Revista Gestão Industrial
ISSN: 1808-0448
http://periodicos.utfpr.edu.br/revistagi

Análise da influência técnica da arquitetura, frequência de testes e tempo médio entre reparo na disponibilidade de um *high integrity pressure protection system*

João Paulo Costa e Silva Nunes
jpaulo.nunes@terra.com.br
Universidade Federal do Rio Grande do Norte (UFRN), Natal, Rio Grande do Norte, Brasil

Leandro de Medeiros Dantas
mdantas.leandro@gmail.com
Universidade Federal do Rio Grande do Norte (UFRN), Natal, Rio Grande do Norte, Brasil

Lucas Araújo dos Santos
araujo.engprod@gmail.com
Universidade Federal do Rio Grande do Norte (UFRN), Natal, Rio Grande do Norte, Brasil

Priscila Valessa Pinheiro Gomes
priscila_valessa@hotmail.com
Universidade Federal do Rio Grande do Norte (UFRN), Natal, Rio Grande do Norte, Brasil

Tiago de Oliveira Barreto
b.02_tiagooliveira@hotmail.com
Universidade Federal do Rio Grande do Norte (UFRN), Natal, Rio Grande do Norte, Brasil

Herbert Ricardo Garcia Viana
hebertviana@hotmail.com
Universidade Federal do Rio Grande do Norte (UFRN), Natal, Rio Grande do Norte, Brasil

RESUMO

Diante da contribuição dos sistemas Instrumentados de Segurança (SIS), em especial os sistemas de alta integridade para proteção à alta pressão (HIPPS), permitindo que diferentes processos sejam levados a níveis cada vez mais seguros, o presente estudo buscou analisar a disponibilidade de um HIPPS em diferentes configurações por meio da influência da arquitetura dos seus componentes, frequências de testes e tempo médio entre os reparos. Para tanto, nos procedimentos metodológicos, foi definido um modelo base de arquitetura para posteriormente serem analisadas diferentes propostas. Tais análises foram subsidiadas pela identificação das variáveis no manual de dados "*Reliability data for Safety Instrumented Systems*" e modelagens matemáticas realizadas por meio de equações propostas no manual do método PDS "*Reliability Prediction Method for Safety Instrumented Systems* PDS *Method Handbook*, 2010 *Edition*", podendo, assim, realizar análises comparativas de tais influências. Como achados da pesquisa, está a verificação de que, de acordo com os cenários estudados, as medidas de tempo médio para reparo e frequência de testes se mostraram mais representativas para a indisponibilidade do sistema do que as variações de arranjos. E, ainda, que o aumento da frequência de teste fomenta a elevação do PFD de falhas independentes; assim como o HIPPs na filosofia degradada, em geral, apresentou uma contribuição muito baixa, sendo irrisória para a análise final da disponibilidade do sistema. Entretanto, quando elevado o MTTR, tais falhas mostram suas importâncias para tais funções. Por fim, como suposto por Marszal e Scharpf (2002), confirmou-se que acionamentos espúrios são mais relevantes em arquiteturas redundantes, independente de tempos de testes e tempos entre reparos.

PALAVRAS-CHAVE: SIS. HIPPS. Probabilidade de Falha. SIL.

INTRODUÇÃO

A demanda por sistemas cada vez mais seguros no controle de processos encontra-se cada vez mais crescente. Nessa linha, há a proposta do Sistema Instrumentado de Segurança (SIS), que mostra sua importância na detecção de eventos perigosos e prevenção de acidentes. Estes são instalados com o objetivo de executar uma função instrumentada de segurança, permitindo que o processo seja levado a níveis cada vez mais seguros, e por esse motivo são utilizados em diversos setores industriais (OUACHE; KABIR, 2016; SIMON et al., 2019).

Os SIS tornaram-se cada vez mais objeto de estudos devido sua contribuição para diversas aplicações técnicas, tendo o papel de apresentar função relacionada ao monitoramento e manutenção da segurança de qualquer equipamento sob seu controle. Sistemas de detecção de incêndio e gás, de desligamento de processos e de emergência são exemplos de SIS utilizados para evitar que condições operacionais anormais se transformem em um acidente (HAUGE et al., 2010).

Nesse contexto de importância, existem estudos que buscam mitigar os riscos associados a esses sistemas por meio da aplicação de métodos quantitativos que permitem mapear a probabilidade de ocorrência dos eventos pessoais, ambientais ou patrimoniais. Esses métodos permitem a classificação do nível de integridade de segurança (SIL) de um SIS, um indicador que mensura o nível tolerável de indisponibilidade de um sistema (LANGERON et al., 2008). O SIL indicará a probabilidade mínima de o equipamento realizar com sucesso o que foi projetado para fazer quando demandado, e seu projeto precisa compreender a probabilidade potencial de um evento indesejado, bem como as possíveis consequências desse evento (MARSZAL; SCHARPF, 2002).

O projeto de um SIS consiste no envolvimento de três subsistemas principais, sendo eles: sensores, placa lógica e elementos finais, e envolve a obtenção de níveis mínimos de integridade de segurança, conforme exigido pela norma internacional IEC 61508. Tais níveis serão atingidos com a redução da probabilidade de falha na demanda (PFD) do SIS, em conformidade com outros fatores de segurança. A tolerância às falhas, isto é, sua capacidade de manter-se contínuo sem falhas, geralmente é alcançada com as redundâncias de componentes no sistema, sendo as formas mais básicas de redundância a de hardware e software (TORRES-ECHEVERRI´A, MARTORELL e THOMPSON 2009; XIE et al., 2019).

Na indústria de petróleo, devido às grandes pressões e vazões nas tubulações, dutos e válvulas responsáveis pelo transporte da matéria prima aos locais de armazenamento do petróleo, a utilização de HIPPS (sistema de proteção de pressão de alta integridade) é amplamente aceita como um sistema de proteção robusto. Ele é capaz de proteger suas instalações, seja uma plataforma, balsa ou refinarias, contra o aumento repentino de pressão que pode causar ruptura da tubulação, cessando o fluxo antes de exceder a pressão máxima, evitando assim, além de um possível desastre ambiental, uma grande perda econômica para a indústria (AMINI; SABER, 2015; WU et al., 2018).

Nesse sentido, tendo em vista a necessidade de explorar o cenário de sistemas instrumentados de segurança, o objetivo deste trabalho consiste em

analisar a disponibilidade em diferentes configurações a de um HIPPS por meio da influência da arquitetura dos seus componentes, frequências de testes e tempo médio entre os reparos.

REVISÃO DA LITERATURA

SISTEMAS DE ALTA INTEGRIDADE PARA PROTEÇÃO À ALTA PRESSÃO (HIPPS) E NÍVEL DE INTEGRIDADE DE SEGURANÇA (SIL)

Um sistema de alta integridade para proteção à pressão é uma aplicação específica de um SIS, projetado de acordo com normas específicas, por exemplo, a IEC 61508, IEC 61551 e API 17O. Sua função é proteger um sistema de escoamento de fluidos contra eventos de sobre pressão por meio do fechamento da fonte de pressão (BAI; BAI, 2010).

O HIPPS é projetado como um sistema autônomo que detecta o aumento de pressão em tubulações ou dutos, permitindo o fechamento rápido de uma ou mais válvulas de bloqueio antes que a pressão aumente excessivamente, causando danos ao sistema. Tal função requer um sistema altamente confiável, disponível e de veloz atuação. Seus principais componentes são: (i) transmissões de pressão; (ii) controladores lógico-programáveis; (iii) válvulas solenoides e (iv) válvulas de bloqueio (API 17O, 2014).

No intuito de garantir disponibilidade e prevenir fechamentos espúrios e indesejados do HIPPS, usualmente mais de um transmissor de pressão é utilizando no sistema, por exemplo, em lógica de votação 2oo3, ou seja, em uma configuração tripla de transmissores o evento de sobre pressão só é positivamente confirmado caso ao menos dois transmissores acusem a sobre pressão.

No que tange ao padrão de funcionamento, o controlador lógico-programável monitora os transmissores e envia sinais elétricos para as válvulas solenoides que, por sua vez, regulam o circuito hidráulico pressurizado que comanda a abertura e o fechamento das válvulas de bloqueio. O sistema de detecção e atuação de um HIPPS é essencialmente eletromecânico e deve ser independente de qualquer outro sistema que exista no local onde ele será instalado (BAI; BAI, 2010).

