Segurança funcional: Medição de temperatura de forma segura conforme norma IEC 61508

Folha de dados WIKA IN 00.19

Introdução

Sob certas condições, os sensores de temperatura podem ser usados em sistemas de segurança em conformidade com a IEC 61508. As especificações do sensor de temperatura como termorresistência ou termopar, bem como características técnicas dos transmissores de temperatura precisam ser levadas em conta para a aplicação dos sistemas de segurança.

Este informativo técnico descreve o básico da segurança funcional em conformidade com a IEC 61508 e aconselha um design de um sistema de segurança do ponto de vista de medição de temperatura.

Necessidade para redução de risco

Devido ao aumento das expectativas da sociedade sobre a segurança das instalações industriais, os riscos apresentados nas instalações foram cada vez mais reduzidos ao longo do tempo. Foram criadas diretrizes e padrões para ajudar cada operador a operar sua planta com os mais altos níveis de segurança. Realizar análises de acidentes e avaliações de risco é a base para isso. O objetivo é reduzir o risco apresentado por um instalação industrial a um risco aceitável em linha com os valores da sociedade por meio de medidas de segurança.

Para evitar falha em uma instalação industrial, são empregados sistemas elétricos / eletrônicos / eletrônicos programáveis (sistemas E / E / PE). A totalidade de todas as funções de segurança necessárias que servem para manter o estado seguro de uma planta é referido como um sistema instrumentado de segurança SIS ou sistema relacionado à segurança.

Um exemplo desse sistema de segurança é um sistema de monitoramento de temperatura que, quando os limites de temperatura são excedidos, desliga de forma confiável o fornecimento de energia de uma planta, colocando-a no estado seguro e evitando assim um evento perigoso.

Arquitetura de um sistema relacionado à segurança

Um sistema eletrônico elétrico / eletrônico / eletrônico programável consiste basicamente nos elementos sensores, controlador e atuador. Neste caso, se refere a uma arquitetura de um único canal do sistema de segurança (sistema 1oo1). A arquitetura descreve a configuração específica de elementos de hardware e software em um sistema. Um sistema 1oo1 indica que o sistema é composto por um canal, que deve operar de forma segura para que a função de segurança possa ser realizada (1 out of 1). Para sistemas de segurança com arquitetura multicanal, os elementos de hardware ou software são implementados com redundância (consulte "Sistemas redundantes").

Exemplo de uma arquitetura de um único canal para um sistema instrumentado de segurança

Um sensor de temperatura com modelos de transmissor de temperatura T32.1S (versão de montagem em cabeçote) e T32.3S (versão de montagem de trilho) pode ser usado pelo operador da planta como um subsistema de sensor de um sistema instrumentado de segurança.

Transmissor de temperatura, modelo T32.xS

Base legislativa

A série de normas IEC 61508 "Segurança funcional de sistemas elétricos / eletrônicos / eletrônicos programáveis de segurança relacionados à segurança" é referida como um padrão de segurança fundamental. Elas descrevem as medidas para prevenção e contenção de falhas em instrumentos e plantas e podem ser utilizadas independentemente do setor industrial.

A IEC 61508 deve ser usada em particular quando:
- A função de segurança é implementada através de um sistema E/E/EP
- Uma falha no sistema instrumentado de segurança levará perigo às pessoas e ao meio ambiente
- Não existe uma regulamentação especifica para o projeto de sistemas de segurança

A IEC 61508 representa o estado da arte em relação ao projeto de sistemas instrumentados de segurança. Com o design dos sistemas de segurança, a melhor tecnologia disponível e, portanto, a IEC 61508, deve ser seguida.

Para planejadores, contratados e operadores do sistema de segurança, também existem padrões específicos de aplicação. São, por exemplo, a IEC 61511 "Segurança funcional - sistemas instrumentados de segurança para o setor da indústria de processos" para a indústria de processos e EN 62061 "Segurança de máquinas - Segurança funcional de sistemas elétricos, eletrônicos e programáveis de controle eletrônicos relacionados à segurança", para construção de máquinas.

Um sensor de temperatura pode ser usado em um sistema instrumentado de segurança de acordo com a norma IEC 61508 quando o instrumento é usado em conjunto com um transmissor de temperatura certificado para aplicações relevantes de segurança. O modelo de transmissor de temperatura T32.xS da WIKA foi desenvolvido com referência à IEC 61508 para uso na indústria de processos e certificado pela TÜV Rheinland para esta aplicação.

