Sistemas Instrumentados de Segurança (SIS)

Autor: Elisio Carvalho Silva

Data: 13/01/2012

Introdução

Os sistemas instrumentados de segurança (SIS) são utilizados para permitir uma maior segurança num equipamento ou sistema. Eles farão parte da camada de proteção para evitar que o equipamento ou sistema culmine num evento acidental devido a sua operação. Quanto melhores projetados e mantidos mais eficazes eles serão em prevenir acidente.

Para identificar e definir um SIS em um determinado equipamento ou processo é necessário efetuar análise de risco, e daí fazer uma análise das camadas de proteção para saber se há camadas suficientes para evitar um acidente e, se não houver, quanto de camada será necessária para manter o equipamento ou sistema em condições seguras conforme os padrões legais ou da empresa.

Variáveis que compõem na determinação de um SIS

As análises de risco e de camadas de proteção devem ser realizadas por um grupo multidisciplinar com o propósito de identificar os riscos e camadas necessários para prevenir um acidente. Quanto maior o risco, maior deverá ser a disponibilidade do SIS, ou seja, ficará mais tempo operando adequadamente para atuar de forma segura. Inversamente, pode-se dizer que será menor a sua probabilidade de falha em demanda (PFD). No intuito de atingir a disponibilidade adequada, o grupo de análise deve ficar atento em relação aos seguintes tópicos:

- Falhas randômicas e sistêmicas (λ e λ^{DF});
- Intervalo de teste (T);
- Causas comuns de falha (fator β);
- Tempo médio de recuperação de um canal de SIS após apresentar problemas (MTTR);
- Cobertura de detecção de falhas (C^{D});
- Fração de falhas seguras (SFF); e
- Tolerância de falhas do hardware (HFT).

Falhas randômicas

As falhas randômicas (λ) serão consideradas constantes no tempo e poderão ser encontradas em bancos de dados, informações do fabricante ou conforme histórico da unidade industrial. As falhas para o cálculo da PFD médio (PFDavg) deverão ser as falhas perigosas não detectadas (λ^{DU}). No entanto, as falhas perigosas detectadas (λ^{DD}), aquelas que, embora sejam visíveis, também deverão ser consideradas para o cálculo da PFDavg. As falhas seguras não deverão entrar nos cálculos porque quando elas ocorrem, deixam o processo em um modo seguro, portanto não permitirão eventos acidentais. Veja na Tabela 1 fórmula de cálculo da PFDavg considerando apenas λ^{DU} e o intervalo de teste T.

Tabela 1 – Cálculo PFD para diversas arquiteturas
Fonte: Smith

Number of units, n	Number required to operate, m = 1	m = 2	m = 3	m = 4
1	$\lambda T/2$			
2	$\lambda^2T^2/3$	λT		
3	$\lambda^3T^3/4$	λ^2T^2	$3\lambda T/2$	
4	$\lambda^4T^4/5$	λ^3T^3	$2\lambda^2T^2$	$2\lambda T$

Falhas sistêmicas

As falhas sistêmicas (λ^{DF}) são mais difíceis de serem determinadas, uma vez que estão muito relacionadas às falhas de gestão, tais como: falha de projeto, falha de manutenção, erro na avaliação de risco, erro na especificação, erro na instalação e comissionamento, erro no gerenciamento de mudança, etc. as quais podem ser minimizadas por meio de um sistema de gestão baseado na IEC 61511 ou ISA–84.01.

Intervalo de teste

O intervalo de teste deve ser definido conforme as boas práticas de engenharia, recomendações do fabricante, procedimentos internos da empresa, histórico de operação, restrições operacionais e necessidade da redução do risco. Importante salientar que o intervalo de teste tem uma contribuição importante na composição do cálculo da PFDavg do SIS e, consequentemente, na capacidade de prevenir o evento acidental. Por isso, é fundamental fazer o balanço de todos os fatores a ele relacionado.

Causas comuns de falha

As causas comuns de falha (CCF – fator β) incluem eventos randômicos ou sistêmicos que provocam falhas simultâneas em equipamentos múltiplos em sistemas redundantes (no caso

de SIS, arquitetura com votação diferente de 1oo1). Alguns autores consideram as seguintes situações como causas comuns de falha:

- Falha de calibração de sensores;
- Obstrução de tomadas únicas de sensores redundantes;
- Manutenção incorreta ou falta de manutenção;
- Especificação errada;
- Bypass indevido;
- Estresse de componentes devido a temperatura, corrosividade do meio, etc.

