Guia de Aplicação de Qualidade de Energia

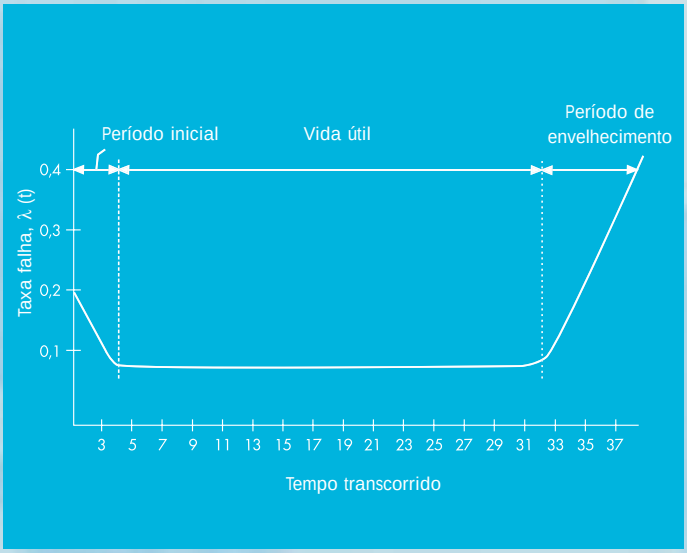
Education and Culture

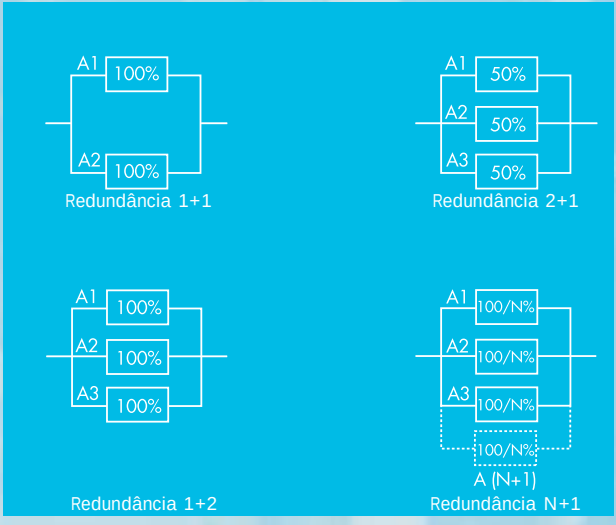
Leonardo da Vinci

Resiliência

Resiliência, Confiabilidade e Redundância

4.1





Resiliência

PROCOBRE Connects Life.™

Copper Institute

Resiliência

Resiliência, Confiabilidade e Redundância

Gary Marshall, WSP Communications Ltd &
David Chapman, Copper Development Association
Maio 2002

European Copper Institute (ECI)

O Instituto Europeu do Cobre é uma joint venture entre a ICA (Associação Internacional do Cobre) e o IWCC (Conselho Internacional do Cobre Forjado). Por sua qualidade de membro, o ECI age em nome dos maiores produtores de cobre do mundo e dos fabricantes líderes da Europa, na promoção do cobre na Europa. Formado em janeiro de 1996, o ECI é apoiado por uma rede de dez Associações de Desenvolvimento do Cobre (CDAs) no Benelux, França, Alemanha, Grécia, Hungria, Itália, Polônia, Escandinávia, Espanha e o Reino Unido. Fomenta os esforços empreendidos inicialmente pela Associação de Desenvolvimento de Produtos de Cobre, criada em 1959, e a INCRA (Associação Internacional de Pesquisa do Cobre) formada em 1961.

Instituto Brasileiro do Cobre - PROCOBRE

É uma instituição sem fins lucrativos, constituída por empresas produtoras e transformadoras de cobre com a missão de estimular o uso técnico e econômico do metal, promovendo sua utilização correta e eficiente. Desenvolve projetos nas várias áreas de aplicação do metal, divulgando as vantagens da utilização do cobre na energia elétrica, nas instalações hidráulicas e de gás, na arquitetura, no design e decoração de interiores, na saúde e muitas outras.

Reconhecimentos

Este projeto foi realizado com o apoio da Comunidade Européia e da International Copper Association, Ltd.

Advertência

O European Copper Institute, a WSP Communications Ltd, a Copper Development Association e o Instituto Brasileiro do Cobre, negam responsabilidade por qualquer dano direto, indireto, conseqüente ou incidental que possa resultar do uso da informação, ou da inabilidade para usar as informações ou dados contidos nesta publicação.

Copyright© European Copper Institute, Copper Development Association and WSP Communications Ltd.

A reprodução é autorizada com a condição de que o material não seja abreviado e a fonte seja reconhecida.

PROCOBRE Connects Life.™

Av. Brigadeiro Faria Lima, 2128-cj.203
Cep 01451-903
São Paulo - SP
Brasil

Tel./Fax: 55 11 3816-6383
e-mail: procobrebrasil@copper.org
Internet: www.procobre.org

European Copper Institute
168 Avenue de Tervueren
B-1150 Brussels
Belgium

Tel: 00 32 2 777 70 70
Fax: 00 32 2 777 70 79
Email: eci@eurocopper.org
Website: www.eurocopper.org

Resiliência, Confiabilidade e Redundância

Introdução

Disponibilidade - a proporção de tempo em que o sistema está realmente disponível para executar trabalho real - é um dos parâmetros fundamentais na determinação da qualidade de uma alimentação de energia. Os valores absolutos de disponibilidade requeridos ou esperados são muito elevados - um usuário doméstico típico na Europa Ocidental espera uma disponibilidade de 99,98%, enquanto um usuário comercial pode requerer mais de 99,996%. Esses altos níveis de disponibilidade não acontecem naturalmente ou por acaso: são o resultado de um procedimento de projeto e de manutenção excelente, e da atenção aos detalhes.