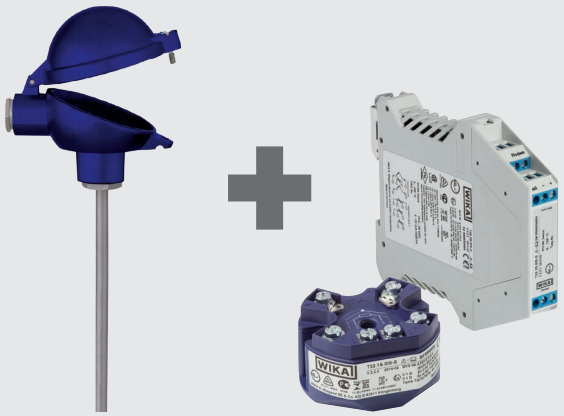
Um sensor de temperatura sem transmissor de temperatura, por exemplo, uma termorresistência ou um termopar, não é coberto pela IEC 61508, uma vez que (por exemplo) um resistor de medição é um componente elétrico simples que não pode realizar nenhum autodiagnóstico nem detectar erros.

Para sensores de temperatura sem transmissor de temperatura certificado pela IEC 61508, somente as taxas de falha podem ser especificadas. Isso ocorre porque sempre depende do instrumento de avaliação do operador quanto a quais tipos de falha podem ser detectados e reconhecidos de forma segura no sensor de temperatura.

Com a certificação do transmissor de temperatura modelo T32.xS, o transmissor de temperatura foi considerado em conexão com um sensor de temperatura. No manual de segurança "Informações sobre a segurança funcional do transmissor de temperatura modelo T32.xS", são especificados os valores característicos relevantes para a segurança do transmissor de temperatura, os sensores de temperatura conectados e toda a montagem.

Para a avaliação, o subsistema do sensor é dividido nos elementos "sensor de temperatura" e "transmissor de temperatura". Os sensores de temperatura são classificados como componentes do tipo A (componente elementar) e o transmissor de temperatura como componentes do tipo B (componente complexo).

Subsistema de sensor consistindo em transmissor de temperatura e sensor de temperatura



Termopar ou termorresistência | **Transmissor de temperatura modelo T32.xS**

Avaliação de sistemas relacionados à segurança

A probabilidade de que uma função de segurança sob demanda seja realizada (ou seja, quando ocorre uma falha no sistema) é definida pela integridade de segurança. Para obter uma medida dos requisitos de integridade de segurança, estes são divididos em quatro níveis de integridade de segurança (SIL). Se o SIL 4 for alcançado, a probabilidade de que a função de segurança seja executada é máxima e, assim, a máxima redução de risco possível é assegurada.

Níveis de integridade de segurança

O termo “SIL“ é, portanto, um parâmetro importante do sistema de segurança, mas é frequentemente usado como sinônimo de “Segurança funcional“.

O nível de integridade de segurança sempre se refere a todo o sistema de segurança. Um elemento não tem SIL, mas ainda pode ser adequado para uma aplicação SIL. Por exemplo, o transmissor de temperatura modelo T32.xS sozinho não forma um sistema relacionado à segurança. O operador é responsável por definir e manter o nível de integridade de segurança requerido, bem como todo o sistema de segurança e os elementos individuais!

A WIKA, como um fabricante de sensor de temperatura, dá suporte ao usuário nisto. Por um lado, por confirmar que os requisitos da IEC 61508 foram atendidos durante o desenvolvimento do T32.xS. Por outro lado, o operador pode ser fornecido com os dados característicos de segurança adequados para o projeto da planta e a avaliação da função de segurança.

Requisitos em um sistema de segurança

Para projetar um ponto de medição de temperatura otimizado para um sistema relacionado à segurança, os seguintes aspectos devem ser considerados:

- O estado seguro da planta e a função de segurança de cada elemento devem ser definidos pelo operador.
- O nível de integridade de segurança exigido deve ser determinado pelo operador do sistema de segurança através de uma avaliação de risco, ex.: gráficos de risco.
- As condições de operação do sensor (meio de processo, influências ambientais) devem ser suficientemente especificadas para que o ponto de medição de temperatura possa ser projetado de maneira otimizada em cooperação com a WIKA.
- As instruções na documentação da WIKA sobre o sensor utilizado devem ser observadas.
- Certifique-se de que as partes molhadas são adequadas para o meio de medição.

Fundamental para uma segurança ideal no ponto de medição de temperatura é o projeto correto do sensor de temperatura, correspondente aos requisitos do processo. O próximo passo é a seleção de um transmissor de temperatura adequado para sistemas de segurança, que detecta tantos tipos de falhas quanto possível do sensor de temperatura e do próprio transmissor.

