UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
DEPARTAMENTO ACADÊMICO DE ELETRÔNICA
AUTOMAÇÃO INDUSTRIAL

JOSENEY DOMINGUES DA SILVA

ESTUDO SOBRE SISTEMAS INSTRUMENTADOS DE SEGURANÇA: conceitos, regulamentação e aplicações na indústria

MONOGRAFIA

CURITIBA
2012

JOSENEY DOMINGUES DA SILVA

ESTUDO SOBRE SISTEMAS INSTRUMENTADOS DE SEGURANÇA: conceitos, regulamentação e aplicações na indústria

Monografia de conclusão do Curso de Especialização em Automação Industrial do Departamento Acadêmico de Eletrônica da Universidade Tecnológica Federal do Paraná apresentada como requisito parcial para obtenção do grau de Especialista em Automação Industrial.

Prof. MSc. Guilherme Alceu Schneider

CURITIBA
2012

AGRADECIMENTOS

A Deus pela saúde, capacidade e oportunidades. A minha família que, pacientemente, me apoiou e aceitou as ausências causadas pela busca dos meus objetivos.

Ao professor orientador, MSC. Guilherme A. Schneider que acreditou nesta proposta e orientou a realização deste trabalho.

We must try to anticipate and prevent accidents before they occur. This has been one of the hard lessons learned from past accidents and why various process safety regulations was passed in different parts of the world.

(GRUHN; CHEDDIE, 2006)

Nós devemos tentar antecipar e prevenir acidentes antes que eles ocorram. Esta tem sido uma das difíceis lições aprendidas em acidentes ocorridos e a razão de várias regulamentações sobre segurança de processo terem sido aprovadas em diferentes partes do mundo.

(GRUHN; CHEDDIE, 2006 – tradução nossa)

RESUMO

SILVA, Joseney D. **Estudo sobre sistemas instrumentados de segurança:** Conceitos, regulamentação e aplicações na indústria. 2012. 59 p. Monografia - Especialização em Automação Industrial do Departamento Acadêmico de Eletrônica, Universidade Tecnológica Federal do Paraná, Curitiba, 2012.

Este estudo, focado na indústria de processo, apresenta conceitos relativos a Sistemas Instrumentados de Segurança – SIS, a regulamentação internacional associada e sua evolução. São abordadas questões relevantes como: as diferentes características e requisitos aplicáveis aos sistemas de segurança e sistemas de controle; a segregação requerida entre sistemas de controle e de segurança pelos diferentes padrões da indústria e pelas referências normativas; as exceções admitidas por norma, tanto funções de controle executado por sistemas de segurança como execução de Funções Instrumentadas de Segurança - SIF por sistemas de controle. Apresenta brevemente a técnica LOPA, para análise dos riscos de processo e seleção do Nível de Integridade de Segurança – SIL. Cada uma das fases do ciclo de vida do SIS é detalhada, seguindo o roteiro estabelecido na norma IEC 61511 de 2003. Considerações acerca de topologias típicas para diferentes SIL são mostradas assim como um exemplo de aplicação industrial e as configurações mais comuns de elementos finais e sensores. Uma aplicação específica de SIS, o HIPPS – High Integrity Pressure Protection System também foi incluído dentre as aplicações. Na abordagem sobre as tecnologias utilizadas, deve ser destacado o desenvolvimento do protocolo Foundation Fieldbus para a execução de Funções Instrumentadas de Segurança, devido ao grau de inovação. Detalhes do projeto, conhecido como FF-SIF, informações sobre os resultados já obtidos são trazidas ao leitor.

Palavras-chave: Sistemas Instrumentados de Segurança. Sistemas de Intertravamento. Automação. SIL. SIF.

ABSTRACT

SILVA, Joseney D. **Safety Instrumented Systems:** Concepts, rules and industrial applications. 2012. Monografia - Especialização em Automação Industrial do Departamento Acadêmico de Eletrônica, Universidade Tecnológica Federal do Paraná, Curitiba, 2012.

This study focused on process industry, presents concepts related to Safety Instrumented Systems - SIS, international regulations related and its developments. It covers relevant issues as: the different characteristics and requirements for safety systems and control systems; segregation required between control and safety systems by different industry standards and the normative references; exceptions permitted by the industry standards, both control function implemented on safety systems and Safety Instrumented Function - SIF on control systems. Briefly describe the LOPA technique for process risk analysis and selection of the Safety Integrity Level - SIL. Each stage of the life cycle of the SIS is detailed by following the steps set out in the standard IEC 61511-2003. Considerations about typical topologies for different SIL are shown, such as an example of industrial application and the most common settings of sensors and final elements. A specific application of SIS, HIPPS - High Integrity Pressure Protection System was also included among the applications. In the approach on the technology used, it must be noted the development of the Foundation Fieldbus protocol for executing Safety Instrumented Function, given the degree of innovation. Details of the project, known as FF-SIF, information on the results already achieved are brought to the reader.