Tipicamente, os componentes de um HIPPS devem ser certificados com relação à taxa de falhas, para que garantam determinado nível de integridade de segurança (SIL). A partir das taxas de falhas é possível calcular a probabilidade de falha na demanda (PFD) de cada componente do HIPPS, bem como do sistema como um todo. Com o PFD do sistema é possível classificar o HIPPS com relação ao SIL.

O SIL é uma medida da confiança com a qual se espera que um sistema desempenhe sua função de segurança (DUTUIT et al., 2008). Tipicamente, este é discretizado em quatro níveis, de 1 a 4, correspondendo ao grau de disponibilidade média referente às falhas perigosas de uma função instrumentada de segurança (SIF). Alternativamente, cada SIL representa uma faixa de fatores de redução de risco que um SIS, no caso um HIPPS, pode prover a

um determinado processo. A figura 1 apresenta os quatro níveis de integridade de segurança associados às respectivas faixas de PFD, disponibilidade e fator de redução de risco:

Figura 1 - Níveis de Integridade de Segurança de um SIS

Níveis de Integridade de Segurança (SIL)			
Nível de SIL	Probabilidade de Falha na Demanda (PFD)	Disponibilidade (1-PFD)	Fator Redutor de Risco
SIL 1	0,1 - 0,01	0,90-0,99	10-100
SIL 2	0,01-0,001	0,99-0,999	100-1000
SIL 3	0,001 - 0,0001	0,999-0,9999	1000-10000
SIL 4	0,0001-0,00001	0,9999-0,99999	10000-100000

Fonte: API 17O (2014)

MÉTODO PDS

Conforme exposto na literatura, existem diferentes métodos e normas que visam projetar, implantar e manter sistemas relacionados à segurança. A norma IEC 61508 pode ser considerada como o principal padrão internacional para especificação e projeto de um sistema instrumentado de segurança (SIMON; MECHRI; CAPIZZI, 2019). Esta norma possui variações para indústria de processos (IEC 61511), máquinas (IEC 62061), plantas nucleares (IEC 61513) e linhas ferroviárias (EN 50126, EN 50128 e EN 50129), destinando-se para cada integrante das respectivas áreas.

Em relação aos métodos, o método PDS será objeto de estudo deste artigo e trata-se de uma evolução quanto às normas IEC 61508 e IEC 61511, estando alinhado aos principais princípios defendidos por estas, entretanto, oferecendo abordagem mais eficaz e prática para implementação dos aspectos quantitativos. Utilizado para quantificação da indisponibilidade de segurança e perda de produção de sistemas instrumentados de segurança, se diferencia em relação às normas pela interpretação distinta acerca da classificação de falhas, além de abordagem alternativa à modelagem de falhas comuns e incorporação de falhas, segundo Hauge et al. (2010).

Desenvolvido por especialistas das áreas de confiabilidade e segurança, dispõe de uma abordagem mais crítica e realista, considerando todas as principais categorias de causas de falhas, auto testes automáticos, teste funcional, falhas sistêmicas, função de segurança completa e redundâncias, como os principais fatores que afetam a confiabilidade durante a operação de um sistema. Ainda segundo Hauge et al. (2010), as aplicações do método que mais se destacam são encontradas em sistemas de segurança na indústria de petróleo e gás *offshore* e *onshore*.

Classificação de falhas

Os SIS controlam os principais riscos nas instalações de processos, e cada falha ocorrida na realização de uma atividade por determinado equipamento ou sistema pode ser categorizada de acordo com sua causa, podendo ser falhas aleatórias ou sistemáticas. Para que seja desenvolvido um SIS confiável,

garantindo contínua confiabilidade, é vital que ambas as falhas sejam controladas (CLARKE, 2012).

Falhas aleatórias

Caracterizadas como falhas físicas, as falhas aleatórias são causadas por estresse excessivo no dispositivo e também por sua degradação natural, podendo acontecer a qualquer momento durante a vida útil e sua ocorrência não segue um padrão, mas ocorre aleatoriamente no tempo. (SUMMERS e GENTILE, 2006). Caracteriza-se, ainda, por ser quase sempre permanente e atribuível a algum componente ou módulo específico (GOBLE e CHEDDIE, 2005).

A taxa de falhas aleatórias normalmente não pode ser reduzida e, em vez disso, o foco deve estar em sua detecção e manuseio. A manipulação de dados estatísticos e tratamentos podem ser aplicados a falhas aleatórias, portanto, os riscos associados à elas podem ser calculados (BASU, 2017).

Segundo Clarke (2012), atualmente, volta-se mais o foco para o controle de falhas sistemáticas do que aleatórias, em virtude de contínuas melhorias na confiabilidade e nos diagnósticos do hardware, responsáveis pela redução nas taxas de falhas aleatórias. Por outro lado, o aumento da complexidade do sistema está ocasionando mais oportunidades para falhas sistemáticas.

Falhas sistemáticas

As falhas sistemáticas ocorrem sempre que um conjunto de condições particulares é atendido e, portanto, repetível (ou seja, itens sujeitos ao mesmo conjunto de condições falharão consistentemente), sendo assim, aplicam-se tanto ao hardware quanto ao software (KRITZINGER, 2017). Este tipo de falha não impede que o sistema permaneça capaz de operar, no entanto, ele não consegue desempenhar a função desejada ou consegue desempenhar, porém de forma degradada.

Oriundas do erro humano em áreas como especificação, design, fabricação, programação, operação e manutenção, as falhas sistemáticas são mais difíceis de medir e controlar, sendo geralmente decorrentes de falhas em um sistema de gestão (CLARKE, 2012). Ainda segundo o autor, o controle de falhas sistemáticas precisa ser feito levando em consideração não apenas erros específicos, definíveis, mas também fatores intangíveis que criam condições sob as quais os erros são mais prováveis de ocorrer. Segundo Hauge et al. (2010), falhas sistemáticas são falhas dependentes que podem levar a falhas de causa comum em um sistema.

Cada dispositivo tem muitas oportunidades de erro sistemático, entretanto, conforme a complexidade da SIF aumenta, a probabilidade de detecção desses erros diminui. Como qualquer nova tecnologia, existe o potencial para muitas falhas desconhecidas ou ainda não identificadas. Devido à natureza complexa e não aleatória de falhas sistemáticas, é difícil prever ou analisá-las estatisticamente (SUMMERS; GENTILE, 2006).

Tipicamente, utiliza-se o fator Beta (β) para se contabilizar falhas de causas comuns (sistemáticas) em um sistema. Assume-se que certa fração das falhas

(igual a β) é de causa comum, ou seja, falhas estas que causarão a falha simultânea ou em curto período de tempo de todos os componentes redundantes de um SIS (HAUGE et al., 2010), fator este posteriormente analisado por Mechri, Simon e Ben Othman (2012) para avaliar sua relação com as probabilidades de falha na demanda (PFD).

Detecção de falhas

Existem diferentes tipos de modos de falha possíveis em um sistema instrumentado de segurança e, diante da possibilidade de serem desconhecidos e imprevisíveis, devem ser considerados diagnósticos adicionais para identificação destes. Uma das características do SIS é que as falhas são normalmente ocultas e, para que sejam detectadas e removidas em um sistema de segurança, é imprescindível a realização de testes (HAUGE et al., 2010).

As principais técnicas aplicadas para detectar falhas perigosas e melhorar a disponibilidade do SIS são os autotestes automáticos e os testes funcionais. Adicionalmente, é possível ocorrer a detecção de falhas durante as demandas de processo, na operação do sistema.

Auto testes Automáticos

Utilizados para identificar falhas perigosas que possam impedir o SIS de realizar as funções requeridas, são capazes de detectar falhas automaticamente sem exigir o desligamento do processo. Realizados manualmente e com mais frequência do que os testes funcionais, os auto testes automáticos ocorrem em intervalos de tempo que variam entre horas e segundos e detectam falhas essencialmente aleatórias de um componente ou módulo de um SIS (WU et al., 2018).

Os modos de falha típicos de um HIPPS que podem ser detectados pelos autotestes são perda ou deriva de sinal, sinal fora de faixa ou válvula final de bloqueio na posição errada (HAUGE et al., 2010). Ainda segundo estes autores, a fração de falhas detectadas pelo auto teste automático é chamada de cobertura de diagnóstico e quantifica o efeito destes. O efeito real no desempenho do sistema de uma falha detectada pelo auto teste automático dependerá da configuração do sistema e da ação tomada quando a falha do equipamento for detectada.