Determinação do nível de integridade de segurança máxima possível com o exemplo do modelo de transmissor de temperatura T32.xS

Para determinar o nível de integridade de segurança de um sistema relacionado à segurança, devem ser determinados os requisitos para a integridade de segurança sistemática e a integridade da segurança do hardware.

Integridade de segurança sistemática

Para cumprir os requisitos para a integridade de segurança sistemática, devem ser tomadas em consideração falhas sistemáticas. Falhas sistemáticas são falhas de projeto, falhas de fabricação ou falhas de operação. Para reduzir isso, a IEC 61508 especifica medidas de segurança que devem ser mantidas durante toda a vida útil (ciclo de vida do produto) de um sistema técnico. O ciclo de vida de segurança dos sistemas de segurança começa com a concepção e termina com o desmantelamento. Como parte do gerenciamento de segurança durante o desenvolvimento do T32.xS, foram evitadas falhas sistemáticas, por exemplo, por meio de atividades de validação e verificação, bem como planejamento e documentação completa. Assim, o software do modelo T32.xS cumpre até os critérios de SIL 3 relativos à integridade de segurança.

Integridade da segurança do hardware

Falhas aleatórias
Para avaliar a integridade da segurança do hardware, devem ser observadas falhas aleatórias. Estas são causadas por alterações aleatórias do comportamento de um componente, ex: circuito aberto, curto-circuito ou mudança aleatória no valor de um capacitor em um circuito elétrico. Falhas aleatórias não podem ser evitadas. Somente a probabilidade de ocorrência de tal falha pode ser calculada. A taxa de falha é dada na unidade FIT (Falhas no tempo ou termo inglês “Failures in Time“) .

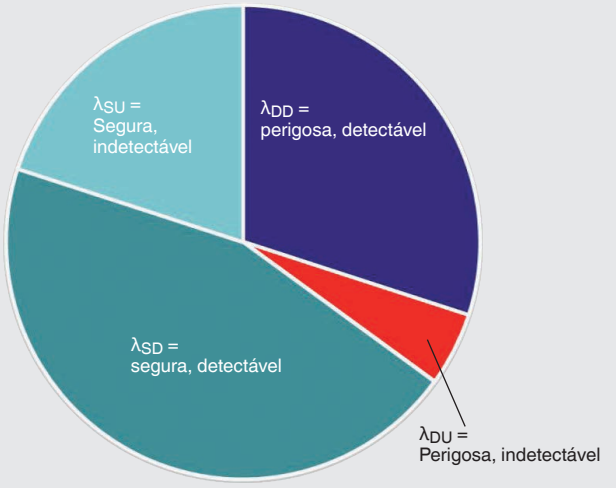
Ela é definida como: $1\ FIT = 10^{-9}\ \frac{1}{h}$

A totalidade de todas as falhas em um intervalo de tempo a uma taxa constante de falha é referida como a taxa de falha de base λB. A taxa de falha de base é composta por falhas perigosas λD = falhas perigosas e não perigosas λS = seguras, que têm impacto na função de segurança.

$$\lambda = \lambda_S + \lambda_D$$

Dependendo se uma falha, por exemplo, pode ser detectada através de uma função de diagnóstico da eletrônica no sistema de segurança ou permanece não detectada, as falhas perigosas e não perigosas são ainda divididas.

Subdivisão das taxas de falhas



Tipos de falhas em um sensor de temperatura
As seguintes falhas podem ocorrer em um sensor de temperatura. Circuito aberto - o circuito de medição é interrompido

- Curto circuito - dois cabos de conexão estão conectados sem querer
- Variação devido a mudanças no material do resistor ou variação na tensão termoelétrica
- Mudança na resistência da ponta, ex: através de mudanças de temperatura

Dependendo das funções de detecção de falha do transmissor de temperatura usado, o tipo de falha (λSD, λSU, λDD, λDU) para diferentes falhas no sensor de temperatura deve ser definido.

Tabela 1: Detecção de falhas através do modelo de transmissor de temperatura T32.xS

Possíveis casos de falha em sensores de temperatura	Termorresistência, 2 fios	Termorresistência, 3 fios	Termorresistência, 4 fios	Termopar
Circuito aberto	λ_{DD}	λ_{DD}	λ_{DD}	λ_{DD}
Curto circuito	λ_{DD}	λ_{DD}	λ_{DD}	**λ_{DU}**
Variação	**λ_{DU}**	**λ_{DU}**	**λ_{DU}**	**λ_{DU}**
Mudança na resistência da ponta	**λ_{DU}**	λ_{DD} 1)	λ_{DD}	λ_{DD}

1) Uma mudança da resistência da ponta em uma ligação a 3 fios só pode ser detectada com base no entendimento de que os cabos de conexão entre o resistor de medição e o transmissor são do mesmo comprimento e têm a mesma seção transversal do condutor.