Keywords: Safety Instrumented Systems. Interlocking Systems. Automation. SIL. SIF.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
AIChE	American Institute of Chemical Engineers
ALARP	*As Low As Reasonably Practicable* (Tão Baixo Quanto Razoavelmente Praticável)
ANSI	American National Standards Institute
API	American Petroleum Institute
APR	Análise Preliminar de Riscos
BPCS	*Basic Process Control System*
CCPS	Center for Chemical Process Safety
Conama	Conselho Nacional do Meio Ambiente
CLP	Controlador Lógico Programável
DCS	*Digital Control System*
FMEDA	*Failure Modes, Effects and Diagnostic Analysis*
FTOL	Freqüência Tolerável
HAZOP	*Hazards and Operability Study* (Estudo de Perigos e Operabilidade)
HIPPS	*High Integrity Pressure Protection System*
HSE	UK Health & Safety Executive
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IHM	Interface Homem-Máquina
IPL	*Independent Protection Layer* (Camada de Proteção Independente)
ISA	Instrumentation, Systems, and Automation Society
LOPA	*Layers of Protection Analysis* (Análise de Camadas de Proteção)
MTBF	*Mean Time Between Failures* (Tempo Médio entre Falhas)
MTTF	*Mean Time to Fail* (Tempo Médio para Falhar)
MTTFS	*Mean Time to Fail Safe* (Tempo Médio para Falhar no modo Seguro)
MTTR	*Mean Time to Repair* (Tempo Médio para Reparo)
NEC	National Electric Code
NFPA	National Fire Protection Association
OSHA	Occupational Safety & Health Administration
PFD	*Probability of Failure on Demand* (Probabilidade de Falha sob Demanda)
PFDavg	Probabilidade Média de Falha sob Demanda;
PLC	*Programmable Logic Controller*
RRF	*Risk Reduction Factor* (Fator de Redução de Risco)
SDCD	Sistema Digital de Controle Distribuído
SIF	Safety Instrumented Function (Função Instrumentada de Segurança)
SIL	Safety Integrity Level (Nível de Integridade de Segurança)
SIS	Safety Instrumented System
SRS	Safety Requirements Specification (Especificação de Requisitos de Segurança)
TAF	Factory Acceptance Test (Teste de Aceitação em Fábrica)
TMR	Triple Modular Redundancy
TÜV	Techinische Überwachungs Verein (Agência de Inspeção Técnica)

SUMÁRIO

1 INTRODUÇÃO

Neste capítulo serão apresentados o tema, o problema e as premissas, os objetivos geral e específicos bem como as justificativas, a metodologia e a estrutura do trabalho.

1.1 TEMA

Entidades governamentais têm exigido ações preventivas tanto para a instalação e ampliação quanto para a operação de empreendimentos que possam causar degradação ambiental (CONSELHO..., 2008, p. 748).

Devido aos riscos inerentes à operação de indústrias de processo (química, petroquímica, petróleo e outras), a magnitude de potenciais desastres decorrentes de eventos perigosos impedem o método de tentativa e erro, o que contribui para a aplicação freqüente de sistemas de proteção (GRUHN; CHEDDIE, 2006, p. 4).

Com o objetivo de atingir ou manter um estado seguro de um processo ou equipamento pela ação automática específica frente a um determinado desvio operacional são empregadas Funções Instrumentadas de Segurança (Safety Instrumented Function - SIF), conforme definição da N 2595 (COMISSÃO..., 2011).

Quando o operador e o sistema de controle falha no controle de processo as SIFs são acionadas, levando o processo para a condição segura (GRUHN; CHEDDIE, 2006).

Para implementação de SIFs podem ser utilizados sistemas mecânicos, pneumáticos, elétricos ou eletrônicos. No caso de Sistemas Instrumentados de Segurança – SIS estes são compostos por iniciadores, executores de lógica e elementos finais segundo a IEC 61508-1 (INTERNATIONAL..., 2010). A figura 1 apresenta sistemas de controle e de segurança com as estações de operação, manutenção e engenharia integradas, porém com as redes, programas e dispositivos específicos segregados (EMERSON PROCESS, 2012 a).