Testes Funcionais

São realizados para detectar falhas ocultas de um SIS que não foram reveladas por auto testes automáticos. Para Hauge et al. (2010, p. 17), o teste funcional é realizado manualmente em intervalos de tempo pré-definidos, visando testar os componentes envolvidos na execução da função instrumentada de segurança para identificação de falhas. O teste pode ser ainda completo, em que o objetivo é detectar todas as falhas detectáveis do SIS, ou parcial, em que se busca detectar apenas alguns modos de falha (ROUVROYE e WIEGERINCK, 2006).

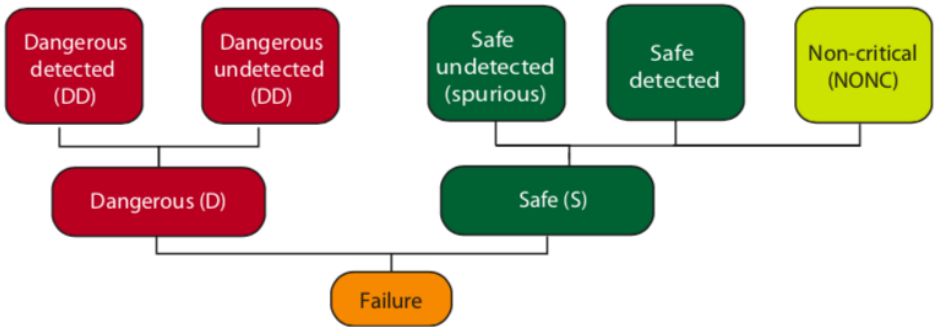
Normalmente, o teste funcional é considerado robusto, em que todas as falhas não detectadas são reveladas e reparadas durante o teste. Dessa forma, o SIS é restaurado em uma condição tão boa quanto nova (IEC 61508, 2010). Entretanto, em uma condição real, o teste funcional pode ser imperfeito por não ser capaz de revelar todos os tipos de falhas não detectadas, ou por ser realizado em condições diferentes de uma situação real de demanda (SIMON; MECHRI; CAPIZZI, 2019).

Ao não ser capaz de detectar integralmente as falhas e permitindo que algumas partes da função instrumentada de segurança não sejam testadas, o método PDS utiliza adição da probabilidade do teste de falhas independentes (PTIF) para atender essa demanda.

Modos de falha

Segundo Alizadeh e Sriramula (2018), os modos de falha dos SIS são categorizados em falhas seguras e falhas perigosas. Estes são subdivididos em outras duas categorias, aquelas que são detectáveis e não detectáveis. A Figura 2 mostra de forma sintética a relação entre os modos de falha.

Figura 2 - Modos de Falha



Fonte: Rausand (2014)

A falha denominada segura ocorre quando após uma demanda sobre um componente, o sistema mantém-se em segurança. Geralmente a ocorrência é gerada por demandas espúrias. Em nível de classificação, as falhas seguras são divididas em detectáveis e não detectáveis. As falhas seguras não detectáveis caracterizam-se por não serem detectadas por teste automático ou incidentalmente por pessoal e, portanto, resultam em uma demanda espúria do componente. Já na falha segura detectável, a falha espúria é detectada antecipadamente pelo teste automático ou incidentalmente por pessoal (JIN et al., 2015).

As falhas perigosas impedem que o SIS desempenhe sua função, ou seja, o componente não opera sob demanda. Da mesma forma, as falhas perigosas são divididas em detectadas e não detectadas. Na falha detectada, o sistema conseguirá identificar o problema de forma imediata. Já na não detectada, não ocorrerá a revelação até que um teste de prova (ou teste funcional) seja realizado ou até que ocorra uma demanda real pelo sistema (ALIZADEH; SRIRAMULA, 2018; SAL; NAIT-SAID; BOURARECHE, 2017).

As falhas seguras e perigosas são consideradas críticas no sentido de que elas afetam duas das principais funções de um HIPPS: (i) a capacidade de bloquear um fluxo sob demanda ou (ii) manter o sistema em produção quando este opera em condições seguras. As falhas seguras são usualmente reveladas instantaneamente quando ocorrem, enquanto as falhas perigosas permanecem "dormentes" e podem ser detectadas por testes funcionais ou durante demanda real (HAUGE et al., 2010).

É possível realizar uma quantificação dos grupos dos modos de falhas em duas grandes categorias. A primeira fração do modo de falha é denominada de falhas perigosas (D), que ocorre quando a demanda é comprometida. Esse grupo está dividido em não detectáveis (λDU) e detectáveis (λDD), como a nomenclatura sugere, serão casos em que a falha poderá ou não ser detectada. Da mesma forma, a segunda fração do modo de falha é denominada de falhas seguras (S) e estes também estão divididos em falhas seguras detectáveis e não detectáveis (AZIZPOUR; LUNDTEIGEN, 2019).

De acordo com Azizpour e Lundteigen (2019), para os processos que necessitam de sistemas de segurança, as falhas DU são categoricamente mais danosas, pois ficam ocultas até a realização de um teste de prova seja realizado. Até então, o sistema fica desprotegido, podendo acarretar futuramente consequências maiores.

Medidas de desempenho para perda de falha

Segundo o método PDS, existem três potenciais contribuintes para a perda de segurança de um SIS. Hauge et al. (2010) classifica-os em:

1) Indisponibilidade devido às falhas perigosas não detectáveis: Indisponibilidade causada por falhas que são detectadas apenas durante testes funcionais ou sobre demanda.
2) Indisponibilidade devido às falhas independentes de testes: Indisponibilidade causada por falhas perigosas ocultas que não são reveladas durante testes funcionais, mas apenas durante uma demanda real. Essas falhas são denominadas Falhas Independentes de Testes (TIF).
3) Indisponibilidade devido a tempo de inatividade conhecidos ou planejados: Essa indisponibilidade é causada por componentes retirados para reparo ou para teste/manutenção.

Nos tópicos seguintes serão abordados os conceitos dos precursores para a perda de segurança de um SIS. Como os conceitos são exclusivos do método PDS, buscou-se trazer as referências de acordo como é tratado no livro *Reability Prediction Method for Safety Instrumented System* do Hauge et al. (2010).

Probabilidade de Falha na Demanda (PFD)

Para realizar o atendimento da capacidade da meta de segurança de um SIS, o padrão IEC 61509 propõe a aplicação de dois métodos para identificação de falha na demanda: a Probabilidade de Falha na Demanda (PFD) para sistemas de

baixa demanda e a Probabilidade de Falha por Hora (PFH) para sistemas de alta demanda (Innal et al., 2014). Nesse artigo, será abordado apenas a aplicação em baixa demanda dado que é a abordagem mais abordada na literatura (DUTUIT et al., 2008; JIN et al., 2015; AZIZPOUR e LUNDTEIGEN, 2019), bem ser a situação operacional típica de um HIPPS que, por exercer uma SIF, apresenta baixa frequência de atuação. Com isso, na literatura, Azizpour e Lundteigen (2019) definem a PFD como a probabilidade média da incapacidade de um SIS para executar sua função de segurança quando demandado em baixas demandas.

Vale salientar que, conforme Marszal e Scharpf (2002) sugerem, a probabilidade de falha na demanda de um dispositivo depende, além da taxa de falhas perigosas e não detectáveis, de sua frequência de testes e reparos. O PFD de um dispositivo não testado torna-se maior à medida que o tempo aumenta, uma vez que as falhas tendem a não ser corrigidas. Para uma taxa de falha constante, a relação entre taxa de falhas e intervalo de teste é exponencial. Com essa relação é possível obtermos o PFD máximo. Todavia, o PFD médio se enquadra melhor no cenário, isso porque a demanda poderá ocorrer em qualquer momento durante o intervalo de um teste. Com isso, torna-se desnecessário aplicar a probabilidade de falha no teste completo.

Probabilidade de Falha Independente de Teste (PTIF)

É relevante abordar que, em condições reais, não se pode assumir categoricamente que a confiabilidade de um teste funcional estará livre de imperfeições, podendo estar sujeito a condições falhas. Com isso, algumas falhas perigosas poderão passar despercebidas pelo SIS, mesmo após um teste funcional. No método PDS, esse processo é atendido pela adição da probabilidade da falha independente de teste (PTIF) (HAUGE et al., 2010).

