilidade necessária e uma boa relação custo-benefício.

Inicialmente será abordado o método de análise de diagramas de blocos que são úteis para analisar a confiabilidade de sistemas simples. Posteriormente, será abordado o método de análise da árvore de falhas, que é mais versátil e fácil de aplicar para sistemas complexos do que a análise por diagramas de blocos.

O método de análise da árvore de falhas usado e aperfeiçoado ao longo dos anos é atraente, pois não exige um trabalho teórico extenso e é uma ferramenta prática que qualquer engenheiro pode aprender a usar. Embora os programas de computador estejam disponíveis para auxiliar no desenvolvimento e análise de árvores de falhas complexas, este artigo mostra que as árvores de pequenas falhas, que são facilmente analisados manualmente, também são muito úteis.

Conceitos de confiabilidade

A Tabela 1 define as medidas frequentemente utilizadas para descrever o desempenho de confiabilidade de produtos, assumindo a falha constante e as taxas de reparo.

TABELA 1 - DEFINIÇÕES DE MEDIÇÕES DE CONFIABILIDADE

Medida	Definição
Disponibilidade (A)	Aplicada tanto para o desempenho de componentes individuais ou de um sistema, é a fração de tempo que um componente ou sistema está em serviço e realiza satisfatoriamente a sua função.
Indisponibilidade (U)	É a fração de tempo que um componente ou sistema está fora de serviço devido a falhas ou interrupções programadas. Matematicamente, a indisponibilidade = (1 - disponibilidade).
Falha	Determina o término da capacidade de um item de executar a sua função especificada.
Taxa de falha (λ)	Taxa de falhas é a frequência, com a qual um sistema ou um componente projetado falha. Representa o número médio de falhas de um componente por unidade de tempo de exposição e pode ser calculado pegando-se o número total de falhas dividido pelo tempo total de operação do equipamento. Geralmente, o tempo é expresso em anos e a taxa de falha é dada por falhas no ano.
Taxa de reparo (μ)	Semelhante à taxa de falhas, representa o número total de reparos dividido pelo tempo total de operação do equipamento.
Tempo médio entre falhas (MTTF)	Representa o tempo médio até a primeira falha de um equipamento. O tempo médio entre o início de operação ou retorno de reparo até a nova falha. Para uma taxa de falha constante, $MTTF = \lambda^{-1}$.
Tempo médio para reparos (MTTR)	Tempo médio para corrigir uma falha e restabelecer o equipamento à condição de funcionamento. Inclui preparação, manutenção ativa e tempo de logística. Para uma taxa de reparo constante, $MTTR = \mu^{-1}$.
Tempo médio entre falhas (MTBF)	O tempo médio entre falhas para unidades reparadas e de volta a operação.

Formalmente, o MTBF é a soma do MTTF e o MTTR. Como MTTR é geralmente pequena, assumimos que o MTBF é aproximadamente igual à MTTF e que $MTBF = \lambda^{-1}$.

Por exemplo, suponha que a confiabilidade de um dispositivo é dada em tempo médio entre falhas (MTBF) e seja de 100 anos. A taxa de falha é de 1/100 falhas por ano. E, se o sistema tem 300 destes dispositivos, então podemos esperar $300 \cdot (1/100) = 3$ falhas em dispositivos por ano.

Os relés de proteção e os sistemas de proteção, destinados à operação contínua durante todo o ciclo de vida, são projetados para serem reparados. Portanto, medidas de confiabilidade devem incluir a possibilidade de falha e de reparo.