O projetista pode utilizar as Tabelas D.1 a D.5 do anexo D da IEC 61508 parte 6 para estimar o valor de β. Observe que as tabelas são aplicadas apenas para hardware, não incluindo software por ser mais difícil de modelar falhas sistêmicas.

Tempo médio de recuperação de um canal de SIS após apresentar problemas (MTTR)

O MTTR é importante porque poderá ocorrer uma segunda falha não detectada num segundo canal enquanto o primeiro está em manutenção devido a uma falha detectada, conforme mostra o segundo termo da Equação 1. Por isso, é fundamental que a manutenção seja mais breve possível para que o MTTR seja mínimo e tenha pouca influência na PFDavg do SIS. Se o tempo de manutenção for longo, a probabilidade de falha do SIS aumentará uma vez que a redundância do sistema reduziu. Em geral, esse termo é desprezível porque o MTTR é muito pequeno. Veja Equação 1 para uma configuração 1oo2:

$$\mathrm{PFD}_{\mathrm{avg}} = \left[\left((1-\beta)\times\lambda^{DU}\right)^2 \times \frac{TI^2}{3}\right] + \left[(1-\beta)\times\lambda^{DU}\times\lambda^{DD}\times MTTR\times TI\right] + \left[\beta\times\lambda^{DU}\times\frac{TI}{2}\right] + \left[\lambda_F^D\times\frac{TI}{2}\right]$$

Equação 1 – cálculo da PFDavg para configuração 1oo2
Fonte- ISA-TR84.00.02-2002 - Part 2

Cobertura de detecção de falhas

A cobertura de detecção de falha ajudará a melhorar a PFDavg de um SIS porque reduzirá as falhas não detectadas. Isso significa que os componentes do SIS terão a capacidade de detectar algumas falhas perigosas e colocar o equipamento ou sistema no modo seguro. Lembre-se que para o cálculo da PFDavg as falhas perigosas não detectadas têm uma maior influência no resultado.

$\lambda^{DD}=C^{D}*\lambda^{D}$

$\lambda^{DU}=(1-C^{D})*\lambda^{D}$ onde:

λ^{DD} = falha perigosa detectada

λ^{DU} = falha perigosa não detectada
C^D = fator de cobertura de detecção de falha perigosa
λ^D = falha perigosa

Observe que quanto maior for o C^D menor será a falha perigosa não detectada. Isso significa que à proporção que aumenta C^D, poderá economizar em outras ações relacionadas ao SIS, por exemplo, poderá aumentar o intervalo de teste. C^D é sempre um valor entre 0 e 1.

Fração de falhas seguras (SFF)

As falhas seguras detectáveis (λ^{SD}) e não detectáveis (λ^{SU}) levam a uma parada segura do processo. A falha perigosa detectável pode levar a uma condição segura por ação humana, ou seja, ao falhar haverá informação que está em falha, e o ser humano atuará para colocar o processo em condição segura, assim como, providenciará manutenção o mais rápido possível para o sistema em falha. Porém, a falha perigosa não detectável não proporciona uma parada segura e nem informação que o SIS está em falha. Daí a necessidade de saber qual essa fração de falha, conforme mostra a equação abaixo, para ajudar na determinação do nível de integridade de segurança (SIL) do SIS.

$$SFF=\lambda^{SD}+\lambda^{SU}+\lambda^{DD}/\lambda^{SD}+\lambda^{SU}+\lambda^{DD}+\lambda^{DU}$$

Quanto maior o SFF maior será o SIL como mostra as Tabelas 2 e 3, que coincidem com a numeração da tabela da IEC-61508-2. O SFF está representado na coluna *"safe failure fraction of an element"*.