Nessa óptica, o mesmo autor define a Probabilidade de Falha Independente de Teste (PTIF), como a possibilidade de que um componente de um SIS não consiga executar sua função pretendida devido a uma falha (latente) não detectável pelo teste funcional.

Indisponibilidade por tempo de inatividade (DTU)

Hauge (2010) define a Indisponibilidade por tempo de Inatividade (DTU) como a não disponibilidade de um SIS causada pela retirada de um componente para reparo, teste ou manutenção. Nesse contexto, a DTU é composta por dois outros elementos, a Indisponibilidade por inatividade devido ao reparo de taxas de falhas perigosas (DTU_r) e Indisponibilidade por tempo de inatividade planejada (DTU_t). O primeiro elemento (DTU_r) resulta em um período conhecido em que estará indisponível, devido a falha perigosa. A duração média dependerá do tempo médio de reparo (MTTR), isto é, o tempo necessário desde o momento que foi identificada até a sua correção. Já o segundo elemento (DTU_t) gerará uma indisponibilidade por uma atividade planejada resultante de testes funcionais ou manutenção preventiva.

Uma contribuição relevante deixada pelo autor, Hauge et al. (2010), é que dependendo da filosofia operacional e da configuração da fábrica de processo e

do SIS, deve ser decidido se é relevante incluir apenas o DTU_r, apenas o DTU_t ou todo o DTU = DTU_r + DTU_t na mensuração geral da segurança contra perdas.

Indisponibilidade crítica de segurança (CSU)

No método PDS, de acordo com Hauge et al. (2010), os valores da indisponibilidade crítica de segurança (CSU) são usados para quantificar a perda de segurança. Nesse sentido, CSU é a probabilidade de que um componente ou o SIS irá falhar em executar automaticamente uma ação de segurança durante a ocorrência de um evento acidental e não é conhecido que o SIS está indisponível.

Nesse sentido, quando o tempo de inatividade é conhecido, a formulação é dada pela equação (1):

$$CSU = PFD + PTIF + DTU \quad (1)$$

O termo DTU poderá ser suprimido da equação quando o tempo de inatividade não for conhecido.

Taxa de Acionamento Espúrio (STR)

De acordo com Jin et al. (2015), a Taxa de Acionamento Espúrio (STR) poderá ocorrer em um componente quando um sistema de segurança for acometido por uma falha segura não detectada. Ela ocorre quando a falha não é ocasionada, mas há o alerta do sistema. Um exemplo disso, de acordo com o mesmo autor, é quando o detector de gás emite um alarme quando não há vazamento de gás; o sensor de nível exibe o nível alto de líquido enquanto o nível real do líquido está dentro da faixa normal.

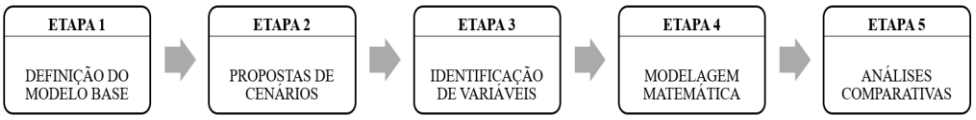
Além disso, segundo considerações de Hauge et al. (2010), existe uma relação direta entre o STR e a taxa de falha segura não-detectável (λ_{SU}). De forma mais ampla, essa mesma relação poderá ser relacionada com os casos em que exista redundância 1ooN.

Os autores Lundteigen, Rausand e Utne (2009) acrescentam que são experimentadas mais ativações espúrias quanto mais componentes redundantes houver nos sistemas, que devem ser balanceados com os efeitos positivos ocasionados por essas arquiteturas.

METODOLOGIA

O presente estudo trata-se de uma pesquisa aplicada de cunho descritivo, subsidiado por uma abordagem quali-quantitativa. Para tanto, no que se referem aos procedimentos utilizados, foram definidas cinco etapas de execução, como mostradas na Figura 3.

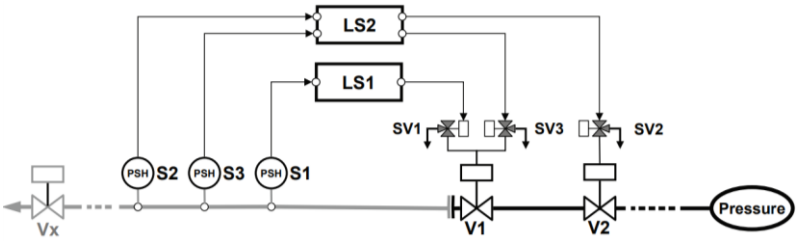
Figura 3 - Etapas do procedimento de pesquisa



Fonte: Autores (2019)

Na Etapa 1 - definição do modelo-base - foi selecionado uma arquitetura simples de um sistema HIPPs de proteção a alta pressão (Figura 4), no qual estão identificados transmissores de pressão (PSH), solucionador lógico (LS), válvulas solenoides (SV) e válvulas de bloqueio (V).

Figura 4 - Arranjo do modelo base



Fonte: ISO (2016)

Etapa 2 - Uma vez identificado o modelo-base, diferentes cenários foram modelados com redundâncias e/ou redução de componentes e variação das lógicas de votação, totalizando 13 (treze) diferentes cenários, sumarizados na tabela 1.

Tabela 1 - Cenários estudados

CENÁRIO	ARQUITETURA	CENÁRIO	ARQUITETURA
1	PT2oo3+CLP1oo2+SOL1oo2+SDV1oo2	8	PT1oo2+CLP1oo3+SOL1oo2+SDV1oo2
2	PT2oo3+CLP1oo3+SOL1oo2+SDV1oo2	9	PT1oo2+CLP1oo2+SOL1oo3+SDV1oo3
3	PT2oo3+CLP1oo2+SOL1oo3+SDV1oo3	10	PT2oo3+CLP1oo1+SOL1oo2+SDV1oo2
4	PT1oo3+CLP1oo2+SOL1oo2+SDV1oo2	11	PT2oo3+CLP1oo1+SOL1oo1+SDV1oo1
5	PT1oo3+CLP1oo3+SOL1oo2+SDV1oo2	12	PT1oo2+CLP1oo1+SOL1oo2+SDV1oo2
6	PT1oo3+CLP1oo2+SOL1oo3+SDV1oo3	13	PT1oo2+CLP1oo1+SOL1oo1+SDV1oo1
7	PT1oo2+CLP1oo2+SOL1oo2+SDV1oo2		

Fonte: Autores (2019)

É válido ressaltar que nas arquiteturas supracitadas os componentes: transmissores de pressão (PT), solucionadores lógicos (CLP), válvulas solenoide (SOL) e válvulas de bloqueio (SDV); apresentam-se seguidos de seus sistemas de votação. Por exemplo, a arquitetura "PT2oo3+CLP1oo2+SOL1oo2+SDV1oo2" referência: PT's na lógica de votação em que dois dos três deles detectando sobre pressão, acionará o sistema de segurança (2oo3); 2 (dois) solucionadores lógicos com votação 1oo2; 2 (duas) válvulas solenoides na votação 1oo2 e 2 (duas) válvulas de bloqueio com ativação 1oo2.

Etapa 3 - As variáveis identificadas (Tabela 2) são oriundas do manual de dados "*Reliability data for Safety Instrumented Systems*", uma vez que este apresenta os dados de confiabilidade adequados para análises SIL conforme a IEC 61508 e IEC 61511.

Tabela 2 - Principais parâmetros de confiabilidade para os componentes

COMPONENTE	Taxas de Falha (por 10^6 horas)				P_{TIF}	β	T (h)	MTTR (h)
	λ_s	$\lambda_{crítico}$	λ_{DU}	λ_{SU}				
Transmissores de Pressão	0,5	1,3	0,3	0,4	$5{,}0 \cdot 10^{-4}$	4%	4320	8
Entrada Analógica (simples)	0,4	0,44	0,04	0,4	$5{,}0 \cdot 10^{-6}$	3%	8640	8
CLP	0,3	0,33	0,03	0,3	$5{,}0 \cdot 10^{-6}$	3%	8640	8
Saída Digital (simples)	0,3	0,33	0,03	0,3	$5{,}0 \cdot 10^{-6}$	3%	8640	8
Válvula Solenoide	1,9	3	0,8	1,7	N/A	3%	4320	1
Válvula de Bloqueio	2,3	5,3	2,1	2,1	$1{,}0 \cdot 10^{-4}$	3%	4320	8

Fonte: Adaptado de Hauge; Onshus (2010)

Etapa 4 - As modelagens matemáticas realizadas seguiram as equações propostas no manual do método PDS "*Reliability Prediction Method for Safety Instrumented Systems PDS Method Handbook, 2010 Edition*" para cálculos de PFD, TIF, DTU, CSU e STR, apresentadas na tabela abaixo.