A menos que o projetista tome medidas para evitá-lo, a disponibilidade diminui potencialmente em cada conexão, dispositivo de proteção, cabo, etc. ao longo da instalação de forma que é mais alta no ponto de acoplamento comum (PCC, do inglês Point of Common Coupling) e mais baixa nos terminais do equipamento.

A disponibilidade no PCC é tipicamente cerca de 99,98%, em grande parte porque a rede de alimentação é altamente redundante, isto é, existem muitas rotas disponíveis entre o consumidor e os pontos de geração, sendo cada rota monitorada e mantida continuamente para assegurar a mais alta (economicamente justificável) disponibilidade. Se uma falta se desenvolve, há uma probabilidade muito alta de que uma rota alternativa esteja disponível, de forma que não ocorre nenhuma interrupção, ou no pior caso uma interrupção curta, de energia para a carga. O projeto da instalação fica muito para trás neste aspeto, usando ainda ligações de linha única, transformadores individuais sem reserva ou conexões de manobra cruzada. Colocando isto de outra forma, a rede pode sobreviver à falha de um ou mais componentes individuais ou conexões - é resiliente - enquanto a instalação tem muitos pontos isolados individuais onde a falha causará a interrupção do fornecimento.

Desde meados do último século foi dada grande ênfase na confiabilidade de componentes e subsistemas. O interesse levou à redução da taxa de falhas, aumentando assim o tempo de vida útil.

Durante a última década mudou o foco; os projetistas e analistas de sistemas estão agora muito mais preocupados com a disponibilidade dos seus sistemas. Disponibilidade alta requer muito mais que confiabilidade alta. Dependendo da situação e da importância do equipamento para a operação, também pode exigir tempos de reparo curtos, um grau de redundância on-line, substituição “à quente” de subsistemas críticos, estratégias de diagnóstico boas e estoques de reserva apropriados. Qualquer que seja a situação, a manutenção de disponibilidade alta requer cuidadoso planejamento futuro e bom gerenciamento de manutenção. Na realidade, está muito mais relacionada à administração e ao planejamento que à engenharia.

Confiabilidade alta, embora não suficiente em si mesma, ainda é uma exigência fundamental; manter disponibilidade alta de equipamento não confiável não é realista porque requer muito esforço e um grande estoque de peças sobressalentes e equipamento redundante. O projeto resiliente requer a disposição inteligente de equipamento inerentemente confiável numa topologia redundante, em conjunto com procedimentos de manutenção bem definidos e rigorosamente implementados.

A exigência básica de alta confiabilidade de unidades individuais é discutida na próxima seção.

Panorama

Confiabilidade

A confiabilidade é medida em termos de tempo médio até a falha (MTTF, do inglês Mean Time to Failure). O MTTF é especificado em horas e é o tempo médio que leva cada membro individual de uma população grande de peças de produção standard para falhar. Medir a confiabilidade é difícil e consome tempo; é um número estatístico derivado de uma combinação de experiências históricas com

componentes semelhantes e ensaios relativamente de curto prazo em um grande número dos componentes em questão. À medida que os produtos se desenvolvem, acumulam-se dados de um período mais longo e a confiança no índice MTTF aumenta. Mas não é uma garantia!

Uma falha pode acontecer de forma catastrófica, quer dizer, é completa e repentina, como a falha de uma lâmpada incandescente, ou por degradação, ou seja, é gradual ou parcial, como uma unidade eletrônica que funciona fora da especificação. No caso de uma alimentação elétrica, uma perda completa de energia seria uma falha catastrófica, enquanto um desvio de tensão ou de freqüência seria considerado como uma degradação. Uma falha é primária se não é causada por falha em outra parte do sistema, e secundária se é o resultado da falha de outra parte do sistema. Como exemplo, a falha normal de uma lâmpada incandescente seria uma falha primária, mas a falha que segue uma sobretensão severa seria uma falha secundária porque é o resultado de uma falha em outro lugar. Dados de confiabilidade podem fornecer informação apenas sobre falhas primárias.

Algumas falhas podem ser óbvias, como a queima de uma lâmpada incandescente, mas em outros casos, pode ser muito mais difícil determinar que aconteceu uma falha. Por exemplo, um circuito eletrônico complexo que tem que atender uma especificação detalhada falhou se qualquer parâmetro se deslocou fora dos limites especificados, embora isto pode não ser aparente para o usuário. Um circuito de interface eletrônico pode ser obrigado a ter uma certa imunidade à tensão de ruído; uma falha na manutenção desta imunidade não seria notada sob condições livres de ruído, mas os sintomas seriam aparentes sob condições mais extremas. Em tais casos, falhas e erros podem parecer fortuitos e é provável que seja difícil localizar a causa e efetuar um reparo rapidamente.