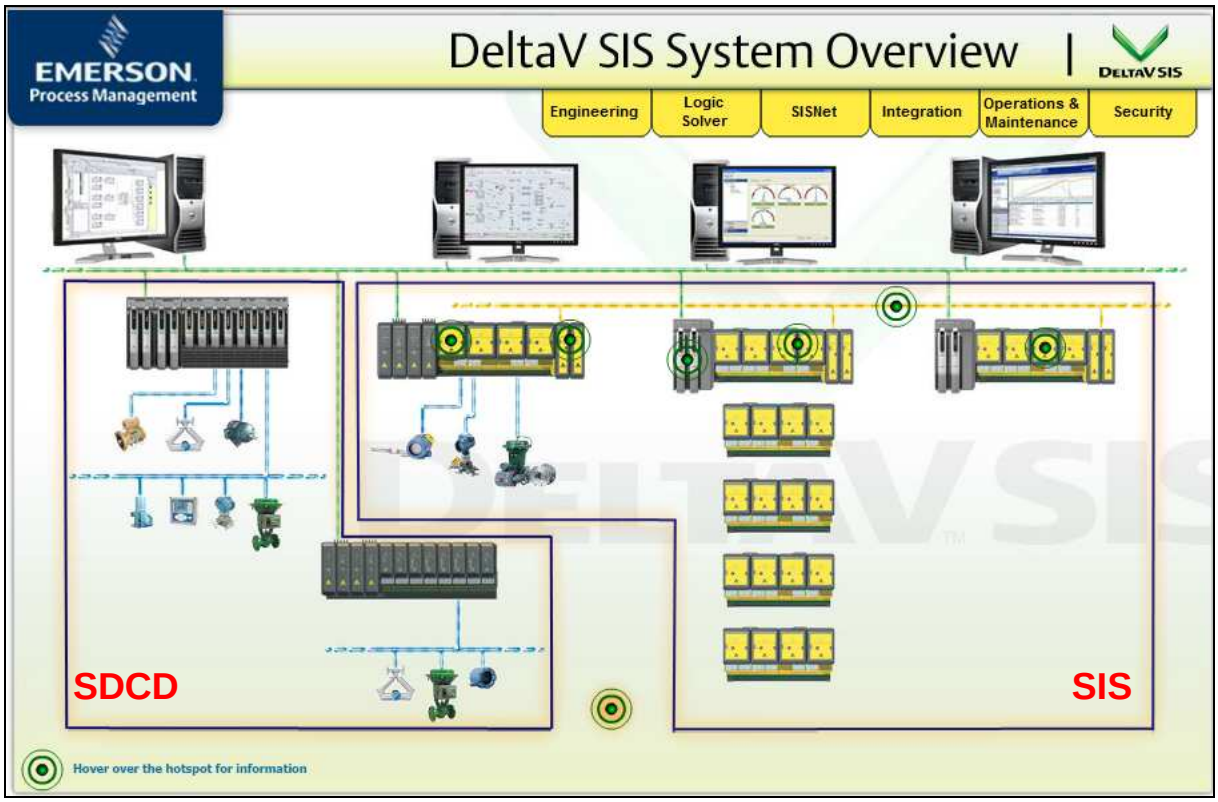

Figura 1: Visão Geral do Sistema DeltaV SIS
Fonte: adaptado de Emerson Process (2012 a)

Para subsidiar o presente estudo foi verificada a regulamentação associada aos SIS. Foram pesquisadas normas técnicas brasileiras no sitio da Associação Brasileira de Normas Técnicas – ABNT (ASSOCIAÇÃO..., 2012), não sendo localizadas normas relativas aos SIS e correlatos. Foram então consultadas as normas técnicas internacionais da International Electrotechnical Commission – IEC e normas nacionais como as da ISA – Instrumentation, Systems and Automation Society e da American Petroleum Institute – API.

Neste estudo serão apresentados os conceitos identificados, as regulamentações levantadas e exemplos de aplicação de sistemas instrumentados de segurança na indústria de processo, com foco na indústria de petróleo e suas especificidades.

1.2 PROBLEMA E PREMISSAS

Para aplicação de SIS nas indústrias de processo devem ser observadas as disposições contidas na IEC 61511-1 (INTERNATIONAL..., 2003), referentes à especificação, projeto, instalação e manutenção de SIS na indústria de processo.

Uma vez identificada a necessidade de utilização de um SIS, devem ser seguidas as normas e regulamentos aplicáveis para o ciclo de vida do sistema (GRUHN; CHEDDIE, 2006). Para alcançar e manter a confiabilidade especificada para o SIS, deve ser observado todo o seu ciclo de vida, escopo de profissionais que atuam na engenharia, operação e manutenção dos sistemas.

Apesar da evolução observada nos SIS e nas normas técnicas, da elaboração de normas técnicas orientadas ao desempenho dos sistemas e da ampliação das responsabilidades dos profissionais que atuam nesta área tais conhecimentos são pouco difundidos (FINKEL et al, 2006). Decorrem deste fato:

- a dificuldade em perceber que intertravamentos, existentes ou novos, são na verdade Funções Instrumentadas de Segurança, para as quais existem requisitos legais e normativos;
- a degradação dos SIS instalados, pela inobservância das especificações e recomendações originadas na fase de estudos durante o ciclo de vida do SIS.

Surge então a possibilidade, aqui explorada, de pesquisar o estado da arte e da prática para produzir material que concentre informações acerca do SIS, dentro do escopo delimitado.

1.3 OBJETIVOS

Nesta seção são apresentados o objetivo geral e os meios empregados em sua busca, os objetivos específicos.

1.3.1. Objetivo Geral

Elaborar um relatório técnico que apresente os conceitos, a regulamentação e algumas aplicações industriais de Sistemas Instrumentados de Segurança – SIS.