Tabela 3 – Principais equações para determinação da indisponibilidade do HIPPs

	VOTAÇÃO	CONTRIB. CAUSA COMUM		CONTRIB. CAUSA INDEPENDENTES
PFD	1oo1	-		$\lambda_{DU} \cdot T/2$
	1oo2	$\beta \cdot \lambda_{DU} \cdot T/2$	+	$[\lambda_{DU} \cdot T]^2/3$
	2oo2	-		$2 \cdot \lambda_{DU} \cdot T/2$
	1oo3	$C_{1oo3} \cdot \beta \cdot \lambda_{DU} \cdot T/2$	+	$[\lambda_{DU} \cdot T]^3/4$
	2oo3	$C_{2oo3} \cdot \beta \cdot \lambda_{DU} \cdot T/2$	+	$[\lambda_{DU} \cdot T]^2$
	3oo3	-		$3 \cdot \lambda_{DU} \cdot T/2$
	VOTAÇÃO	CONTRIBUIÇÃO DO TIF PARA O CSU		
PTIF	1oo1	P_{TIF}		
	1oo2	$B \cdot P_{TIF}$		
	MooN, M<N	$C_{MooN} \cdot B \cdot P_{TIF}$		
	NooN, (N = 1, 2, ...)	$N \cdot P_{TIF}$		
	VOTAÇÃO	TIPO DE FALHA	OPERAÇÃO DEGRADADA	OPERAÇÃO SEM PROTEÇÃO
DTU_R	1oo1	Um componente	N/A	$\lambda_D \cdot MTTR$
	1oo2	Um componente	$2 \cdot \lambda_D \cdot MTTR \cdot \lambda_{DU} \cdot T/2$	N/A
		Dois componentes	N/A	$\beta \cdot \lambda_D \cdot MTTR$
	2oo3	Um componente	$3 \cdot \lambda_D \cdot MTTR \cdot 2\lambda_{DU} \cdot T/2$	N/A
		Dois componentes	$(C_{2oo3}-C_{1oo3}) \cdot \beta \cdot \lambda_D \cdot MTTR \cdot \lambda_{DU} \cdot T/2$	N/A
		Três componentes	N/A	$C_{1oo3} \cdot \beta \cdot \lambda_D \cdot MTTR$
	VOTAÇÃO	STR		
STR	1oo1	λ_{SU}		
	1oo2	$2 \cdot \lambda_{SU}$		
	2oo2	$\beta \cdot \lambda_{SU}$		
	1oo3	$3 \cdot \lambda_{SU}$		
	2oo3	$C_{2oo3} \cdot \beta \cdot \lambda_{SU}$		
	3oo3	$C_{1oo3} \cdot \beta \cdot \lambda_{SU}$		
	1ooN; N = 1, 2, 3, ...	$N \cdot \lambda_{SU}$		
	MooN; 2 ≤ M ≤ N; N = 2, 3, ...	$C_{(N.M+1)ooN} \cdot \beta \cdot \lambda_{SU}$		

Fonte: Adaptado de Hauge et. al (2010)

De posse desses dados, para a análise matemática de cada cenário proposto na Etapa 2, buscou-se analisar a contribuição de cada variação dos componentes em termos das lógicas de votação para posteriormente compor os cenários. Os respectivos PDFs, PTIFs, DTUs e STRs são verificáveis na tabela 4, e é com base nesses valores que a indisponibilidade de cada cenário foi calculada.

Tabela 4 – Parâmetros de confiabilidade para os componentes.

COMPONENTES	PFD-CCF	%(CCF)	PFD-ID	%(ID)	PFD TOTAL	%(PFD)	PTIF	%(PTIF)	CSU	DTU DEGRADADO	DTU SEM PROTEÇÃO	STR
PTs (1oo2)	2,6E-05	98%	5,6E-07	2%	2,6E-05	57%	2,0E-05	43%	4,6E-05	8,29E-09	2,6E-07	8,0E-07
PTs (2oo2)	0	0%	1,3E-03	100%	1,3E-03	72%	5,0E-04	28%	1,8E-03	0	6,4E-06	1,6E-08
PTs (2oo3)	5,2E-05	97%	1,7E-06	3%	5,4E-05	57%	4,0E-05	43%	9,4E-05	2,50E-08	1,3E-07	3,2E-08
PTs (1oo3)	1,3E-05	100%	5,4E-10	0%	1,3E-05	56%	1,0E-05	44%	2,3E-05	8,29E-09	2,6E-07	1,2E-06
CLP (1oo1)	0	0%	4,3E-04	100%	4,3E-04	99%	5,0E-06	1%	4,4E-04	0	8,0E-07	1,0E-06
CLP (1oo2)	1,3E-05	98%	2,5E-07	2%	1,3E-05	99%	1,5E-07	1%	1,3E-05	3,46E-10	2,4E-08	2,0E-06
CLP (1oo3)	6,5E-06	100%	1,6E-10	0%	6,5E-06	99%	7,5E-08	1%	6,6E-06	3,46E-10	2,4E-08	3,0E-06
SOL (1oo1)	0	0%	1,7E-03	100%	1,7E-03	100%	0	0%	1,7E-03	0	1,1E-06	8,0E-07
SOL (1oo2)	5,2E-05	93%	4,0E-06	7%	5,6E-05	100%	0	0%	5,6E-05	3,80E-09	3,3E-08	1,6E-06
SOL (1oo3)	2,6E-05	100%	1,0E-08	0%	2,6E-05	100%	0	0%	2,6E-05	3,80E-09	3,3E-08	2,4E-06
SDV (1oo1)	0	0%	4,5E-03	100%	4,5E-03	98%	1,0E-04	2%	4,6E-03	0	2,4E-05	2,1E-06
SDV (1oo2)	1,4E-04	96%	6,0E-06	4%	1,4E-04	98%	3,0E-06	2%	1,5E-04	2,18E-07	2,4E-05	4,2E-06
SDV (1oo3)	6,8E-05	100%	1,9E-07	0%	6,8E-05	98%	1,5E-06	2%	7,0E-05	2,18E-07	2,4E-05	6,3E-06
SDV (2oo3)	2,7E-04	77%	8,2E-05	23%	3,5E-04	98%	6,0E-06	2%	3,6E-04	6,56E-07	3,6E-07	1,3E-07

Etapa 5 - De posse dos valores de cada componente e do sistema total para os cenários considerados, verificou-se além da influência técnica das diferentes arquiteturas, qual a influência da variação do tempo médio entre reparos (MTTR) e da frequência de testes (T) na disponibilidade de um HIPPS, uma vez que há disparidade entre valores encontrados em sistemas terrestres e marítimos.

RESULTADOS E DISCUSSÕES

A análise de sensibilidade busca verificar a adequação de cada uma das configurações à indisponibilidade aceitável de um HIPPs. Nesta seção são apresentadas as análises de sensibilidade com a variação de: MTTR (para 8 e 2160 horas) e T (para 3, 6 e 12 meses), totalizando 6 combinações.

A Tabela 5 apresenta a contribuição de indisponibilidade de cada uma dos cenários em termos de: probabilidade de falha na demanda de causa comum (PFD-CCF) e identificável (PDF-ID), a probabilidade de falha no teste independente (PTIF), indisponibilidade por paradas degradadas (DTU degradada) e não seguras (DTU sem proteção) e respectivas probabilidade de acionamentos espúrios (falha segura). Para esses números, o MTTR é de 8h e o T de 3 meses.

Tabela 5 – Contribuição de indisponibilidade para cada configuração.