Table 2 – Maximum allowable safety integrity level for a safety function carried out by a type A safety-related element or subsystem

Safe failure fraction of an element	Hardware fault tolerance		
	0	1	2
< 60 %	SIL 1	SIL 2	SIL 3
60 % – < 90 %	SIL 2	SIL 3	SIL 4
90 % – < 99 %	SIL 3	SIL 4	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4

Table 3 – Maximum allowable safety integrity level for a safety function carried out by a type B safety-related element or subsystem

Safe failure fraction of an element	Hardware fault tolerance		
	0	1	2
<60 %	Not Allowed	SIL 1	SIL 2
60 % – <90 %	SIL 1	SIL 2	SIL 3
90 % – <99 %	SIL 2	SIL 3	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4

As duas tabelas são para funções de segurança diferentes:

- Tabela 2 para funções de segurança tipo A: *relays*, solenóides, *boosters* pneumáticos, válvulas. Para esses equipamentos os modos de falha são bem definidos.
- Tabela 3 para funções de segurança tipo B, ou seja, para qualquer produto inteligente com um microprocessador ou com circuito de aplicação integrado específico complexo: sensores inteligentes, sistemas eletrônicos de controle. Esses equipamentos têm projeto complexo e pouca história de falhas o que pode levar a falhas sistêmicas.

Tolerância de falhas do hardware (HFT)

A tolerância de falha do hardware permite que um sistema ou equipamento continue operando de forma segura mesmo ocorrendo falhas de um ou mais *hardware* ou *software.* Por exemplo, uma arquitetura com votação 1oo2 tem HFT de 1, ou seja, permite que haja uma falha de um canal e o processo ou equipamento continue operando de forma segura. Já uma arquitetura de 1oo3 possui HFT de 2. Observe que quanto maior o HFT, maior será o SIL. O HFT está representado na coluna de *"hardware fault tolerance"* das Tabelas 2 e 3. Com o SFF, HFT e o tipo do equipamento será possível definir rapidamente qual o SIL.

Outra maneira de calcular o SIL é por meio de fórmulas simplificadas tal como mostrado na Equação 1. Calcula-se a PFDavg de cada elemento do SIS e daí soma as PFDs e então encontrará a PFDavg total do SIS. Com essa PFDavg total vai na Tabela 4 e define o SIL.

Safety integrity level (SIL)	Average probability of a dangerous failure on demand of the safety function (PFD_{avg})
4	$\geq 10^{-5}$ to $< 10^{-4}$
3	$\geq 10^{-4}$ to $< 10^{-3}$
2	$\geq 10^{-3}$ to $< 10^{-2}$
1	$\geq 10^{-2}$ to $< 10^{-1}$

Tabela 4- Cálculo do SIL e RRF
Fonte- IEC 61508-1

Também pode-se calcular o SIL por meio de árvores das falhas e da análise de Markov.

Conclusão

O projeto de um sistema instrumentado de segurança é fundamental para garantir a sua eficácia em relação à prevenção de acidente. Do contrário, não se poderá garantir que a probabilidade de falha em demanda estará compatível com o nível de risco encontrado nas análises e haverá uma pseudo-proteção o que pode se transformar num acidente e causar grandes prejuízos materiais, ambientais e/ou humanos para a empresa.

Além do projeto adequado, é preciso mantê-lo íntegro por meio de inspeções e testes periódicos a fim de garantir que ele funcionará bem por todo o seu ciclo de vida. Adicionalmente, deve-se efetuar auditorias periódicas com o propósito de verificar se todos os requisitos de segurança do ciclo de vida do SIS estão a ser cumpridos conforme proposto pela IEC 61508 ou IEC 61511/ISA84.01. Importante lembrar que a IEC 61511 e ISA 84.01 foram editadas especificamente para processos industriais.

Precisando de ajuda, entre em contato com a ECS Consultorias.

Referências

CCPS/AIChE. **Guidelines for Safe and Reliable Instrumented Protective Systems.** New Jersey: John Wiley & Sons, 2007.

IEC 61511. Functional Safety – **Safety Instrumented Systems for the process Industry Sector, Partes 1-3**. Geneva 20, Switzerland, 2003

IEC 61508. **Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems, Partes 1-7**. Management Centre: Avenue Marnix 17, B - 1000 Brussels: BSI Standards Publication, 2010.

ISA-TR84.00.02. **Safety Instrumented Functions (SIF)-Safety Integrity Level (SIL) Evaluation Techniques Part 2: Determining the SIL of a SIF via Simplified Equations**. Research Triangle Park, North Carolina 27709, 2002.

SMITH, David. **Reliability, Maintainability and Risk – Practical Methods for Engineers**. Butterworth-Heinemann: Elsevier Ltd, 8th edition, 2011.