1.3.2. Objetivos Específicos

A busca ao objetivo geral proposto será por meio dos seguintes objetivos específicos:

- pesquisar normas técnicas e regulamentos aplicáveis;
- pesquisar bibliografia sobre a aplicação de SIS na indústria de petróleo;
- identificar tecnologias novas e atuais para aplicações de SIS na indústria de petróleo;
- pesquisar possíveis ganhos ou perdas decorrentes da instalação ou ausência de SIS;
- produzir material técnico para subsidiar profissionais que possuam alguma interface com Funções Instrumentadas de Segurança, novas ou já implantadas.

1.4 JUSTIFICATIVAS

Apesar da expansão observada na indústria de processo as normas existentes tais como as elaboradas pela IEC e ISA são normas focadas no desempenho do sistema e não possuem caráter prescritivo (FINKEL et al, 2006, p. 574).

Gruhn e Cheddie (2006, p. 13) correlacionam a abordagem atual das normas com a explosão da plataforma de Piper Alpha, ocorrida no Mar do Norte, pois a

elaboração de normas voltadas a desempenho dos sistemas foi uma das recomendações da comissão que investigou tal evento.

Segundo Gruhn e Cheddie (2006), cada organização deve definir o que é seguro e como os sistemas serão comprovadamente seguros. A liberdade dada pelas normas permite seleção de tecnologias, níveis de redundância e intervalos de teste para atingir o Safety Integrity Level – SIL desejado, o que exige ainda mais conhecimento e experiência das equipes técnicas envolvidas.

Este estudo pretende contribuir com os profissionais em sua busca por informações, pois apresenta além da revisão bibliográfica, uma visão geral das principais normas existentes focando na abordagem das normas da International Electrotechnical Commission – IEC.

1.5 METODOLOGIA

Esta pesquisa, de natureza científica aplicada, segundo seus objetivos mais gerais é classificada como descritiva (GIL, 2010, p. 27).

Para a elaboração desta monografia foram pesquisadas as normas técnicas internacionais e normas estrangeiras consideradas como referência pela comunidade técnica, em uma pesquisa do tipo bibliográfica. A Norma N 2595 (COMISSÃO..., 2011) também foi consultada em função de suas particularidades, tais como seu caráter prescritivo e o uso de Sistema Digital de Controle Distribuído – SDCD para SIL mais baixos (FINKEL et al, 2006).

A pesquisa, em seus pormenores, está descrita nos capítulos 2, 3, 4 e 5.

1.6 ESTRUTURA DO TRABALHO

Esta monografia é composta de cinco capítulos, integrados e complementares.

No capítulo 1 é apresentado o tema e sua delimitação, os objetivos geral e específicos, as justificativas, o problema e premissas associadas, a metodologia e a presente estrutura.

Nos capítulos 2 e 3 é apresentada uma fundamentação teórica sobre os SIS e são destacadas as diferenças entre os sistemas de controle e de segurança. Os diferentes níveis de integridade de segurança, bem como suas particularidades são também abordadas.

Tecnologias, topologias e aplicações de SIF estão expostas no capítulo 4, onde também é apresentado o projeto de Funções Instrumentadas de Segurança com utilização da tecnologia Foundation Fieldbus.

Para finalizar, no capítulo 5 são mostradas as conclusões e sugestões para próximos trabalhos.

2 FUNDAMENTAÇÃO TEÓRICA

No capítulo 2 são apresentadas as definições do nível de integridade de segurança, a técnica LOPA para análise dos riscos de processo e seleção do Nível de Integridade de Segurança requerido, conceitos e especificidades referentes à PLCs, SDCDs e SIS. São também iniciadas as abordagens sobre os regulamentos, parada segura, requisitos do SIS e tolerância a falhas.

2.1 SIL

Nível de Integridade de Segurança – SIL é um critério de desempenho para as SIF que define a probabilidade de não realizar a função especificada, quando demandada (CENTER..., 2001). Os Níveis de Integridade de Segurança existentes com as respectivas probabilidade média de falha sob demanda (PFDavg) e os Fatores de Redução de Risco (RRF) são apresentados na tabela 1.

Tabela 1 – PFD e RRF para cada Nível de Integridade de Segurança (SIL)

SIL	Probabilidade média de falha sob demanda	Fator de Redução de Risco
4	$10^{-5} \leq PFD < 10^{-4}$	$10.000 < RRF \leq 100.000$
3	$10^{-4} \leq PFD < 10^{-3}$	$1.000 < RRF \leq 10.000$
2	$10^{-3} \leq PFD < 10^{-2}$	$100 < RRF \leq 1.000$
1	$10^{-2} \leq PFD < 10^{-1}$	$10 < RRF \leq 100$
0	$10^{-1} \leq PFD$	$RRF \leq 10$

Fonte: adaptado de CENTER... (2001)

2.1.1 SIL 0

As SIF que apresentam PFD menor que 0,1 ou seja, aquelas que requerem uma redução de risco inferior ou igual a 10, são consideradas SIL 0. Somente neste casos a IEC 61511-1 (INTERNATIONAL..., 2003) e a N 2595 (COMISSÃO..., 2011) admitem a utilização do SDCD ou BPCS para implementação das Funções Instrumentadas de Segurança – SIF.