CENÁRIO	PFD-CCF	PFD-ID	PFD-TOTAL	PTIF	CSU	DTU DEGRADADO	CSU total Degradado	DTU sem proteção	CSU total sem proteção	STR	STR (anos)
1	2,53E-04	1,19E-05	2,65E-04	4,32E-05	3,08E-04	2,47E-07	3,08E-04	2,42E-05	3,32E-04	7,83E-06	14,8
2	2,46E-04	1,16E-05	2,58E-04	4,31E-05	3,01E-04	2,47E-07	3,01E-04	2,42E-05	3,25E-04	8,83E-06	13,1
3	1,59E-04	2,13E-06	1,61E-04	4,17E-05	2,03E-04	2,47E-07	2,03E-04	2,42E-05	2,27E-04	1,07E-05	10,8
4	2,14E-04	1,02E-05	2,24E-04	1,32E-05	2,37E-04	2,30E-07	2,37E-04	2,43E-05	2,62E-04	9,00E-06	12,9
5	2,07E-04	9,95E-06	2,17E-04	1,31E-05	2,30E-04	2,30E-07	2,31E-04	2,43E-05	2,55E-04	1,00E-05	11,6
6	1,20E-04	4,46E-07	1,20E-04	1,17E-05	1,32E-04	2,30E-07	1,32E-04	2,43E-05	1,56E-04	1,19E-05	9,7
7	2,27E-04	1,08E-05	2,38E-04	2,32E-05	2,61E-04	2,30E-07	2,61E-04	2,43E-05	2,85E-04	8,60E-06	13,5
8	2,20E-04	1,05E-05	2,31E-04	2,31E-05	2,54E-04	2,30E-07	2,54E-04	2,43E-05	2,78E-04	9,60E-06	12,1
9	1,33E-04	1,01E-06	1,34E-04	2,17E-05	1,55E-04	2,30E-07	1,56E-04	2,43E-05	1,80E-04	1,15E-05	10,1
10	2,40E-04	4,44E-04	6,83E-04	4,80E-05	7,31E-04	2,47E-07	7,32E-04	2,50E-05	7,56E-04	6,83E-06	16,9
11	5,18E-05	6,70E-03	6,75E-03	1,45E-04	6,89E-03	2,50E-08	6,89E-03	2,60E-05	6,92E-03	3,93E-06	29,4
12	2,14E-04	4,43E-04	6,56E-04	2,80E-05	6,84E-04	2,30E-07	6,85E-04	2,51E-05	7,09E-04	7,60E-06	15,2
13	2,59E-05	6,70E-03	6,72E-03	1,25E-04	6,85E-03	8,29E-09	6,85E-03	2,62E-05	6,87E-03	4,70E-06	24,6

Fonte: Autores (2019)

Na configuração apresentada, como o SIL é definido pelo PFD, os cenários 1 a 9 apresentam uma contribuição significativa da indisponibilidade das falhas de causa comum (CCF), ou seja, vinculada à erros humanos, software ou eletrônicos decorrente das montagens paralelas dos equipamentos. As indisponibilidades dos equipamentos independentes (PFD-ID) são mais relevantes nos cenários de 10 a 13, já que possuem equipamentos em votações menores, 1oo2 ou 1oo1, o que faz sentido já que os componentes são praticamente únicos na configuração, o que não incide paralelismos, resultando em baixas indisponibilidades de PFD-CCF.

Nos demais cenários esse padrão se repete, o que é esperado dado que quanto menor a lógica de votação, maior a contribuição da probabilidade de falha de causa independente, ou seja, desgaste natural de materiais.

Dos dados apresentados na tabela 5, percebe-se que as válvulas de bloqueio muito contribuem para o SIL. Dessa forma, os PFD's desse componente influem e muito na definição do SIL de cada configuração, o que faz sentido, pois, esse componente é efetivamente a barreira de segurança desse sistema.

Já quanto às indisponibilidades por acionamentos espúrios (STR), configurações com mais componentes e lógicas de votação mais próximas (1oo2 e 2oo3), tendem a ocorrer mais cedo. O cenário 6 aciona mais rapidamente devido à maior lógica de votação (1oo3). Já o 13 e 11 demoram a serem acionados espuriamente, respectivamente 24,6 e 29,4 anos. Esse conceito reforça a proposição de Marszal e Scharpf (2002) que quanto menos equipamentos, menor a probabilidade de acionamentos espúrios, que são falhas seguras. Porém, são inversamente proporcionais às falhas perigosas não detectáveis, pois são exatamente essas configurações que possuem as maiores probabilidades de falhas.

A Tabela 6 apresenta, respectivamente: o SIL para as configurações em cada uma das combinações; a % relativa de contribuição da indisponibilidade do HIPPs oriunda do CSU e a % relativa da contribuição de indisponibilidade do sistema total na ótica do DTU sem proteção.

Tabela 6 - SIL relativo a cada uma das combinações da análise de sensibilidade

CENÁRIOS	COMBINAÇÃO 1 MTTR=8 | T=3	COMBINAÇÃO 2 MTTR=8 | T=6	COMBINAÇÃO 3 MTTR=8 | T=12	COMBINAÇÃO 4 MTTR=2160 | T=3	COMBINAÇÃO 5 MTTR=2160 | T=6	COMBINAÇÃO 6 MTTR=2160 | T=12
1	SIL 3	SIL 3	SIL 3	SIL 3	SIL 3	SIL 3
2	SIL 3	SIL 3	SIL 3	SIL 3	SIL 3	SIL 3
3	SIL 4	SIL 3	SIL 3	SIL 4	SIL 3	SIL 3
4	SIL 3	SIL 3	SIL 3	SIL 3	SIL 3	SIL 3
5	SIL 3	SIL 3	SIL 3	SIL 3	SIL 3	SIL 3
6	SIL 4	SIL 3	SIL 3	SIL 4	SIL 3	SIL 3
7	SIL 3	SIL 3	SIL 3	SIL 3	SIL 3	SIL 3
8	SIL 3	SIL 3	SIL 3	SIL 3	SIL 3	SIL 3
9	SIL 4	SIL 3	SIL 3	SIL 4	SIL 3	SIL 3
10	SIL 3	SIL 3	SIL 2	SIL 3	SIL 3	SIL 2
11	SIL 2	SIL 2	SIL 1	SIL 2	SIL 2	SIL 1
12	SIL 3	SIL 3	SIL 2	SIL 3	SIL 3	SIL 2
13	SIL 2	SIL 2	SIL 1	SIL 2	SIL 2	SIL 1

Fonte: Autores (2019).

Quanto aos SILs (Tabela 6), em sua maioria, as configurações apresentam um SIL 3, considerado adequado para o ambiente de petróleo. As configurações com SILs inferiores, em geral, são aquelas com a menor quantidade de componentes no sistema e válvulas de segurança com lógica de votação 1oo1. Isso significa que são sistemas sem redundâncias e, portanto, mais susceptíveis a falharem quando demandados, principalmente quanto às válvulas de bloqueio.

As combinações e cenários que excederam o padrão foram aquelas com T de 3 meses e 3 componentes de válvulas de fechamento na votação 1oo3. Isso significa que menores tempos entre testes conferem uma maior disponibilidade do sistema na demanda, bem como os elementos finais do sistema na lógica 1oo3, pois a ativação de somente um deles já garante o fechamento do HIPPs quando demandado, já que ele é efetivamente a barreira de segurança.

A combinação de T de 12 meses já indica uma piora na disponibilidade dos sistemas, haja vista que quanto maior o tempo entre os testes, mais susceptíveis aos desgastes naturais e falhas técnicas ou humanas. Já referente ao MTTR, este

não mostrou exercer influência significativa no SIL das configurações, não alterando significativamente a indisponibilidade do sistema.

Tabela 7 - Contribuição da CSU para indisponibilidade do HIPPs em comparação ao DTU sem proteção

CENÁRIOS	COMBINAÇÃO 1 MTTR=8 | T=3	COMBINAÇÃO 2 MTTR=8 | T=6	COMBINAÇÃO 3 MTTR=8 | T=12	COMBINAÇÃO 4 MTTR=2160 | T=3	COMBINAÇÃO 5 MTTR=2160 | T=6	COMBINAÇÃO 6 MTTR=2160 | T=12
1	87,7%	92,7%	96,1%	2,6%	4,5%	8,4%
2	87,5%	92,6%	96,0%	2,5%	4,4%	8,2%
3	83,4%	89,3%	93,8%	1,8%	3,0%	5,3%
4	83,5%	90,7%	95,2%	1,8%	3,5%	6,8%
5	83,1%	90,5%	95,1%	1,8%	3,4%	6,7%
6	74,7%	84,4%	91,3%	1,1%	2,0%	3,7%
7	85,1%	91,5%	95,5%	2,1%	3,8%	7,3%
8	84,8%	91,3%	95,4%	2,0%	3,7%	7,2%
9	78,4%	86,5%	92,3%	1,3%	2,3%	4,3%
10	93,9%	96,7%	98,3%	5,4%	9,8%	17,6%
11	99,3%	99,6%	99,8%	34,3%	50,6%	67,0%
12	93,4%	96,5%	98,2%	5,0%	9,2%	16,8%
13	99,3%	99,6%	99,8%	34,0%	50,3%	66,7%
MÉDIA	**89,6%**	**93,8%**	**96,7%**	**16,9%**	**23,3%**	**30,4%**

Fonte: Autores (2019)

Após análise do PFD, analisaram-se as contribuições de cada elemento na indisponibilidade do sistema. Na Tabela 7, é possível perceber a ação da variação do MTTR e do T. Nas combinações, percebe-se que quanto maior o período entre testes, maior a contribuição de falhas independentes ou de causa comum na indisponibilidade do sistema. Já na ótica do MTTR, quanto maior o MTTR, o sistema possui maior representatividade de falhas oriundas de paradas não programadas, sejam elas por deterioração ou sem proteção.