Disponibilidade é a probabilidade ou fração de tempo que um dispositivo ou sistema é capaz de operar. A equação (1) define a disponibilidade "A" para uma taxa de falha e de reparo constantes.

$$A = \frac{\mu}{\lambda + \mu} = \frac{MTTF}{MTTF + MTTR} \approx \frac{MTBF}{MTBF + MTTR} \quad (1)$$

Usuários do relés de proteção estão frequentemente preocupados com o tempo de inatividade ou indisponibilidade que pode ocorrer em um sistema de proteção. Indisponibilidade é a probabilidade ou fração de tempo em que um dispositivo ou sistema é incapaz de realizar sua função. A equação (2) define a indisponibilidade U para uma taxa de falha e de reparo constantes.

$$U = 1 - A = \frac{\lambda}{\lambda + \mu} = \frac{MTTR}{MTBF} \approx \lambda \cdot MTTR \quad (2)$$

Probabilidade, disponibilidade e indisponibilidade são números adimensionais. No entanto, pode-se convertê-los em minutos ou segundos por ano, multiplicando-se pelos fatores apropriados.

Método de análise de confiabilidade em sistemas

Modelagem de confiabilidade é útil para analisar sistemas físicos e para comparar a performance de diversas configurações. Os métodos mais comuns de análise de confiabilidade são o diagrama de blocos e a análise da árvore de falhas.

Método de diagrama de blocos

Sistemas são constituídos por componentes individuais. Os diagramas de blocos de confiabilidade da Tabela 2 representam a

interligação lógica dos componentes do sistema, que podem ou não coincidir com a sua interligação física. Diagramas de blocos ajudam os engenheiros a avaliar a confiabilidade do sistema a partir do nível de componente para cima.

Em um sistema em série, a falha de qualquer componente irá resultar na falha do processo. Portanto, o sistema em série tem menor confiabilidade do que os componentes analisados individualmente. Um relé e um disjuntor é um exemplo de um sistema em série.

Em um sistema paralelo, ambos os componentes devem falhar para o sistema falhar. A confiabilidade do sistema é maior do que a confiabilidade de seus componentes analisados individualmente. Dois relés redundantes formam um sistema paralelo, por exemplo.

Se as falhas de um sistema podem ser causadas por eventos que não sejam falhas de componentes, tais como interfaces externas, o modelo deve incluir explicitamente tais elementos externos como blocos no diagrama.

Como exemplo, considere dois sistemas de proteção. Um deles é composto por um único relé e o outro é um sistema redundante paralelo com dois relés idênticos, mas independentes. Se a taxa de falha de um único relé é de 0,0033 por ano e a média de tempo de reparo é de 48 horas, podemos determinar o tempo médio entre falhas (MTBF) e da indisponibilidade (U) para cada configuração.

Para um sistema com um único relé:

$$\lambda = 0,0033 \text{ falhas/ano}$$

$$MTBF = 1/\lambda = 1/0,0033 \text{ falhas/ano} = 300 \text{ anos}$$

(uma falha a cada 300 relés por ano)

$$U = \lambda \cdot MTTR = (0,0033 \text{ falhas/ano}) (48 \text{ horas})$$

$$(1/8.760 \text{ horas/ano}) = 1,81 \cdot 10^{-5}$$

$$U = (1,81 \cdot 10^{-5}) (525.600 \text{ minutos/ano})$$

$$= 9,5 \text{ minutos/ano}$$

Para um sistema de redundância paralela:

$$MTBF_p = 3/2\lambda = 3/2 (0,0033 \text{ falhas/ano}) =$$

$$455 \text{ anos (uma falha a cada 455 relés por ano)}$$

$$UP = \lambda^2 \cdot MTTR^2 = (0,0033)^2 (482) (1/8.760)^2$$

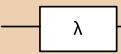
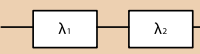
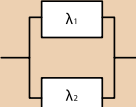
$$= 3,27 \cdot 10^{-10}$$

$$UP = 1,72 \cdot 10^{-4} \text{ minutos/ano} = 0,01 \text{ segundo/ano}$$

A redundância paralela aumenta a MTBF em 50% e reduz a indisponibilidade para perto de zero. Observe que, com sistemas de redundância paralela, menor indisponibilidade vem a um custo de mais manutenção. Se qualquer uma das unidades paralelas falhar, os usuários devem detectar essa falha e repará-la em benefício de menor indisponibilidade.