Na literatura, as taxas de falha para termopares e termorresistência são dadas em diferentes aplicações e configurações. As taxas de falha são baseadas no "pior caso" de uma falha no sensor e servem de orientação para o projeto de sistemas instrumentados de segurança. As taxas de falha devem ser utilizadas levando em consideração as condições de operação e o cabo de conexão entre o ponto de medição e o transmissor. Elas são diferenciadas de acordo com os requisitos de vibração no local de operação (baixo estresse / alto estresse) e no tipo de conexão entre o ponto de medição e o transmissor de temperatura (montagem direta / cabo de ligação) (ver "Definições e abreviaturas").

Tabela 2: Taxas de falha para termopares sem transmissor de temperatura 2)

Tipo de falha	Montaem direta		Cabo de ligação	
	Baixo estresse	Alto estresse	Baixo estresse	Alto estresse
Circuito aberto	95 FIT	1.900 FIT	900 FIT	18.000 FIT
Curto circuito	4 FIT	80 FIT	50 FIT	1.000 FIT
Variação	1 FIT	20 FIT	50 FIT	1.000 FIT

2) As taxas de falha indicadas são baseadas em cálculos pela WIKA usando dados básicos da exida.com L.L.C (veja a página 12 "Literatura e fontes", "Exida")

Tabela 3: Taxas de falha para termorresistência com ligação a 4 fios sem transmissor de temperatura [2)]

Tipo de falha	Montagem direta		Cabo de ligação	
	Baixo estresse	Alto estresse	Baixo estresse	Alto estresse
Circuito aberto	42 FIT	830 FIT	410 FIT	8.200 FIT
Curto circuito	3 FIT	50 FIT	20 FIT	400 FIT
Variação	6 FIT	120 FIT	70 FIT	1.400 FIT

Tabela 4: Taxas de falha para termorresistência com ligação a 2 ou 3 fios sem transmissor de temperatura [2)]

Tipo de falha	Montagem direta		Cabo de ligação	
	Baixo estresse	Alto estresse	Baixo estresse	Alto estresse
Circuito aberto	38 FIT	758 FIT	371 FIT	7.410 FIT
Curto circuito	1 FIT	29 FIT	10 FIT	190 FIT
Variação	9 FIT	173 FIT	95 FIT	1.900 FIT

2) As taxas de falha indicadas são baseadas em cálculos pela WIKA usando dados básicos da exida.com L.L.C (veja a página 12 "Literatura e fontes", "Exida")

Limitação do nível de integridade de segurança de um elemento

O máximo nível de integridade de segurança "SIL" alcançável de um elemento do sistema de segurança é limitado pelos seguintes fatores:

- Proporção de falhas seguras de um elemento de hardware (Safe Failure Fraction, SFF)
- Hardware Fault Tolerance (HFT)
  A tolerância a falhas de hardware representa uma medida do grau de redundância do sistema de segurança. Com uma tolerância de falha de hardware de N, N + 1 é o número mínimo de erros que podem levar à perda de uma função de segurança. Um sistema instrumentado de segurança com arquitetura de canal único possui uma tolerância de falha de hardware de 0.
- Complexidade dos componentes (componentes tipo A e B)
  - Os componentes de tipo A são componentes principais cujo desempenho de falha está totalmente definido e cujo mau funcionamento é identificado. Os componentes de tipo A são, por exemplo, termorresistências e termopares.
  - Para componentes complexos do tipo B, o desempenho de falha de pelo menos um componente não está definido ou não está totalmente definido. Um componente de tipo B é, por exemplo, um circuito eletrônico contendo um microprocessador. O transmissor de temperatura T32.xS é definido como um componente de tipo B (veja a tabela 5).

Para calcular o valor SFF dos sensores e dos termopares que estão conectados ao transmissor de temperatura T32.xS, as taxas de falha dos sensores de temperatura devem ser subdivididas nas categorias (λS, λDD, λDU), levando em consideração o diagnóstico função do transmissor. Consequentemente, o valor SFF pode ser calculado de acordo com a seguinte fórmula:

$$SFF = \frac{\lambda_{DD} + \lambda_S}{\lambda_{DU} + \lambda_{DD} + \lambda_S}$$

Assim, os sensores de temperatura definidos como componentes do tipo A em uma arquitetura de canal único (HFT = 0) devem ser usados em sistemas instrumentados de segurança até SIL 2 e um SFF ≥ 60 % é mantido de acordo com a tabela 5. Para a mesma aplicação, para o transmissor de temperatura T32.xS como componente do tipo B, é necessário um SFF ≥ 90 %.