Tabela 8 - Contribuição da DTU deteriorado quando comparada ao CSU

CENÁRIOS	COMBINAÇÃO 1 MTTR=8 | T=3	COMBINAÇÃO 2 MTTR=8 | T=6	COMBINAÇÃO 3 MTTR=8 | T=12	COMBINAÇÃO 4 MTTR=2160 | T=3	COMBINAÇÃO 5 MTTR=2160 | T=6	COMBINAÇÃO 6 MTTR=2160 | T=12
1	0,07%	0,08%	0,08%	15,99%	17,58%	18,05%
2	0,07%	0,08%	0,08%	16,26%	17,91%	18,40%
3	0,10%	0,12%	0,13%	21,26%	24,48%	26,27%
4	0,09%	0,10%	0,10%	19,95%	20,49%	20,24%
5	0,10%	0,10%	0,10%	20,40%	20,97%	20,72%
6	0,16%	0,17%	0,18%	29,89%	31,65%	32,49%
7	0,08%	0,09%	0,09%	18,00%	18,99%	19,04%
8	0,08%	0,09%	0,09%	18,36%	19,40%	19,47%
9	0,13%	0,15%	0,16%	25,71%	28,22%	29,50%
10	0,03%	0,03%	0,03%	7,81%	8,23%	8,36%
11	0,00%	0,00%	0,00%	0,10%	0,10%	0,10%
12	0,03%	0,03%	0,03%	7,95%	8,19%	8,23%
13	0,00%	0,00%	0,00%	0,03%	0,03%	0,03%
MÉDIA	**0,09%**	**0,09%**	**0,09%**	**18,00%**	**18,79%**	**18,56%**

Fonte: Autores (2019)

Na Tabela 8, referente à frequência de testes, o seu aumento é inversamente proporcional à contribuição dos componentes deteriorados à indisponibilidade do HIPPs, pois estes complementam as informações apresentadas na tabela anterior. Para o MTTR, os comportamentos também são divergentes. Neste caso, quando do aumento do MTTR, há uma maior representatividade da deterioração na não disponibilidade. Para sistemas deteriorados, porém, a média é de 18%.

Nesse sentido, as indisponibilidades por paradas sem proteção são mais significativas na análise do HIPPs, que analisaremos a seguir.

Tabela 9 - Contribuição da DTU sem proteção quando comparada ao CSU.

CENÁRIOS	COMBINAÇÃO 1 MTTR=8 | T=3	COMBINAÇÃO 2 MTTR=8 | T=6	COMBINAÇÃO 3 MTTR=8 | T=12	COMBINAÇÃO 4 MTTR=2160 | T=3	COMBINAÇÃO 5 MTTR=2160 | T=6	COMBINAÇÃO 6 MTTR=2160 | T=12
1	12,3%	7,3%	3,9%	97,4%	95,5%	91,6%
2	12,5%	7,4%	4,0%	97,5%	95,6%	91,8%
3	16,6%	10,7%	6,2%	98,2%	97,0%	94,7%
4	16,5%	9,3%	4,8%	98,2%	96,5%	93,2%
5	16,9%	9,5%	4,9%	98,2%	96,6%	93,3%
6	25,3%	15,6%	8,7%	98,9%	98,0%	96,3%
7	14,9%	8,5%	4,5%	97,9%	96,2%	92,7%
8	15,2%	8,7%	4,6%	98,0%	96,3%	92,8%
9	21,6%	13,5%	7,7%	98,7%	97,7%	95,7%
10	6,1%	3,3%	1,7%	94,6%	90,2%	82,4%
11	0,7%	0,4%	0,2%	65,7%	49,4%	33,0%
12	6,6%	3,5%	1,8%	95,0%	90,8%	83,2%
13	0,7%	0,4%	0,2%	66,0%	49,7%	33,3%
MÉDIA	**10,4%**	**6,2%**	**3,3%**	**83,1%**	**76,7%**	**69,6%**

Fonte: Autores (2019)

A Tabela 9 complementa os valores referentes à CSU. Como pode ser percebido, a variação da frequência de testes altera a representatividade do DTU em sistemas sem proteção, porém, a alteração do MTTR que altera significativamente estas contribuições, invertendo os responsáveis pela indisponibilidade do sistema: com baixo MTTR, maior é a incidência dos componentes na indisponibilidade, e com altos MTTRs, a ausência de proteção dos sistemas é que mais respondem pela disponibilidade do HIPPs.

CONSIDERAÇÕES FINAIS

Esta produção, além de ampliar as discussões acadêmicas sobre o uso da metodologia PDS para cálculo da disponibilidade de sistemas instrumentados de segurança, permitiu realizar uma análise da influência técnica da arquitetura, frequências de testes e tempo médio entre reparo na variação da disponibilidade de um HIPPS.

Assim, constatou-se que, apesar de ter sido averiguado que quanto maior a redundância de equipamentos, maiores serão os valores de PFD, maior SIL e menor STR; de acordo com as combinações expostas, as medidas de tempo médio para reparo e frequência de testes se mostraram mais representativas para a indisponibilidade do sistema do que as variações de arranjos. E, ainda, que o aumento da frequência de teste fomenta a elevação do PFD de falhas independentes.

A análise de sensibilidade permitiu concordar com a proposição de Marszal e Scharpf (2002), de que a probabilidade de falha na demanda de um dispositivo depende de sua frequência de testes e reparos. Foi observado que, a medida que a frequência de testes aumenta, o PFD acompanha, porém, não foi possível observar se a relação seria exponencial, como sugerido pelos autores.

Já quanto às ativações espúrias (STR), percebeu-se seu aumento com a inserção de componentes redundantes nos sistemas, conforme previsto por

Lundteigen, Rausand e Utne (2009). Apesar disso, devem-se balancear estes efeitos com aqueles positivos oferecidos pelas arquiteturas redundantes.

Por fim, destaca-se que o HIPPs na filosofia degradada, em geral, apresenta uma contribuição muito baixa, sendo irrisória para a análise final da disponibilidade do sistema. Entretanto, quando o MTTR é elevado, principalmente usados em sistemas submarinos, essas falhas mostram suas importâncias para tais funções.

Analysis of the technical influence of the architecture, frequency of tests and average time between repair in the availability of a high integrity pressure protection system

ABSTRACT

In view of contribution of the safety instrumented system (SIS), especially in high integrity systems for high pressure protection (HIPPS), allowing that different processes to be leveraged to even more secured levels, the present study sought to analyze the availability of a HIPPS in different configurations through the influence of architecture, test frequencies and average time between repairs (MTTR). Therefore, in the methodological procedures, a base model architecture was defined to analyze different proposals. Such analyzes were subsidized by identifying the variables in the data manual "Reliability data for Safety Instrumented Systems" and math models performed using equations proposed in the PDS method manual "Reliability Prediction Method for Safety Instrumented Systems PDS Method Handbook, 2010 Edition" to analyze such influences. As results of the research, it is verified that, according to the scenarios studied, the MTTR and test frequency were more representative for the system unavailability than the variations of the arrangements. Also, the increase in the test frequency promotes the increase of the PFD from independent failures; as well as the HIPPs in the degraded philosophy, in general, presented a very low contribution, being innocuous for the availability. However, when the MTTR increases, such failures show their importance to such functions. Finally, as proposed by Marszal e Scharpf (2002), spurious trips are more relevant in redundant architectures, independent of test times and between repairs.

KEYWORDS: SIS. HIPPS. Probability of Failure. SIL.