Diagramas de blocos são úteis para analisar a confiabilidade de sistemas simples. A análise da árvore de falhas é mais versátil e fácil de aplicar para sistemas complexos do que a análise por diagramas de blocos.

TABELA 2 – MTBF E INDISPONIBILIDADE PARA DIVERSAS CONFIGURAÇÕES DE SISTEMA. CADA BLOCO REPRESENTA UM COMPONENTE DO SISTEMA COM A FALHA E AS TAXAS DE REPARO CONSTANTES

	Sistema simples	Sistema em série	Sistema em paralelo
			
MTBF	$\frac{1}{\lambda}$	$\frac{1}{\lambda_1 + \lambda_2}$	$\frac{1}{\lambda_1} + \frac{1}{\lambda_2} = \frac{1}{\lambda_1 + \lambda_2}$
Indisponibilidade	$\lambda \cdot MTTR$	$\lambda_1 \cdot MTTR_1 + \lambda_2 \cdot MTTR_2$	$\lambda_1 \cdot MTTR_1 \cdot \lambda_2 \cdot MTTR_2$

Método da análise da árvore de falhas

A análise da árvore de falhas é uma ferramenta prática para responder a perguntas como esta: “Como a falha de um componente pode contribuir para um evento de falha específico?”. Os engenheiros podem usar a análise da árvore de falhas para comparar a confiabilidade relativa dos esquemas de proteção propostos. A análise da árvore de falhas é adequada para considerar o desempenho, a confiabilidade de cima para baixo de um sistema para um evento específico de falhas.

Para a construção de cada árvore, você deve identificar quais as falhas de componente podem causar uma falha na operação ou uma operação incorreta. O evento de falha de interesse é chamado de “evento principal”. Um sistema pode ter mais de um evento principal que mereça ser investigado. A taxa de falha para o evento principal é uma combinação das taxas de falhas dos eventos básicos que contribuem para o seu acontecimento. “Eventos básicos” são falhas de componentes individuais, com taxas de falhas identificadas. São usadas portas lógicas “E” (AND), “OU” (OR) e outras portas para representar as combinações de taxas de falhas. É possível usar disponibilidade, indisponibilidade ou MTBF no lugar de taxas de falhas na análise de árvore de falhas.

Taxa de falha e indisponibilidade de dispositivos

A taxa de falha do dispositivo nos dá o número de falhas que se pode esperar por unidade de tempo. Durante o tempo de vida útil de um dispositivo, frequentemente, assumimos uma taxa de falha constante.

As taxas de falhas podem vir a partir de cálculos teóricos ou a partir das experiências de campo. Por exemplo, imaginemos que exista uma população em serviço de 10 mil dispositivos e observamos dez falhas de dispositivos em um ano. Uma estimativa da taxa de falha a partir desses dados de campo é de 10/10.000 = 0,001 falhas por ano. A recíproca dá um MTBF estimado de 1.000 anos. Isso não significa que um dispositivo irá durar mil anos.

A taxa de falha é muito útil na previsão de custos de manutenção, mas não revela o histórico de um dispositivo se este estará disponível a operar quando solicitado. Assim, precisamos considerar a indisponibilidade do dispositivo. Indisponibilidade é a fração de tempo que um dispositivo não pode executar sua função.

Conforme visto na equação (2), temos a indisponibilidade U de um dispositivo para uma taxa de falha λ e de taxa de reparo constantes que é dada por:

$$U = 1 - A = \frac{\lambda}{\lambda + \mu} = \frac{MTTR}{MTBF} \approx \lambda MTTR$$

Relés com funções de autotestes e com contatos de alarme monitorado têm melhor disponibilidade, caso não existam procedimentos de testes periódicos. Isso porque um dia com o relé fora de serviço a cada dois anos devido aos testes rotineiros causa uma indisponibilidade muito maior que a indisponibilidade, por conta de falhas automaticamente detectadas pelos relés e que são prontamente reparadas.

Como exemplo, considere um relé de proteção com autotestes “watchdog” que detecte todas as falhas no equipamento. Se o relé tem um MTBF de 100 anos, então ele tem uma taxa de falha de 0,01 falhas/ano.