A figura 1 mostra a taxa de falha λ(t), em função do tempo. É freqüentemente chamada como uma "curva da banheira" e é típica das obtidas para muitos componentes eletrônicos. Tem três seções distintas:

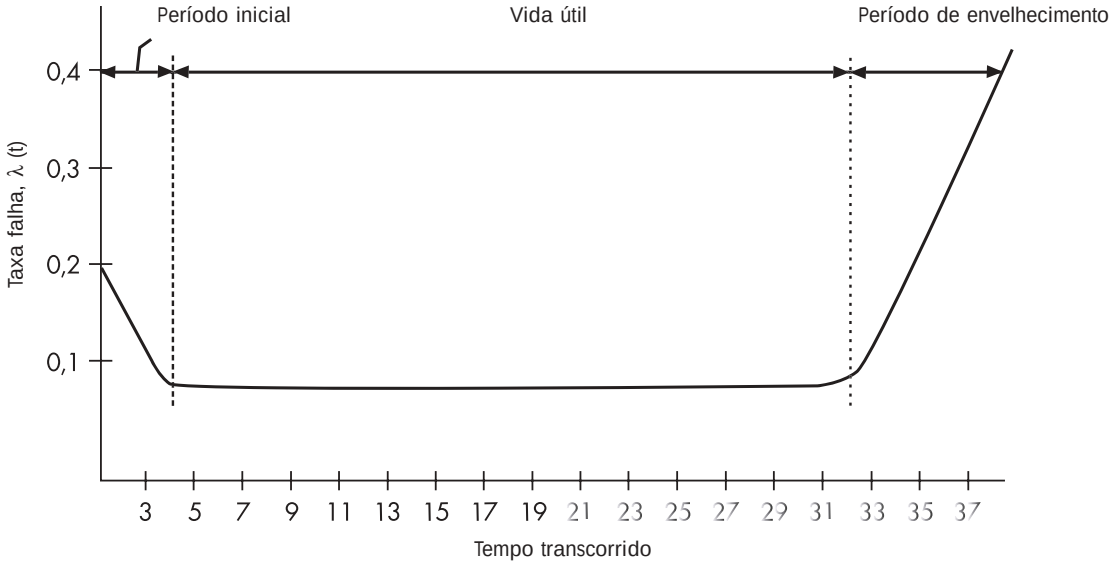


Figura 1 - Taxa de falha em função do tempo.

Período inicial ou "período de queima"

É o período (até a unidade de tempo 4 na Figura 1), quando λ(t) está diminuindo a medida que falham componentes fracos ou abaixo do padrão. É conhecido como período inicial, falha precoce, mortalidade infantil ou "período de queima" (burn-in). As razões para os primeiros três termos são óbvias. O período inicial é um processo usado às vezes nas fases finais de fabricação de componentes de forma a eliminar falhas precoces. Envolve os componentes que funcionaram sob condições normais (ou condições controladas um pouco mais severas que o normal para acelerar o processo) por um tempo suficientemente longo para superar o período inicial.

Vida útil ou período operacional normal

É um período de $\lambda(t)$ efetivamente constante, relativamente baixa (da unidade de tempo 5 até a unidade de tempo 31 na Figura 1), conhecido como a vida útil ou período de operação normal. Durante este tempo, a taxa de falha é independente do tempo durante o qual o componente funcionou. Em outras palavras, a probabilidade de falha de um componente é a mesmo ao longo deste período.

Desgaste ou período de envelhecimento

Este é o período em que a taxa de falha aumenta abruptamente com o tempo (além da unidade de tempo 31 na Figura 1), conhecido como o período de desgaste ou de envelhecimento.

A curva da banheira descreve o comportamento que poderia ser esperado para muitos tipos de componentes, ou até mesmo para sistemas complexos como um UPS. Adotando o exemplo familiar das lâmpadas incandescentes, falhas durante o período inicial poderiam ser devidas a filamentos que foram mal fixados aos seus suportes, que foram localmente desenhados muito finos ou que têm fendas. Outra causa de falha precoce poderia ser invólucros de vidro mal vedados, levando à oxidação do filamento. Durante a vida útil os filamentos evaporam gradualmente e ficam mais finos até quebrar, geralmente sob solicitação térmica induzida por surtos de corrente ao acender. Se todos os bulbos fossem idênticos e operados sob condições idênticas, falhariam todos ao mesmo tempo. Contudo, já que nenhum processo de fabricação produzirá componentes idênticos, alguns terão defeitos sérios que conduzem a falha durante o período inicial, e a taxa de falha diminui assim que os componentes mais fracos são eliminados. Igualmente, é razoável esperar uma série de falhas durante o período de desgaste. No caso de lâmpadas incandescentes, a composição do filamento, sua espessura, comprimento e forma variarão ligeiramente de bulbo para bulbo, levando assim a um intervalo de tempo após o que finalmente quebram. A medida que os bulbos envelhecem, sua probabilidade de falha aumenta, dando origem à parte direita da curva da banheira.

É talvez mais difícil entender por que deveria ocorrer qualquer falha durante o período operacional normal, uma vez que as falhas precoces foram eliminadas e não houve ainda qualquer desgaste significativo. Uma análise detalhada das numerosas formas em que uma lâmpada incandescente poderia falhar seria extremamente complexa por causa da variedade de processos mecânicos, térmicos e químicos que podem acontecer. A ampla gama de possibilidades, cada uma com sua própria dependência de tempo, leva em média a produzir uma probabilidade de falha que é efetivamente independente do tempo. O processo é chamado “sem memória” (memory-less), porque a probabilidade de falha é assumida independentemente do histórico prévio. Estas falhas também são chamadas às vezes catastróficas porque são inesperadas. Na realidade, em muitos casos, os processos de desgaste estão acontecendo já a um nível muito baixo, de forma que o processo não é na verdade “sem memória”.