REFERÊNCIAS

ALIZADEH, S.; SRIRAMULA, S. Unavailability assessment of redundant safety instrumented systems subject to process demand. **Reliability Engineering & System Safety**, v. 171, p. 18–33, mar. 2018. crossref

AMERICAN PETROLEUM INSTITUTE. API 17O: Subsea High Integrity Pressure Protection Systems (HIPPS). 1th ed. [s.i.]: **American Petroleum Institute**, p. 54, 2014.

AMINI, Z.; SABER, I. N. H. **Application of High Integrity Pressure Protection Systems**. p. 12, [s.d.].

AZIZPOUR, H.; LUNDTEIGEN, M. A. Analysis of simplification in Markov-based models for performance assessment of Safety Instrumented System. **Reliability Engineering and System Safety**, v. 183, n. September 2018, p. 252–260, 2019. crossref

BAI, Y.; BAI, Q.. Subsea Engineering Handbook. Burlington, MA: **Elsevier**, p. 919, 2010. crossref

BASU, S. Plant Hazard Analysis and Safety Instrumentation Systems. 1. ed. London: **Academic Press**, 2017. ISBN 978-0-12-803763-8. crossref

CLARKE, P. **Proactive minimization of systematic failures in safety instrumented systems**. In: HAZARDS ASIA PACIFIC CONFERENCE, 2013.

DUTUIT, Y.; RAUZY, A. B.; SIGNORET, J.-P. A snapshot of methods and tools to assess safety integrity levels of high-integrity protection systems. Proceedings of the Institution of Mechanical Engineers, Part O: **Journal of Risk and Reliability**, v. 222, n. 3, p. 371–379, set. 2008. crossref

DUTUIT, Y.; INNAL, F.; RAUZY, A.; SIGNORET, J. -P. Probabilistic assessments in relationship with safety integrity levels by using Fault Trees. **Reliability Engineering and System Safety**, v. 93, n. 12, p. 1867–1876, 2008. crossref

GOBLE, W.; M. CHEDDIE, H. L. **Safety Instrumented Systems Verification – Pratical Probabilistic Calculations**. 1. ed. Durham: ISA. 2005.

HAUGE, S.; LUNDTEIGEN, M. A.; HOKSTAD, P.; HÅBREKKE, S.. **Reliability Prediction Method for Safety Instrumented Systems PDS Method Handbook, 2010 Edition**. Multiclient - PDS Forum, 2010.

HAUGE, S.; ONSHUS, T.. **Reliability data for Safety Instrumented Systems**. Multiclient - PDS Forum, 2010.

INNAL, F.; CHEBILA, M.; DUTUIT, Y. Uncertainty handling in safety instrumented systems according to IEC 61508 and new proposal based on coupling Monte Carlo analysis and fuzzy sets. **Journal of Loss Prevention in the Process Industries**, v. 44, p. 503–514, nov. 2016. crossref

INNAL, F.; DUTUIT, Y.; CHEBILA, M. Safety and operational integrity evaluation and design optimization of safety instrumented systems. **Reliability Engineering & System Safety**, v. 134, p. 32–50, fev. 2015. crossref

INTERNATIONAL ELECTROTECHNICAL COMMISSION. IEC 61508-1: **Functional safety of electrical/electronic/programmable electronic safety-related systems** – Part 1: General requirements. 2. ed. Genebra: IEC, 2010.

ISO 2016. **Petroleum, petrochemical and natural gas industries --Reliability modelling and calculation of safety systems**. CEN ISO/TR 12489:2016. BSI Standards Limited, 2016.

JIN, J; PANG, L.; ZHAO, S.; HU, B. Quantitative assessment of probability of failing safely for the safety instrumented system using reliability block diagram method. **Annals of Nuclear Energy**, v. 77, p. 30–34, 2015. crossref

KRITZINGER, D. Aircraft System Safety: Assessments for Initial Airworthiness Certification. 1. ed. Cambridge: **Woodhead Publishing Limited**, 2017. ISBN 978-0-08-100889-8.

LANGERON, Y.; BARROS, A.; GRALL, A.; BÉRENGUER, C.; Combination of safety integrity levels (SILs): a study of IEC61508 merging rules. **J. Loss Prev. Process. Ind.** 21 (4), 437–449, 2008. ISSN 0950-4230. crossref

LUNDTEIGEN, M. A.; RAUSAND, M.; UTNE, I. B. Integrating RAMS engineering and management with the safety life cycle of IEC 61508. **Reliability Engineering and System Safety**, v. 94, n. 12, p. 1894–1903, 2009. crossref

LIU, Y.; RAUSAND, M. Reliability assessment of safety instrumented systems subject to different demand modes. **Journal of Loss Prevention in the Process Industries**, v. 24, n. 1, p. 49–56, jan. 2011. crossref

MARSZAL, E. M.; SCHARPF, E. W. Safety Integrity Level Selection: Systematic Methods Including Layer of Protection Analysis. **Research Triangle Park**, NC: ISA, 2002.

MECHRI, W.; SIMON, C.; BEN OTHMAN, K. 2012. Uncertainty analysis of common cause failure in safety instrumented systems. **Proc. Inst. Mech. Eng. Part O J. Risk Reliab.** 226, 450e460. crossref

PAPADOPOULOS, Y. et al. **Automatic allocation of safety integrity levels. Proceedings of the 1st Workshop on Critical Automotive applications Robustness & Safety - CARS '10**. Anais... In: THE 1ST WORKSHOP. Valencia, Spain: ACM Press, 2010. Disponível em: <http://portal.acm.org/citation.cfm?doid=1772643.1772646>. Acesso em: 21 maio. 2019.

RAUSAND, M.. **Reliability of Safety-Critical Systems: Theory and Applications**. 1. ed. Hoboken, NJ: Wiley, 2014. ISBN 978-1-118-11272-4. crossref

ROUVROYE, J.L.; WIEGERINCK, J.A. Minimizing costs while meeting safety requirements: modeling deterministic (imperfect) staggered tests using standard Markov models for SIL calculations. **ISA (Instrum. Soc. Am.)** Trans. 45 (4), 611–621, 2006. ISSN 0019-0578. crossref

SAL, R.; NAIT-SAID, R.; BOURARECHE, M. Dealing with uncertainty in effect analysis of test strategies on safety instrumented system performance. **International Journal of System Assurance Engineering and Management**, v. 8, n. S2, p. 1945–1958, nov. 2017. crossref

SIMON, C.; MECHRI, W.; CAPIZZI, G. Assessment of Safety Integrity Level by simulation of Dynamic Bayesian Networks considering test duration. **Journal of Loss Prevention in the Process Industries**, v. 57, p. 101-113, 2018. crossref

SUMMERS, A; GENTILE, M. **Random, Systematic, and Common Cause Failure:** How do you manage them? Process Safety Progress, v. 5, p. 333-338, dez. 2006. crossref

TORRES-ECHEVERRÍA, A. C.; MARTORELL, S.; THOMPSON, H. A. Design optimization of a safety-instrumented system based on RAMS+C addressing IEC 61508 requirements and diverse redundancy. **Reliability Engineering & System Safety**, v. 94, n. 2, p. 162–179, fev. 2009. crossref

XIE, L.; HÅBREKKE, S.; LIU, Y.; LUNDTEIGEN, M. A. Operational data-driven prediction for failure rates of equipment in safety instrumented systems: A case study from the oil and gas industry. **Journal of Loss Prevention in the Process Industries**, v. 60, p. 96–105, jul. 2019. crossref

WU, S.; ZHANG, L.; LUNDTEIGEN, M.A.; LIU, Y.; ZHENG, W. Reliability assessment for final elements of SISs with time dependent failures. **J. Loss Prev. Process. Ind.** 51, 186–199, 2018. crossref

Recebido: 22 Jul. 2019
Aprovado: 09 Out. 2020
DOI: 10.3895/gi.v16n1.10385
Como citar:
NUNES, J.P.C.S. et al. Análise da influência técnica da arquitetura, frequência de testes e tempo médio entre reparo na disponibilidade de um high integrity pressure protection system. **R. Gest. Industr.**, Ponta Grossa, v. 16, n. 1, p. 99-120, Jan./Mar. 2020. Disponível em: http://periodicos.utfpr.edu.br/revistagi .
Correspondência:
João Paulo Costa e Silva Nunes
Universidade Federal do Rio Grande do Norte (UFRN), Natal, Rio Grande do Norte, Brasil.