- Primeiro vamos assumir que a função de autoteste detecta problemas em questão de segundos, mas leva dois dias para reparar a falha, uma vez que é detectada. Se o contato do relé de alarme é monitorado, então o relé pode estar de volta em serviço em dois dias, e a indisponibilidade é de 0,01 falhas/ano \cdot 2 dias = 0,02 dias/ano.
- No entanto, se o contato de alarme não é monitorado, devemos considerar como descobrir as falhas no relé. Suponhamos que testá-lo a cada dois anos e repará-lo no mesmo dia em que este é testado. Se um teste detecta uma falha, então na média o relé está fora por um ano. A indisponibilidade é 1 ano \cdot 0,01 falhas por ano = 3,65 dias/ano e isso é 183 vezes pior que a situação anterior.

Sem o autoteste e monitoramento do contato de alarme, o MTTR pode ser muito maior. Com os relés eletromecânicos, por exemplo, as falhas podem não ser detectadas até que a próxima falta no sistema de potência ocorra.

Neste ponto, é importante lembrar que, dependendo do sistema a ser analisado, faz-se necessário o automonitoramento de demais funções que devem ser observadas durante a especificação do equipamento. Como exemplo, os relés de proteção com funções de monitoramento de interfaces de comunicação Ethernet, que são muito importantes para a confiabilidade de sistemas em IEC-61850 ou sistemas de detecção de arco voltaico em painéis de média e baixa tensão, visto que podem monitorar as fibras óticas responsáveis pela detecção de luminosidade.

A Tabela 3 relaciona os valores de confiabilidade para um número de componentes nos sistemas de proteção.

TABELA 3 – VALORES DE CONFIABILIDADE POR EQUIPAMENTOS	
Componente	Indisponibilidade $\cdot 10^{-6}$
Relé de proteção, falha de confiança	18
Relés de proteção, falha de segurança	2
Relé de proteção, falha de hardware	55
Relé de proteção, falha de interface Ethernet	274
Gateway de comunicação	385
Switch Ethernet	477
Roteador Ethernet	557
Transformadores de corrente	11
Transformadores de tensão	44
Sistemas de baterias	27
Disjuntores	300
Equipamentos de microondas analógicos	200
Equipamentos de tom	100
Canal de fibra ótica	100
Fiação	200

Construção da árvore de falhas

A Figura 1 mostra um sistema de proteção de sobrecorrente constituído de um relé de sobrecorrente, um disjuntor, um transformador de corrente, um sistema de baterias DC e fiação associada. Confiabilidade é uma das principais preocupações para esta aplicação. A árvore de falhas da figura nos ajuda a analisar a confiabilidade do sistema. Os valores de indisponibilidade são aplicados na Tabela 3 para os componentes individualmente. Note que o evento de indisponibilidade principal é a soma das indisponibilidades independentes de eventos básicos. Neste sistema simples, a falha de qualquer componente provoca falha no sistema. A indisponibilidade do sistema é $556 \cdot 10^{-6}$.

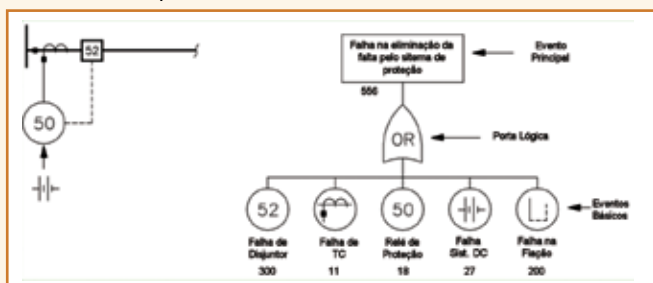


Figura 1 – Árvore de falhas para um sistema de proteção de sobrecorrente simples.

Se tivermos redundância, representada por portas AND (E), devemos primeiro determinar a indisponibilidade simultânea dos dois componentes, que é o produto de suas indisponibilidades.