A fabricação de componentes e conjuntos freqüentemente envolve um “processo de queima” de forma que aqueles sujeitos a falha no período inicial possam ser removidos da cadeia de fornecimento. Em muitos casos, componentes eletrônicos não alcançam seu período de desgaste durante a vida operacional - eles podem ter vidas úteis muito mais longas do que a vida operacional do sistema no qual são usados. Deveriam ser estabelecidos procedimentos de manutenção de rotina para assegurar que componentes que podem sofrer desgaste - baterias recarregáveis, por exemplo - sejam substituídos bem antes do começo do envelhecimento. Por causa disto, pode-se geralmente assumir que os componentes são utilizados apenas durante seu período de vida útil e que têm uma taxa de falha constante.

Tempo médio até a falha (MTTF)

O tempo médio até a falha é um termo que é aplicado a partes não reparáveis como lâmpadas incandescentes, e é uma medida do tempo médio até a falha de um número grande de partes semelhantes que operam sob condições especificadas. As condições de ensaio são importantes, por exemplo, um aumento na temperatura de operação ou na tensão da maioria dos componentes reduzirá

o MTTF.

Na prática, o MTTF é calculado em muitos casos a partir de dados obtidos durante um período de tempo no qual não falham todos os componentes. Neste caso:

$$\text{MTTF} = \frac{\text{Tempo de operação total para todos os componentes}}{\text{Número de falhas naquele tempo}}$$

Tempo médio entre falhas (MTBF)

No caso de componentes ou elementos de sistema que podem ser reparados, as taxas de falha são freqüentemente expressadas em termos do tempo médio entre falhas (MTBF, do inglês Mean Time Between Failures) em lugar do tempo médio até a falha (MTTF). Esta é uma medida do tempo médio em que uma peça de equipamento executa sua função sem precisar reparo (embora pode requerer manutenção programada de rotina).

Como MTTF e MTBF são quantidades estatísticas, um grande número de falhas deve ser registrado para estabelecer confiança no resultado. Testar uma peça de equipamento durante um tempo muito longo é impraticável, portanto é habitual testar um número grande de amostras simultaneamente por um período mais curto, e determinar o número total de falhas no tempo de operação total para todas as amostras. Este método assume que os modos de falha no período inicial e no período de envelhecimento não estão envolvidos.

Disponibilidade e tempo médio para reparo (MTTR)

Os usuários de sistemas estão agora mais preocupados com a disponibilidade do que com a

$$\text{Disponibilidade} = \frac{\text{MTBF}}{\text{MTBF} + \text{MTTR}}$$

confiabilidade. A disponibilidade de um sistema ou de um componente é a proporção de tempo no qual está operando corretamente e disponível para uso. É a relação entre o tempo de operação e o tempo total, o qual é a soma dos tempos de operação e de reparo. O tempo médio necessário para reparos é chamado tempo médio para reparos (MTTR, do inglês Mean Time to Repair).

Os tempos de MTTR são especificados pelos fabricantes sob condições ideais, assumindo, por exemplo, que o local da falha é óbvio, que o nível de habilidade exigido para identificá-lo está disponível, que peças sobressalentes e procedimentos de reparo adequados estão disponíveis e que, uma vez consertado, o sistema pode ser testado e recomissionado. Na vida real, as falhas ocorrem no pior momento possível. Um determinado MTTR de vinte minutos é uma pequena vantagem se um engenheiro tiver que viajar para o local para identificar o problema e então obter peças de um depósito ou, pior ainda, de um distribuidor. Logo após do reparo, o sistema deve ser testado e recomissionado antes de poder iniciar novamente o trabalho real. Cada um destes passos pode tomar muito mais tempo que o próprio reparo. Algumas perdas de tempo podem ser evitadas - podem ser mantidas peças sobressalentes críticas no local, o pessoal próprio pode ser treinado para suprir as habilidades técnicas necessárias - mas estes passos têm que ser implementados com boa antecedência e apresentam suas próprias implicações de custo. Adotando o exemplo simples de um conserto de televisão que toma, digamos, 30 minutos para substituir uma placa de circuito, o fabricante citaria um MTTR de meia hora. Mas o usuário vê as coisas de forma diferente. O aparelho quebra quando a loja de conserto está fechada. Tem que ser recebido, a falha identificada, e localizadas as peças para substituição. Depois que um orçamento estiver pronto e aprovado, a peça é adquirida, e - agora começam os 30 minutos -

instalada e testada. No próximo dia o aparelho é devolvido ao usuário, que experimentou um MTTR de talvez uma semana. Se o MTBF for bastante longo, o usuário pode estar bastante satisfeito, mas se o MTBF é curto o usuário pode muito bem querer ter um aparelho de televisão redundante disponível!

Muitas vezes, o reparo será feito mediante a substituição por um componente ou subsistema novo ou previamente consertado. Quando um subsistema consertado é utilizado, tem que ser lembrado que apenas alguns dos componentes são novos, enquanto os componentes restantes já são velhos. O MTTF deve ser menor que o de uma unidade nova.

Para ser completamente justo, o MTTR deveria incluir também o tempo ocioso necessário para manutenção preventiva normal em serviço, como a revisão de um motor de gerador, substituição das baterias ou limpeza dos filtros dos ventiladores de um UPS, etc. Felizmente, o tempo ocioso de máquina para permitir a manutenção preventiva pode ser planejado de forma que a interrupção seja minimizada, mas muitas vezes não pode ser eliminado.