2.1.2 SIL 1

Com PFD entre 0,01 e 0,1, estas SIFs são normalmente implementadas com sensor, resolvedor de lógica e elemento final de controle únicos (CENTER..., 2001).

2.1.3 SIL 2

As SIFs com $10^{-3} \leq PFD < 10^{-2}$ são tipicamente implementadas com redundância total dos sensores, dos resolvedores de lógica e dos elementos finais de controle (CENTER..., 2001).

2.1.4 SIL 3

As SIF que requerem $10^{-4} \leq PFD < 10^{-3}$ são tipicamente implementadas com redundância total dos sensores, dos resolvedores de lógica e dos elementos finais de controle (CENTER..., 2001). Para alcançar o desempenho requerido por tais funções devem ser elaborados projetos cuidadosos e estabelecidas rotinas freqüentes de testes. Muitas companhias têm um número limitado de malhas SIL 3 devido ao alto custo normalmente associado à esta estrutura.

2.1.5 SIL 4

As aplicações com o maior Nível de Integridade de Segurança – SIL previsto nas normas, requerem $10^{-5} \leq PFD < 10^{-4}$. Devido à dificuldade em alcançar e manter níveis de performance tão elevados durante o ciclo de vida do SIS, devem ser evitadas SIFs com SIL 4. Se o resultado da análise indicar este nível de segurança, devem ser estudadas mudanças no processo para aumentar a segurança intrínseca e adicionadas camadas extras de proteção com vista a reduzir o SIL da Função Instrumentada de Segurança conforme recomendação da IEC 61511-1 (INTERNATIONAL..., 2003).

2.2 LAYERS OF PROTECTION ANALYSIS – LOPA

Acidentes ocorrem quando eventos com reduzida probabilidade são combinados. A prevenção pode ser obtida pelo uso de camadas de proteção independentes que dificultam a propagação de eventos perigosos e reduzem o risco do processo para níveis aceitáveis. Aumentar o número de camadas de proteção reduz a probabilidade de acidentes, porém é mais efetivo investir no aumento da segurança intrínseca do processo (GRUHN; CHEDDIE, 2006).

Grandes máquinas e equipamentos são projetados para serem inerentemente seguros, terem alta confiabilidade e onde necessário são protegidos por camadas de proteção compatíveis com os riscos. Devido às solicitações dinâmicas em períodos de instabilidade do processo ou paradas abruptas mecanismos de falhas são iniciados ou acelerados. A IEEE Std 493 (INSTITUTE..., 2007, p. 259) indica algumas falhas elétricas que poderiam levar a tempo de parada de até 48 horas.

Finkel et al (2006) citam uma variedade de técnicas para análise dos riscos de processo e seleção do Nível de Integridade de Segurança (Safety Integrity Level – SIL) de cada função de segurança. Assim como Mitchell e Herena (2010), citam a preferência pela técnica semiquantitativa, chamada Análise das Camadas de Proteção (Layers of Protection Analysis – LOPA).

A metodologia LOPA foi desenvolvida para determinar se existem camadas independentes de proteção (IPLs) suficientes para os cenários acidentais identificados na análise de riscos, considerando a freqüência dos eventos iniciadores, severidade das conseqüências e probabilidade de falha das IPLs (CENTER..., 2001).

As camadas de proteção devem ser efetivas em prevenir ou mitigar as conseqüências de um evento perigoso, ser independentes de outras IPLs associadas com o perigo identificado e devem ser projetadas para facilitar validações regulares das funções de proteção (CENTER..., 2001). Na figura 2 são mostradas camadas de proteção típicas, conforme a IEC 61511-3 (INTERNATIONAL..., 2003).

Na tabela 2 são mostrados alguns exemplos de valores de risco presente no processo ou tolerado em tais indústrias.

Tabela 2 – Freqüência típicas para eventos iniciadores

Evento	Faixa de freqüência (por ano)	Exemplo de valor escolhido por uma indústria (por ano)
Falha de tanque atmosférico	10^{-3} a 10^{-5}	10^{-3}
Falha de selo de bomba	10^{-1} a 10^{-2}	10^{-1}
Falha em vaso de pressão	10^{-5} a 10^{-7}	10^{-6}
Falha de malha de instrumentação em BPCS	10^{-1} a 10^{-2}	10^{-1}

Fonte: adaptado de CENTER... (2001)

Valores máximos típicos de risco tolerado por algumas empresas e típicos utilizados como critério para a aplicação da técnica LOPA são apresentados na Tabela 3. As tabelas 1, 2 e 3 devem ser lidas em conjunto pois riscos como os indicados na tabela 2 devem ser reduzidos para valores como os da tabela 3 por meio da adição de camadas de proteção tais como SIS, que contribuem com valores constantes na tabela 1 (CENTER..., 2001).