Tabela 5: Nível máximo de integridade de segurança de um componente dependente da tolerância de falha de hardware, da complexidade dos componentes e da fração de falha segura

SFF	Tolerância de falha do hardware					
	0		1		2	
	Tipo A	Tipo B	Tipo A	Tipo B	Tipo A	Tipo B
< 60 %	SIL 1	Não permitido	SIL 2	SIL 1	SIL 3	SIL 2
60 … < 90 %	SIL 2	SIL 1	SIL 3	SIL 2	SIL 4	SIL 3
90 … < 99 %	SIL 3	SIL 2	SIL 4	SIL 3	SIL 4	SIL 4
≥ 99 %	SIL 3	SIL 3	SIL 4	SIL 4	SIL 4	SIL 4

Somente se o valor SFF tanto do transmissor de temperatura como do sensor de temperatura atender ao limite especificado, são esses elementos permitidos para sistemas instrumentados de segurança com o SIL correspondente. Além disso, o valor PFD de toda a função de segurança deve satisfazer os requisitos da tabela 6.

Limitação do SIL de todo o sistema de segurança

A norma IEC 61508 especifica valores que limitam o nível de integridade de segurança de todo o sistema de segurança. Dependendo da frequência com que o sistema de segurança é exigido, dois valores característicos são diferenciados:

■ **PFH** (probabilidade de falha perigosa por hora)
Frequência média de uma falha perigosa da função de segurança para um modo de operação com taxas de demanda altas ou contínuas (alta demanda). Estes modos são particularmente relevantes para a construção de máquinas.

■ **PFDavg** (probabilidade de falha na demanda)
Probabilidade média de falha perigosa na demanda de uma função de segurança para um modo operacional com baixa taxa de demanda (baixa demanda).

Tproof indica o intervalo do teste de repetição. Após este intervalo, através de um teste adequado (teste de prova), o sistema é levado a um estado quase "tão novo" dentro da vida de serviço estipulada. Com este teste, falhas perigosas e indetectáveis também podem ser detectadas. Para um sensor de temperatura, é assegurado pela calibração regular que o valor medido ainda está dentro da exatidão necessária. Com isso, uma derivação inaceitavelmente alta também é excluída.

Com um intervalo de teste de prova de um ano (Tproof = 8.760 h), os seguintes valores de PFDavg resultam para uma termorresistência com ligação a 4 fios e um transmissor de temperatura modelo T32.xS conectado:
- Condição ambiental: baixo estresse
- Conexão entre o ponto de medição e o transmissor: Montagem direta
- Taxa de falha λDU = 16 FIT [3)]

$$PFD_{avg} = 0{,}5 * \lambda_{DU} * T_{proof}$$
$$= 0{,}5 * 16\ FIT * 8760\ h = 7{,}15 * 10^{-5}$$

Assim, esta combinação, em relação aos requisitos do valor PFDavg, é adequada para sistemas de segurança com maior nível de integridade de segurança para SIL 2, no entanto, devido à estrutura de um único canal (ver "Limitação do nível de integridade de segurança de um elemento") e o SFF, está limitado a SIL 2.

A fórmula descrita acima é derivada da IEC 61508. Supõe-se que o período de tempo de 8 horas, que é necessário para a renovação do sistema, é insignificantemente pequeno em comparação com o intervalo de teste de prova de 8.760 h.

O valor de PFDavg é quase que linear ao intervalo de teste de prova, Tproof. Quanto menor o intervalo de teste de prova, melhor será possível o valor de PFDavg. Da mesma forma, o intervalo de teste de prova pode ser aumentado se o valor PFDavg de todo o sistema for menor do que o valor limite permitido. Se o intervalo de teste de prova for reduzido para 0,5 anos, o valor de PFDavg é reduzido para metade, e se for estendido para 2 anos, é duplicado.

Quanto menor o valor PFDavg ou PFH, maior será o SIL possivel de todo o sistema. Na tabela 6, os valores de característica PFDavg ou PFH recebem um nível de integridade de segurança.