Maximizar a proporção de tempo em que um sistema está disponível envolve um acerto entre confiabilidade de componente e tempo de conserto. Por exemplo, componentes do tipo plug-in são geralmente muito menos confiáveis que os conectados por cabos, por causa das taxas de falhas relativamente altas das conexões. Por outro lado, os tempos de conserto de componentes do tipo plug-in serão muito mais curtos que os dos conectados por cabos, porque eles podem ser substituídos de forma simples por operadores relativamente menos qualificados. O equilíbrio ótimo depende dos valores absolutos de MTBF e o MTTR verdadeiro, levando totalmente em conta as instalações e habilidades disponíveis no local.

A disponibilidade de sistema é simplesmente o MTBF dividido por MTBF mais o MTTR verdadeiro - incluindo os itens extras há pouco discutidos. Valores de disponibilidade insignificantes parecem freqüentemente muito impressionantes, mas devem ser usados com cuidado. Uma disponibilidade aparentemente excelente de 0,9999 se traduz em uma indisponibilidade de cerca de uma hora por ano - um nível completamente inaceitável para muitas operações. Atingir mais do que isto na prática - simplesmente aumentando a confiabilidade - é bastante difícil; os valores de MTBF, sendo estatísticos, não podem ser aceitos em qualquer exemplo particular e os valores de MTTR são geralmente otimistas, sendo baseados nas suposições feitas na atmosfera calma de um sistema de trabalho. Além disso, a complexidade dos sistemas modernos, tais como redes de computadores corporativas e controle de processo de fábrica, significa que um grande número de subsistemas tem que trabalhar juntos com perfeição para manter a operação. Alcançar a disponibilidade mais alta requer uma abordagem de projeto diferente, com foco em tolerar e sobreviver às falhas inevitáveis em lugar de tentar reduzi-las - em outras palavras, um projeto resiliente.

Resiliência

Um sistema resiliente é aquele que pode suportar uma série de falhas de subsistemas e componentes enquanto continua operando normalmente. Isto pode ser conseguido instalando equipamento adicional - redundância - junto com projeto cuidadoso - eliminando pontos isolados de falha - e manutenção bem planejada.

É essencial uma abordagem equilibrada. O acréscimo de equipamento redundante é uma solução óbvia, porém cara, e por isso só deve ser adotada após uma consideração adequada dos custos e benefícios. A introdução de procedimentos de manutenção adequados é relativamente econômica, mas garantir que eles sejam observados corretamente nunca é fácil! Um equilíbrio cuidadoso de soluções técnicas e administrativas ou de procedimento dará a melhor relação custo/benefício.

Os elementos essenciais de uma instalação resiliente são:

- redundância;
- eliminação de pontos isolados de falha;
- bons procedimentos de manutenção.

Redundância

A redundância é um método útil de disponibilidade crescente e otimização do equilíbrio entre efetividade de operação e despesa. Circuitos alternativos, equipamento ou componentes são instalados de forma que, no caso de uma ou várias faltas, a funcionalidade é preservada. O nível e o tipo de redundância fornecida determinam o nível de funcionalidade mantido e o número e tipos de faltas permitidas.

Redundância standby

Redundância standby significa que são providos meios alternativos de executar a função, que permanecem inoperantes até que sejam necessários. É ligada em caso de falha dos meios primários de execução da função. Um departamento de TI poderia manter vários monitores disponíveis e usá-los para substituir aqueles que falham em serviço - é um exemplo de redundância standby.

A desvantagem da redundância standby é que há um período inevitável de interrupção do serviço entre a ocorrência da falha e a colocação em funcionamento da unidade redundante. Tais esquemas são raramente satisfatórios para sistemas críticos em situações comerciais e industriais modernas.

Redundância ativa ou paralela

Na redundância ativa ou paralela, todas as unidades redundantes estão operando simultaneamente em lugar de serem ligadas quando necessário (Figura 2). A abordagem mais óbvia é usar dois componentes, cada um capaz de alimentar a carga completa, de forma que, se um falhar, o outro assumirá a carga - procedimento chamado redundância 1+1. Uma abordagem alternativa é dividir a carga entre várias unidades, cada uma capaz de assumir apenas uma fração da carga, e prover somente uma unidade redundante adicional - a chamada redundância N+1. Para cargas muito críticas, podem ser previstas mais de uma unidade redundante para a capacidade total. Por exemplo, um esquema de redundância 1+2 teria três unidades de capacidade total alimentando a carga e exigiria que as três unidades falhassem antes que o sistema falhasse.

Como não há nenhuma interrupção, a redundância ativa é satisfatória para instalações de computador. O uso de discos duplicados em um servidor de rede é um exemplo de redundância 1+1.

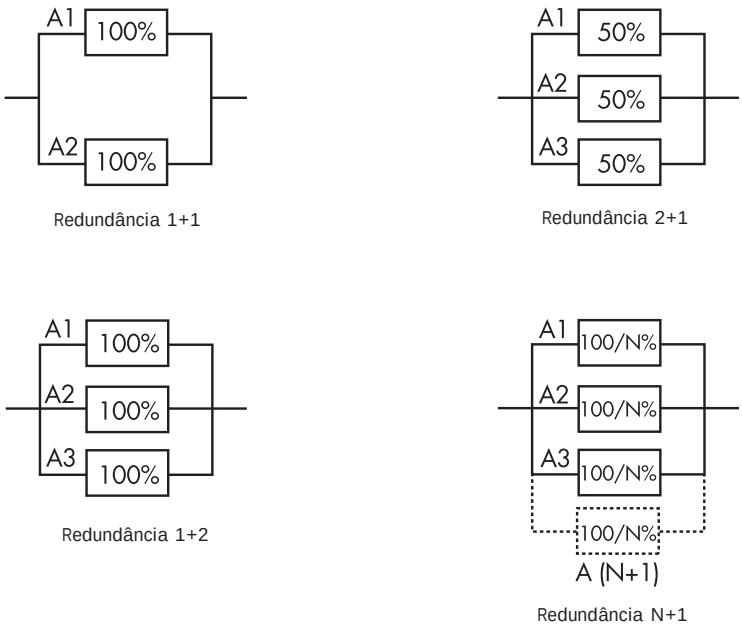


Figura 2 - Exemplos de redundância ativa.