Tabela 3 – Riscos tolerados e critério para uso em LOPA

Fonte	Máximo risco tolerado para a força de trabalho	Risco desprezível para a força de trabalho
Health & Safety Executive, UK (indústrias existentes)	10^{-3}	10^{-6}
Shell (onshore e offshore)	10^{-3}	10^{-6}
BP (onshore e offshore)	10^{-3}	10^{-6}
Critério para LOPA Todos os cenários afetando um indivíduo	10^{-3}	10^{-5}
Critério para LOPA Qualquer cenário afetando um indivíduo	10^{-4}	10^{-6}

Fonte: adaptado de CENTER... (2001)

Deve ser observado que a diversificação das camadas de segurança evita a ocorrência de modos de falha comuns entre as camadas de proteção. A combinação de funcionalidades em uma única camada de proteção tem como resultado a degradação da segurança, motivo pelo qual o uso de SIFs com SIL 3 e 4 são reduzidos e raros respectivamente. Além do custo do ciclo de vida ser alto, pode-se obter a mesma redução de risco provida por SIL 3 pela adição de camadas SIL 2 associada a outra camada de proteção, tal como o uso de dispositivos mecânicos (GRUHN; CHEDDIE, 2006).

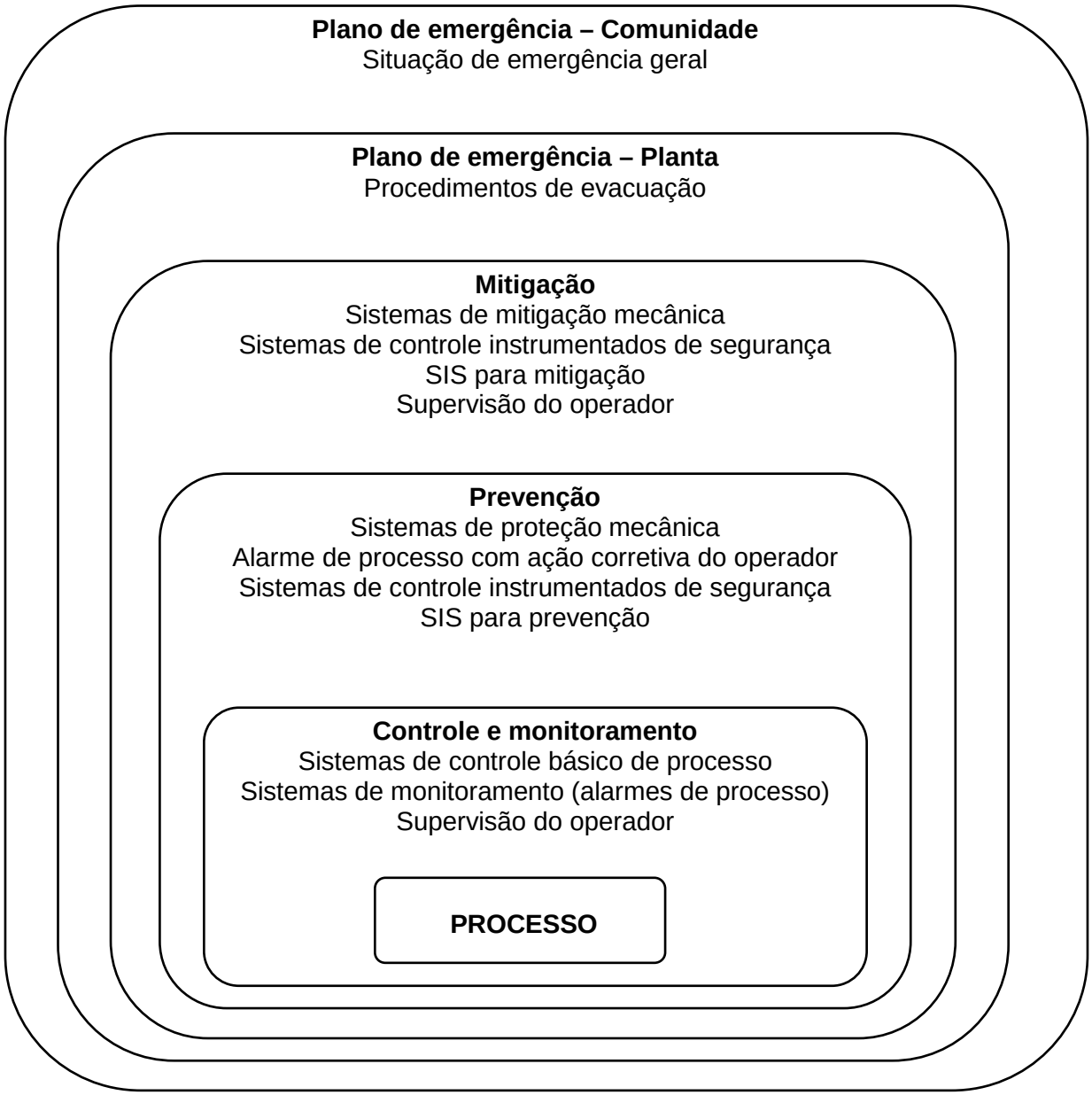

Figura 2: Métodos típicos de redução de riscos em plantas de processo
Fonte: adaptado de IEC 61511-3 (INTERNATIONAL..., 2003)