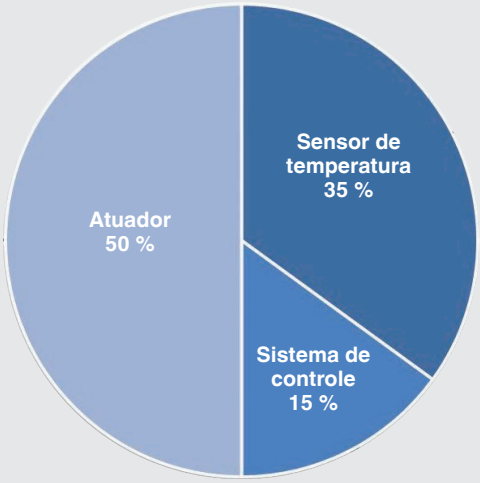
Tabela 6: Limitação do SIL do sistema de segurança pelos valores PFDavg e PFH

Nível de integridade de segurança (SIL)	Probabilidade média de uma falha perigosa na demanda de uma função de segurança (PFDavg)	Frequência média de uma falha perigosa por hora (PFH)
4	≥ 10^{-5} até < 10^{-4}	≥ 10^{-9} até < 10-8 h^{-1}
3	≥ 10^{-4} até < 10^{-3}	≥ 10^{-8} até < 10^{-7} h^{-1}
2	≥ 10^{-3} até < 10^{-2}	≥ 10^{-7} até < 10^{-6} h^{-1}
1	≥ 10^{-2} até < 10^{-1}	≥ 10^{-6} até < 10^{-5} h^{-1}

3) veja a página 12 "Literatura e fontes", manual de segurança "Informações sobre a segurança funcional do transmissor de temperatura modelo T32.xS"

Para o operador do sistema, é sempre o valor PFDavg de todo o sistema de segurança e não o valor de um único elemento relevante. Para avaliação, a seguinte distribuição dos valores de PFDavg para o sistema de segurança foi estabelecida como orientação:

Distribuição do sensor, controlador, atuador no valor PFD total do SIS



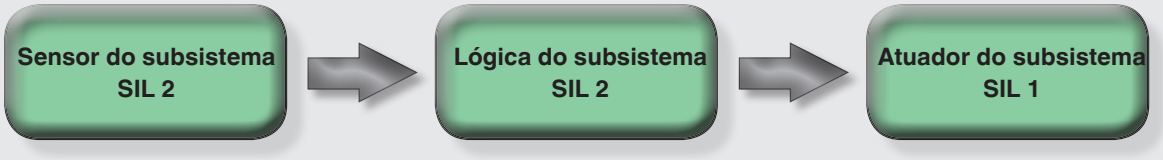
Uma distribuição diferente dos componentes pode ser especificada pelo operador da planta.

Se o sensor usar menos de 35% do valor máximo permitido de PFDavg do sistema de segurança, como para um sensor de temperatura com um transmissor de temperatura modelo T32.xS, o operador pode usar um controlador e um atuador com valores PFDavg correspondentemente inferiores.

Limitações estruturais

As características estruturais do sistema instrumentado de segurança podem limitar o SIL máximo alcançável. Em uma arquitetura de canal único, o SIL máximo é determinado pelo link mais fraco. No sistema de segurança ilustrado, os subsistemas "sensor" e "lógica" são adequados para o SIL 2, enquanto o subsistema "atuador" é adequado apenas para SIL 1. Por conseguinte, o sistema de segurança inteiro só pode atingir um máximo de SIL 1.

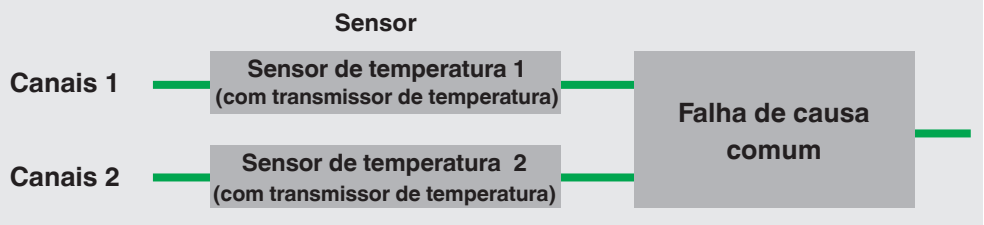
Componentes de um sistema relacionado à segurança



Sistemas redundantes

Se dois sensores de temperatura com o transmissor de temperatura modelo T32.xS forem montados em paralelo, devem ser consideradas falhas de causa comuns. Falhas de causa comuns podem ocorrer, por exemplo, quando condições ambientais ou interferências EMC influenciam vários canais simultaneamente. Essas falhas afetam todos os canais de um sistema redundante ao mesmo tempo.