Redundância N+1

Uma alternativa mais econômica é usar um número maior de unidades de capacidade nominal menor para atender a carga e prover uma unidade redundante extra. Por exemplo, uma carga de 800 kVA poderia ser conectada a cinco unidades UPSs de 200 kVA, sendo quatro delas suficientes para atender a carga. Este procedimento é chamado redundância 4+1 porque são necessárias quatro unidades e uma é redundante. A redundância N+1 pode ser mais econômica de implementar que a 1+1, e é mais flexível; se a carga cresce é simples acrescentar outra unidade de forma que um sistema 2+1 se torna um sistema 3+1. Por outro lado, deveriam ser evitados extremos; toda unidade adicional é outra falha em potencial, portanto há um equilíbrio a ser encontrado entre a resiliência de sistema adicional e o custo adicional e o potencial de falha da unidade (não sistema) acrescida.

Um sistema de disco RAID 5 em um servidor é um exemplo de redundância N+1. Dados de correção de erro adicionais são acrescentados aos dados originais e depois logicamente dispersados em vários discos. Se um disco falhar, todos os dados podem ser recuperados em tempo real dos discos restantes e o conteúdo de disco com falha reconstruído.

Vale a pena notar que o fornecimento de um UPS é, em primeiro lugar, uma aceitação da necessidade de um fornecimento de energia redundante, e a redundância acrescentada para o próprio UPS é uma extensão lógica desse conceito.

Eliminação de pontos de falha isolados

Acrescentar redundância é caro, e assim quanto e o que prover deve ser considerado cuidadosamente.

Uma avaliação de risco deve ser realizada, analisando o risco de ocorrer uma determinada falha e o efeito dessa falha no sistema. Deveria ser dada prioridade para aquelas falhas onde a combinação de probabilidade e efeito de sistema é mais alta - possivelmente incluindo um evento muito raro de efeito

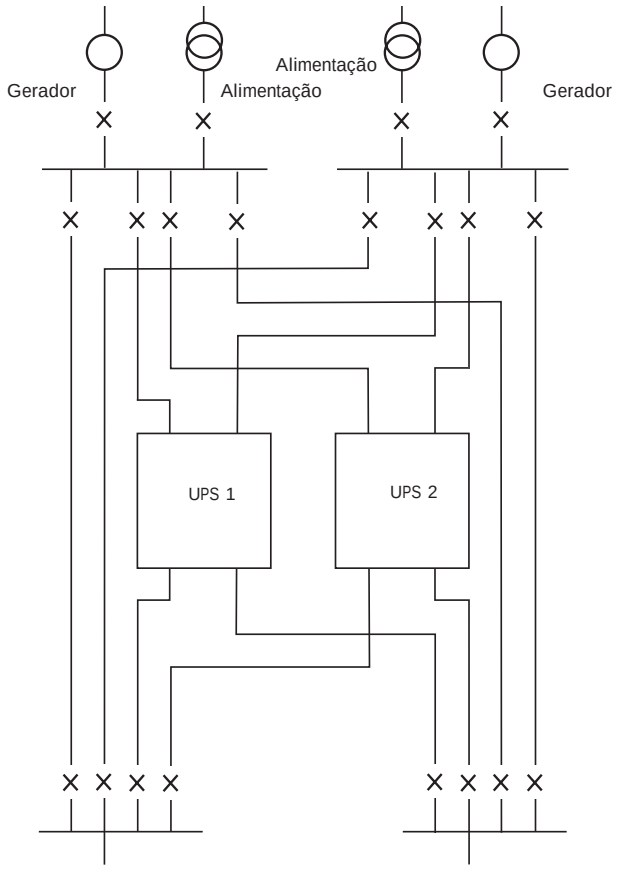


Figura 3 - Exemplo de um sistema resiliente.

catastrófico e um evento freqüente que causa menor distúrbio. Este estudo deveria identificar todos os pontos de falha isolados – aquelas falhas isoladas simples que podem derrubar uma operação inteira. O estudo deveria ser exaustivo e meticuloso, olhando não apenas as peças principais de equipamento, mas também as caixas de controle e a fiação de sinal que as conecta. Se o sistema de controle ou suas interconexões forem a causa da falha, o caro equipamento auxiliar não ajudará!