Este cálculo pressupõe que as falhas são independentes e não provocadas por uma causa comum.

Vamos melhorar o sistema adicionando um relé redundante. A árvore de falhas da Figura 2 contém uma porta E (AND), que expressa a ideia de que ambos os relés de proteção devem deixar de operar para o evento principal ocorrer. Nossa taxa de falhas para os relés em conjunto é de $18 \cdot 10^{-6} \cdot 18 \cdot 10^{-6} = 0,000324 \cdot 10^{-6}$. O montante decorrente da porta OR é $538 \cdot 10^{-6}$. A melhoria da confiabilidade neste caso é pequena porque outras falhas representam maiores indisponibilidades que somente a falha do relé.

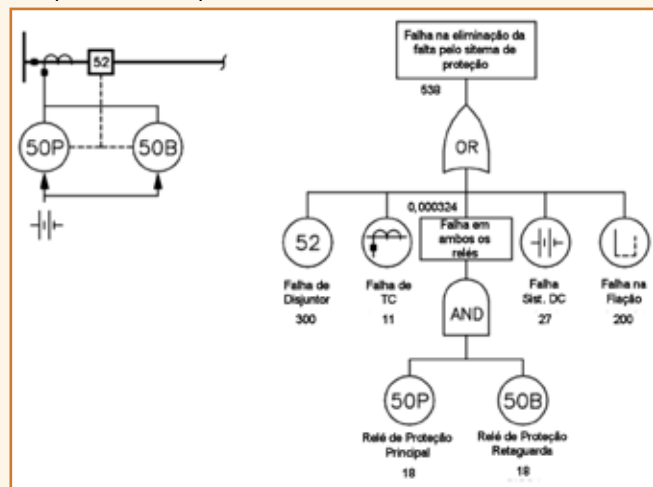


Figura 2 – Árvore de falhas para um sistema de proteção de sobrecorrente com relés redundantes.

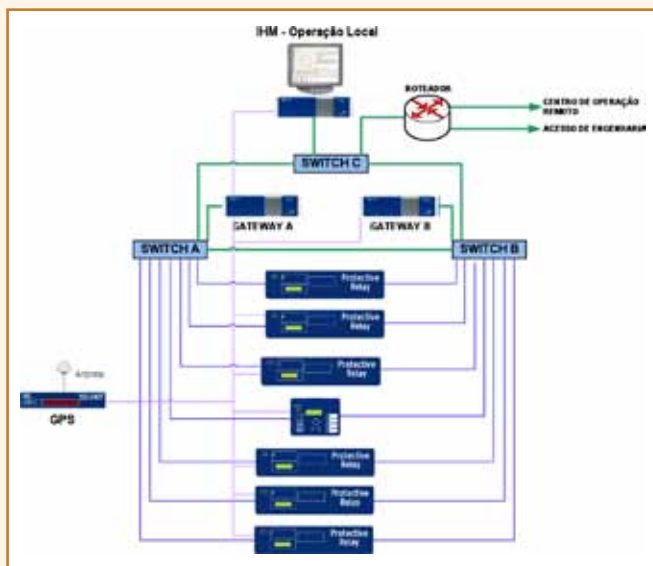


Figura 3 – Sistema de automação de subestação.

Vantagens do método de análise da árvore de falhas

Árvores de falha permitem a comparação da indisponibilidade relativa dos diversos esquemas de proteção. Mantendo árvores de falhas simples e fazendo hipóteses simplificadoras, os engenheiros podem analisar as árvores de falhas facilmente com cálculos manuais. Embora os dados sobre indisponibilidade de componentes individuais sejam aproximados, alguns são apoiados por medições de campo, assim, árvores de falhas dão resultados úteis e próximos da realidade.

A análise de árvores de falhas é um passo fundamental para assegurar a melhor aplicação de recursos de engenharia.