Apesar de pequenas variações encontradas na bibliografia e regulamentos consultados, as camadas de controle e monitoramento, prevenção, mitigação e planos de emergência para a planta e comunidade são recorrentes. O número de camadas de proteção, definido pela natureza do processo e pela redução de risco necessária, varia em função da aplicação e deve iniciar da camada mais central. Dependendo do processo e da segurança obtida com outras camadas de proteção a instalação de SIS pode não ser requerida, motivo pelo qual devem ser criteriosas as análises de risco do processo e de viabilidade das medidas de redução de risco.

2.3 SEPARAÇÃO ENTRE CONTROLE E INTERTRAVAMENTO

Como exemplos de camadas de proteção, podem ser citados os sistemas de controle, monitoramento e os SIS.

Apesar da aparente similaridade dos sistemas de supervisão e controle e dos sistemas de intertravamento, Gruhn e Cheddie (2006) contestam a tese de que sistemas de controle de processo são confiáveis e redundantes o suficiente para executarem funções de intertravamento. Assim como Finkel et al (2006) reiteram que os padrões, práticas recomendadas e diretrizes da indústria recomendam a separação dos sistemas de controle e de segurança, destacando as orientações emanadas pelas organizações IEC, API, HSE, AIChE, ANSI/ISA, NFPA e IEEE.

Como exceção pode-se citar os sistemas de controle instrumentado de segurança, nos quais não é possível dissociar controle e segurança. Segundo a IEC 61511-1 (INTERNATIONAL..., 2003) tais sistemas são raros na indústria de processo e quando necessários são tratados como casos especiais e demandam projeto específico.

Além do atendimento aos requisitos aplicáveis aos Sistemas de Controle Instrumentados de Segurança, deve ser demonstrado que o sistema é capaz de atingir o desempenho de segurança especificado. Um exemplo desta condição especial são os sistemas de controle e de segurança de aviões, nos quais a sobreposição das funções de controle e segurança demanda a utilização de sistemas de segurança para ambos (GRUHN; CHEDDIE, 2006).

No caso de navios, que possuem regulamentação e características bem específicas, a IEC 60092-504 (INTERNATIONAL..., 2001) também determina a segregação das funções de segurança e de controle:

> 4.3 Segregação
>
> …
>
> Funções de proteção (segurança) devem ser independentes de funções de controle e monitoramento (alarme). Quando praticável (exeqüível), funções de controle e monitoramento (alarme) devem ser também independentes. Sistemas reservas (*stand by*) ou outro arranjo de redundância devem ser funcionalmente independentes…
>
> (Tradução nossa)

Para a indústria de processo as especificações dos sistemas consideram requisitos e características específicas do setor. Gruhn e Cheddie (2006, p. 34), afirmam que o controle de processo deve ser ativo, dinâmico e permitir mudanças freqüentes. No entanto os sistemas de segurança tipicamente são passivos, dormentes e exigem a restrição e o controle de mudanças.

Ressalvas devem ser feitas à utilização de sistemas de controle para executar Funções Instrumentadas de Segurança com SIL menor ou igual à 1, conforme previsto na IEC 61511-1 (INTERNATIONAL..., 2003) e na N 2595 (COMISSÃO..., 2011).

2.4 SISTEMA DIGITAL DE CONTROLE DISTRIBUÍDO

Para posicionar o leitor, nas comparações entre sistemas de controle e intertravamento, o Sistema Digital de Controle Distribuído – SDCD é brevemente apresentado, destacando somente alguns conceitos e características principais.

2.4.1 Conceito

O SDCD é um sistema de controle industrial microprocessado. Concebido para substituir controladores analógicos, os sistemas atuais possuem funcionalidades diversas tais como controle de bateladas e controle estatístico de processos (FINKEL et al, 2006).

Segundo FINKEL et al (2006) um SDCD é formado pelas interfaces do sistema com o processo, do sistema com o operador e pela comunicação entre estas interfaces.

2.4.2 Características e aplicações

SDCDs e outros sistemas de controle de processos também se enquadram na definição de Basic Process Control System – BPCS, que são sistemas que monitoram e controlam o processo continuamente (CENTER..., 2001).

Segundo o Center for Chemical Process Safety – CCPS, o BPCS possibilita três diferentes tipos de funções de segurança que podem ser consideradas como camadas independentes de proteção:

- mantém o processo nas condições normais, continuamente;
- identifica condições anormais de processo e alerta o operador;
- realiza ação automática para parar o processo ou retornar às condições normais de operação.