A Figura 3 mostra um exemplo de um sistema de fornecimento de energia resiliente. Este projeto tem duas alimentações independentes, a partir de pontos de rede separados, apoiados por dois geradores auxiliares independentes. A energia de qualquer conexão de entrada pode ser endereçada para uma qualquer ou ambas conexões de saída diretamente ou via qualquer das duas unidades de UPS. Chaves de transferência estáticas são usadas para conectar e isolar equipamentos e caminhos, conforme exigido. Este exemplo é simétrico e assume que as cargas em cada saída são igualmente críticas; em outras circunstâncias, uma saída pode ser usada para alimentar cargas altamente críticas enquanto as outras alimentam cargas normais. Em serviço normal, a energia de uma alimentação seria endereçada para ambas saídas por um UPS. No caso de uma falha de alimentação, seria feita a conexão à alimentação alternativa com o UPS fornecendo energia durante o curto período de transferência. Se a alimentação alternativa não estiver disponível, é dada então partida num gerador auxiliar e uma vez atingida a velocidade de regime, conectado ao sistema; novamente um UPS forneceria energia durante o retardo na partida. Se ambas alimentações e ambos geradores falharem, ou estiverem fora de serviço para manutenção, então as unidades de UPS seriam usadas para alimentar as conexões de saída independentemente. Seria aplicado então um esquema de rejeição de carga para estender o tempo de alimentação.

Este é um exemplo extremo. Seria bastante caro de implementar, mas pode ser justificável em situações onde perda de vida ou perda financeira séria podem resultar da falha. É usado aqui para ilustrar o que pode ser alcançado, mas na maioria das circunstâncias um subconjunto deste sistema seria apropriado, baseado em um exame crítico dos riscos envolvidos e do custo da proteção.

Mantendo um sistema resiliente

Os procedimentos de manutenção são a chave para preservar a resiliência de um sistema e estes procedimentos devem ser levados em conta durante a avaliação de risco. Se, por exemplo, uma de quatro unidades de UPS falhou, e as três unidades restantes estão mantendo a carga, como esta situação é reconhecida de forma que um conserto possa ser efetuado? Qual é o risco de ocorrer uma segunda falha enquanto as unidades restantes estiverem operando com carga mais alta? A carga poderia ter crescido após o comissionamento além da capacidade de apenas três unidades sem a equipe de manutenção estar ciente? Devem ser desenvolvidos procedimentos detalhados para cobrir estas e muitas outras situações durante a fase de análise de risco de forma que possam ser testados rigorosamente.

O fato de que uma instalação tenha sido projetada para ser resiliente pode encorajar o relaxamento dos padrões de manutenção. Afinal de contas, não importa se uma unidade em particular falha – a instalação pode sobreviver sem ela. Esta atitude é uma receita para o desastre. Em primeiro lugar, existem motivos mais do que suficientes para a ocorrência de uma falha e não há nenhuma necessidade de multiplicar as possibilidades. Em segundo lugar, se uma unidade desligar devido a falta de manutenção, é provável que suas equivalentes estejam em um estado semelhante e é possível que falhem da mesma forma quando enfrentadas com carga adicional.

Testar o sistema também é importante. A equipe de manutenção precisa estar confiante de que o sistema poderá lidar com falhas, e tem que executar testes regularmente simulando a perda de itens individuais de equipamento. Este é um passo corajoso, melhor se for adotado inicialmente, no comissionamento da instalação. Tendo estabelecido que a instalação é resiliente, testes regulares podem ser executados com alta confiança de sucesso. Naturalmente, os testes sempre deveriam ser realizados quando as conseqüências da falha estão num mínimo, mas também tem que representar as condições reais da instalação.

Conclusão

A disponibilidade é a preocupação principal de projetistas de instalação e equipes de manutenção. Disponibilidade alta não pode ser alcançada na prática apenas por meio de confiabilidade alta - também são requeridos um bom projeto resiliente e procedimentos de manutenção adequados. O projeto e a implementação de um sistema resiliente é apenas o primeiro passo de uma longa jornada.

Um ponto isolado de falha escondido

A Figura 4 mostra uma instalação na qual uma parte significativa da carga é composta de motores com correção de fator de potência provida por um banco de capacitores automático. Circuitos de controle ligam a capacitância correta para corrigir o fator de potência da carga de motores instantânea, assegurando que a corrente reativa ou "corrente dewattada" seja minimizada. Isto reduz a carga em transformadores, aparelhagens e cabos, bem como a tarifa cobrada pelo fornecedor.

Devido ao fato de que o fator de potência da carga é compensado, a magnitude da corrente é reduzida com relação ao valor normal não compensado. Agora o transformador tem capacidade disponível e é capaz de assumir carga adicional - mas só enquanto o sistema de correção do fator de potência está operando. Se for acrescentada carga extra, e o sistema de correção de fator de potência falhar, a corrente de carga excederá a capacidade do transformador resultando em um desligamento por sobrecarga ou

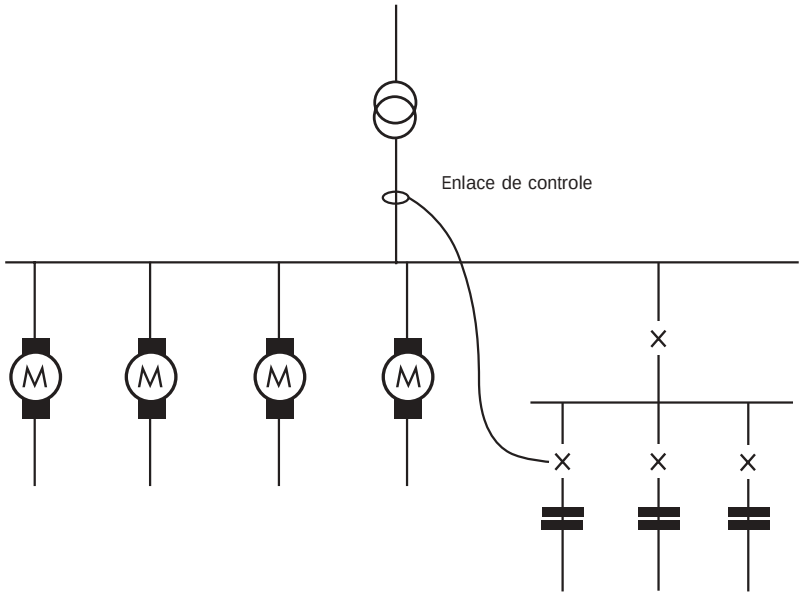


Figure 4 - Correção de fator de potência usando um banco de capacitores automático.

uma falha definitiva.