Confiabilidade em sistemas de automação de subestações

A análise da árvore de falhas para sistemas de automação segue o mesmo raciocínio demonstrado anteriormente. No caso de sistemas de automação, além da confiabilidade, outros aspectos são analisados, entre eles:

- Custos de instalação, equipamentos e comissionamento;
- Taxas de transferência de dados efetiva;
- Custo de manutenção;
- Custos de expansão.

Como exemplo, faremos um exemplo baseado em uma subestação de 13.8/69 kV com oito disjuntores. Todo o esquema de proteção contempla relés de proteção principais e retaguardas em um total de 16 equipamentos. Todos os equipamentos são equipados com uma interface de comunicação Ethernet. São previstos dois gateways de comunicação e um computador industrial com função de IHM Local. A rede de comunicação interna da subestação deverá ser projetada com os switches em anel e IEDs em dupla estrela. Um roteador realiza a comunicação entre a rede da subestação e o centro de operação remoto, conforme ilustra a Figura 3.

Neste sistema de automação, considerando como evento principal a indisponibilidade de recepção de dados ou controle de qualquer um dos oito disjuntores da subestação e usando o método de análise da árvore de falhas com os dados da Tabela 3, temos a indisponibilidade que é de $584,64 \cdot 10^{-6}$.

Melhorando a confiabilidade

Para melhorar a disponibilidade de qualquer sistema, pode-se escolher entre as seguintes opções:

1. Simplificar o sistema usando menos componentes, eliminando assim as possibilidades de falha;
2. Usar componentes com menor índice de falhas, maiores índices de MTBF;
3. Reduzir o tempo de reparo por meio de alarmes de monitoramento e autoteste;
4. Ter peças de reposição disponíveis;
5. Consultar tempos de reparos com os fabricantes dos produtos e levar em consideração a capacidade de executar reparos com agilidade;
6. Verificar prazos de garantia e analisar a política de garantia de fornecedores;
7. Aplicar, hardwares redundantes para reduzir o impacto da falha de um determinado componente do sistema.

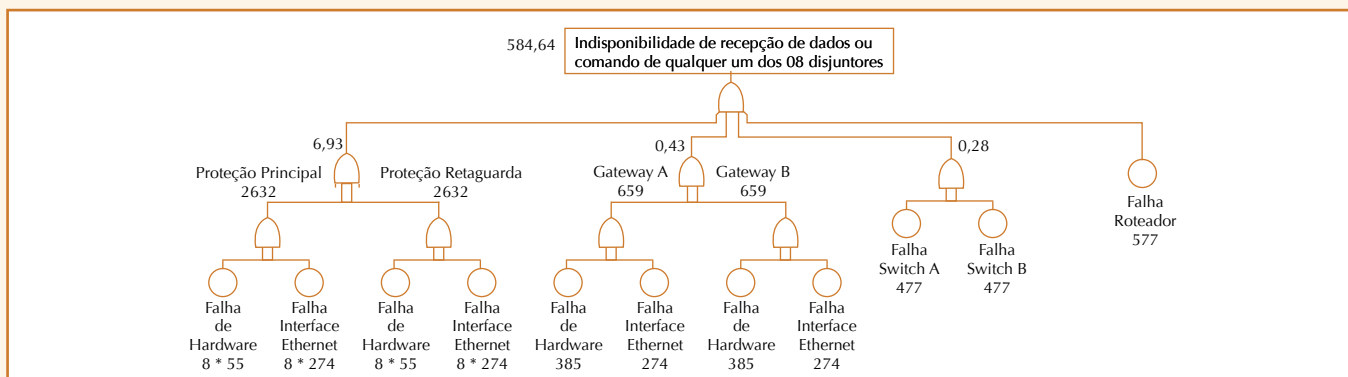


Figura 4 – Sistema de automação de subestação.

*Equipe de engenharia da Schweitzer Engineering Laboratories (SEL)

FIM

Encerramos nesta edição o fascículo sobre “Automação de subestações”. Confira todos os artigos desta série em www.osetoreletrico.com.br
Dúvidas, sugestões e comentários podem ser encaminhados para o e-mail redacao@atitudeeditorial.com.br