Diagrama de bloco de confiabilidade: Sensor de temperatura em configuração redundante



Os sensores de temperatura da figura anterior representam, nesse caso, um sistema de arquitetura de dois canais (1oo2). Essa estrutura é referida como o sistema MooN. Um sistema MooN (M de N) consiste em N canais independentes, dos quais os canais M devem funcionar com segurança para que todo o sistema possa executar a função de segurança.

A ocorrência de falhas de causa comuns é menos provável se os dois sensores de temperatura com transmissores de temperatura usados forem tão diversos quanto possível em relação à construção, princípio de medição e software. Assim, por exemplo, uma termorresistência pode ser usada em um canal e um termopar pode ser usado no outro canal. Para a medição, um poço termométrico pode ser usado para uma termorresistência e outro para o termopar, ou um único poço termométrico pode ser usado para ambos. Ao usar um único poço termométrico, as falhas de causa comum são correspondentemente mais prováveis. Uma maior diversidade é adicionalmente alcançada quando os transmissores de temperatura utilizados são de diferentes fabricantes e diferem em sua construção, bem como em seu software.

Em particular, o transmissor de temperatura WIKA modelo T32.xS tem a vantagem de ser usado em sistemas redundantes homogêneos até SIL 3. Isso significa que um sensor de temperatura com um transmissor de temperatura modelo T32.xS está conectado em paralelo com um segundo instrumento com um transmissor estruturalmente idêntico. Em uma arquitetura de um único canal, o transmissor é adequado até SIL 2. Devido ao desenvolvimento completo e à certificação do transmissor de temperatura modelo T32.xS para todos os elementos conforme norma IEC 61508 (Desenvolvimento de Avaliação Completa), o transmissor também é adequado em um conjunto redundante homogêneo para aplicações SIL 3. Mesmo durante o desenvolvimento, as medidas para evitar falhas no software foram projetadas para uso em aplicações SIL 3. Assim, o transmissor de temperatura modelo T32.xS difere dos instrumentos comprovadamente testados que são apenas adequados para aplicações SIL com base no uso anterior.

Instrumentos de campo comprovadamente testados em uma arquitetura de dois canais conseguem, como máximo, o SIL do instrumento individual. Ao contrário do transmissor de temperatura modelo T32.xS, falhas sistemáticas nestes instrumentos não são prevenidas ou reduzidas em primeiro momento, ex: durante o desenvolvimento do instrumento.

Para explicar o efeito da falha de causa comum, é necessário um "fator β" para calcular o valor do PFD dos sistemas redundantes. O fator β refere-se à proporção de falhas de causa comum não detectadas. De acordo com a IEC 61508-6 e tendo em conta que o período de 8 h, que é necessário para a renovação do sistema, é insignificantemente pequeno em comparação com o intervalo de teste de prova de 8.760 h, o valor de PFD para uma estrutura de 1oo2 é calculado usando a seguinte fórmula simplificada:

$$PFD_{1oo2} = \frac{\lambda_{DU}^2 * T_{proof}^2}{3} + 0{,}5 * \lambda_{DU} * T_{proof} * \beta$$

Para determinar o fator β, primeiro as medidas devem ser definidas para que reduzam a ocorrência de falhas de causa comuns. Através da avaliação de engenharia, deve ser definido, em cooperação com a WIKA, a medida em que cada medida reduz a ocorrência de falhas de causas comuns.

Resumo das recomendações

Para o melhor design possível de um ponto de medição de temperatura para aplicações relacionadas à segurança, os requisitos do capítulo "Requisitos para um sistema de segurança" devem ser seguidos.

Em aplicações de segurança, é recomendado que o transmissor de temperatura modelo T32.xS (versões para montagem em cabeçote ou trilho) seja usado em conjunto com uma termorresistência com ligação a 4 fios ou com um termopar. Através das extensas características de diagnóstico do T32.xS e os benefícios de uma ligação a 3 fios, é garantida uma alta segurança na medição de temperatura.

Para proteger o elemento de medição do meio do processo e para permitir uma calibração rápida e fácil do sensor de temperatura, devem ser utilizados acessórios de proteção com elementos de medição intercambiáveis. É importante prestar atenção especial ao design adequado do poço de proteção de acordo com os requisitos do processo.

Literatura e fontes

1.) IEC 61508:2010:
Segurança funcional relacionada à sistemas de segurança elétrica /eletrônica/eletrônica programável
Beuth Verlag GmbH, 10772 Berlin

2.) Exida:
Manual de Confiabilidade do equipamento de segurança - 3 Edição, 2012, exida.com L.L.C.