O sistema de correção do fator de potência, seu sistema de medição e controle, e até mesmo o seu disjuntor, são todos eles críticos agora para a sobrevivência do transformador e da instalação. A confiabilidade da instalação inteira é reduzida para o menos seguro destes componentes.

Rede de Parceiros

Copper Benelux
168 Avenue de Tervueren
B-1150 Brussels
Belgium

Tel: 00 32 2 777 7090
Fax: 00 32 2 777 7099
Email: mail@copperbenelux.org
Web: www.copperbenelux.org

Contact: Mr B Dôme

Copper Development Association
Verulam Industrial Estate
224 London Road
St Albans AL1 1AQ
United Kingdom

Tel: 00 44 1727 731205
Fax: 00 44 1727 731216
Email: copperdev@compuserve.com
Webs: www.cda.org.uk & www.brass.org

Contact: Mrs A Vessey

Deutsches Kupferinstitut e.V
Am Bonneshof 5
D-40474 Duesseldorf
Germany

Tel: 00 49 211 4796 323
Fax: 00 49 211 4796 310
Email: sfassbinder@kupferinstitut.de
Web: www.kupferinstitut.de

Contact: Mr S Fassbinder

ECD Services
Via Cardinal Maffi 21
I-27100 Pavia
Italy

Tel: 00 39 0382 538934
Fax: 00 39 0382 308028
Email: info@ecd.it
Web: www.ecd.it

Contact: Dr A Baggini

European Copper Institute
168 Avenue de Tervueren
B-1150 Brussels
Belgium

Tel: 00 32 2 777 70 70
Fax: 00 32 2 777 70 79
Email: eci@eurocopper.org
Web: www.eurocopper.org

Contact: Mr H De Keulenaer

Hevrox
Schoebroeckstraat 62
B-3583 Beringen
Belgium

Tel: 00 32 11 454 420
Fax: 00 32 11 454 423
Email: info@hevrox.be

Contact: Mr I Hendrikx

HTW
Goebenstrasse 40
D-66117 Saarbruecken
Germany

Tel: 00 49 681 5867 279
Fax: 00 49 681 5867 302
Email: wlang@htw-saarland.de

Contact: Prof Dr W Langguth

Istituto Italiano del Rame
Via Corradino d'Ascanio 4
I-20142 Milano
Italy

Tel: 00 39 02 89301330
Fax: 00 39 02 89301513
Email: ist-rame@wirenet.it
Web: www.iir.it

Contact: Mr V Loconsolo

KU Leuven
Kasteelpark Arenberg 10
B-3001 Leuven-Heverlee
Belgium

Tel: 00 32 16 32 10 20
Fax: 00 32 16 32 19 85
Email: ronnie.belmans@esat.kuleuven.ac.be

Contact: Prof Dr R Belmans

Polish Copper Promotion Centre SA
Pl.1 Maja 1-2
PL-50-136 Wroclaw
Poland

Tel: 00 48 71 78 12 502
Fax: 00 48 71 78 12 504
Email: pcpm@miedz.org.pl

Contact: Mr P Jurasz

TU Bergamo
Viale G Marconi 5
I-24044 Dalmine (BG)
Italy

Tel: 00 39 035 27 73 07
Fax: 00 39 035 56 27 79
Email: graziana@unibg.it

Contact: Prof R Colombi

TU Wroclaw
Wybrzeze Wyspianskiego 27
PL-50-370 Wroclaw
Poland

Tel: 00 48 71 32 80 192
Fax: 00 48 71 32 03 596
Email: i8@elektryk.ie.pwr.wroc.pl

Contact: Prof Dr H Markiewicz

Gary Marshall

WSP Communications Ltd
Buchanan House
24-30 Holborn
London EC1N 2HS
United Kingdom

Tel.: 00 44 20 7314 5000
Fax: 00 44 20 7314 5700
Email: gary.marshall@wspgroup.com
Website: www.wspgroup.com

David Chapman

Copper Development Association

Copper Development Association
Verulam Industrial Estate
224 London Road
St Albans AL1 1AQ
United Kingdom

Tel: 00 44 1727 731205
Fax: 00 44 1727 731216
Email: copperdev@compuserve.com
Webs: www.cda.org.uk & www.brass.org

PROCOBRE Connects Life.™

Av. Brigadeiro Faria Lima, 2128-cj.203
Cep 01451-903
São Paulo - SP
Brasil

Tel./Fax: 55 11 3816-6383
e-mail: procobrebrasil@copper.org
Internet: www.procobre.org

COPPER

European Copper Institute
168 Avenue de Tervueren
B-1150 Brussels
Belgium

Tel: 00 32 2 777 70 70
Fax: 00 32 2 777 70 79
Email: eci@eurocopper.org
Website: www.eurocopper.org