3.) WIKA Alexander Wiegand SE & Co. KG:
Manual de Segurança “Informações sobre segurança funcional para transmissor de temperatura modelo T32.xS” (revisão de firmware 2.2.3)

Abreviações e definições

Abreviações	Definição
Montagem direta	O transmissor de temperatura é localizado/montado no cabeçote de ligação do sensor de temperatura.
DC	Cobertura diagnóstica
Cabo de ligação	O transmissor de temperatura é localizado fora do cabeçote de conexão do sensor de temperatura e está localizado, por exemplo, em um gabinete distante do ponto de medição (montado remotamente).
FIT	Falhas no tempo
HFT	Tolerância de Falha de Hardware
Alto estresse	Aplicações com vibração (≥ 67 % da máxima resistência do sensor de temperatura
Baixo estresse	Baixa vibração (< 67 % da máxima resistência do sensor de temperatura)
PFD_{avg}	Probabilidade média de uma falha perigosa na demanda da função de segurança
PFH	Frequência média de uma falha perigosa da função de segurança
RTD	“**R**esistance **t**emperature **d**etector”; Termorresistência
SFF	Fração de falhas seguras de um elemento de hardware
SIS	Safety Instrumented System Sistema Instrumentado de Segurança
TC	Termopar
TR	“**T**emperature **R**esistance”; Termorresistência

Impacto da reavaliação do modelo de transmissor de temperatura T32.xS (ver. de firmware 2.2.3) sobre os valores de característica relevantes para a segurança

No âmbito da reavaliação, não foram realizadas mudanças relacionadas à segurança no transmissor de temperatura. A cobertura diagnóstica do transmissor permanece inalterada. Somente a nova abordagem de avaliação levou a uma mudança nos valores de características relevantes para a segurança.

Nova edição da norma IEC 61508
Desde a avaliação inicial do transmissor de temperatura modelo T32.xS, a norma base para segurança funcional, IEC 61508 "Segurança funcional de sistemas elétricos/ eletrônicos programáveis relacionados à segurança" foi atualizado para a revisão IEC 61508: 2010. Da revisão de firmware 2.2.3, o T32.xS será avaliado em relação a esta edição do padrão.

Taxas de falha atualizadas
Nesse contexto, o FMEDA (Modos de Falha, Efeitos e Análise de Diagnóstico) também foi repetido com taxas de falha de componentes atuais. Os cálculos foram baseados em taxas de falha de componentes de acordo com SN29500. Para as termorresistências e os termopares conectados ao transmissor de temperatura, foram utilizadas as taxas de falha determinadas pela exida.com LLC.

Análise elementar do subsistema "sensor"
Com a introdução do termo "elemento" na seção 3.4.5 da IEC 61508- 4: 2010, a interconexão do transmissor de temperatura e termômetro elétrico como um subsistema "sensor" foi considerada e avaliada da seguinte forma:

Elemento 1	**Elemento 2**
Termômetro elétrico sem transmissor (termopar ou temorresistência) Tipo A / SFF ≥ 60 % para HFT = 0 e SIL 2	Transmissor de temperatura modelo T32.xS (sem termopar ou temorresistência) Tipo B / SFF ≥ 90 % para HFT = 0 e SIL 2

Essa consideração separada afeta a avaliação do valor SFF. Por exemplo, o valor requerido de SIL 2 SFF para termopares ou termorresistência cai para 60 %.

Taxas de falha específicas da aplicação
Com a reavaliação do T32.xS, as taxas de falha são definidas especificamente para o aplicativo, dependendo dos níveis de vibração no ponto de instalação do termômetro elétrico e dependendo da conexão do termômetro ao transmissor. Além disso, as taxas de falha para o transmissor de temperatura "autônomo" são calculadas para diferentes configurações.

Melhoria nas taxas de falha
As taxas de falha do transmissor T32.xS com termopar ou termorresistências conectados, mostraram uma tendência de melhoria. Em particular, para as condições de "baixo estresse, acoplamento fechado", a taxa de falha para falhas perigosas e não detectáveis diminuiu.

Efeitos no valor PFDavg
Especialmente para a condição de aplicação "baixo estresse, acoplamento fechado", o valor PFDavg melhorou. Isso permite que o usuário, se necessário, use subsistemas de lógica ou de atuação com valores PFDavg correspondentemente maiores no sistema instrumentado de segurança ou para estender o intervalo de teste de prova.

07/2018 PT based on 10/2014 GB

WIKA do Brasil Ind. e Com. Ltda.
Av. Úrsula Wiegand, 03
18560-000 Iperó - SP/Brasil
Tel. +55 15 3459-9700
Fax +55 15 3266-1196
vendas@wika.com.br
www.wika.com.br