Como exemplo, na figura 3 é apresentada uma visão geral da arquitetura de um SDCD, o sistema DeltaV (EMERSON PROCESS, 2012 b). Segundo informações disponibilizadas no sítio do fabricante, o sistema permite aplicações avançadas (PID, fuzzy, preditivo e redes neurais) e integração com dispositivos e outros sistemas. Com *hardware* composto basicamente por estações de trabalho, controladores e cartões de I/O na figura 3 são destacados:

1 – Rearranjo eletrônico: desacopla o projeto de infra estrutura de I/O do projeto da estratégia de controle, flexibilizando ampliações e alterações.

2 – Controladores da Série S: oferece todas as características e funções da série M com o suporte adicional para o rearranjo eletrônico.

3 – Controladores da Série M: executa estratégias de controle que ajudam a otimizar o processo em configurações simples ou redundantes.

4 – Cartões I/O DeltaV Wireless e link de campo: totalmente redundantes e possibilitam comunicação com a instrumentação Smart Wireless.

5 – Cartões de I/O: subsistema modular provado e projetado para ser instalado próximo aos dispositivos de campo.

6 – Sistema de segurança DeltaV SIS: certificado conforme IEC 61508, ajuda a alcançar a segurança de processo necessária monitorando continuamente a malha de segurança inteira para atuar sob demanda e prevenir paradas espúrias.

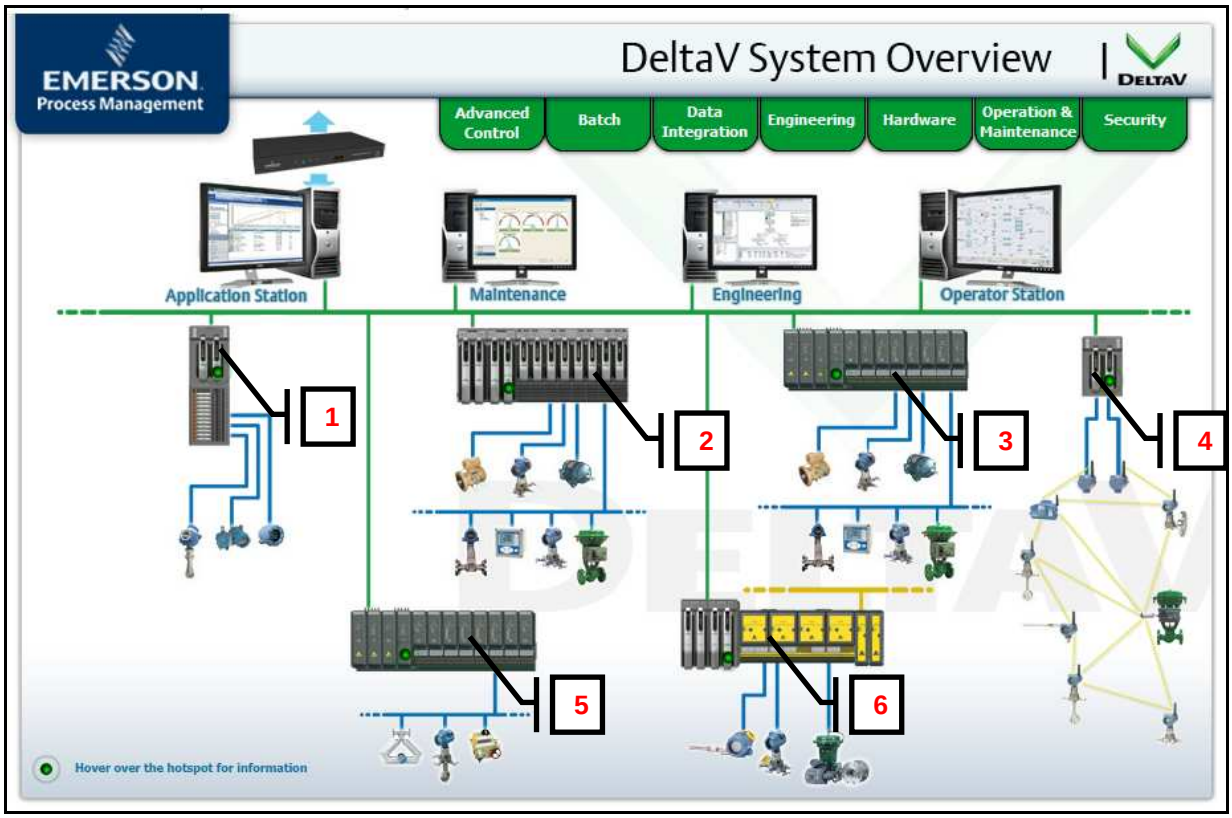

Figura 3: Visão Geral do Sistema DeltaV
Fonte: Emerson Process (2012 b)

2.5 PLCs APLICADOS EM SIS

De acordo com a norma IEC 61131-1 (INTERNATIONAL..., 2003) um Controlador Lógico Programável (CLP ou do inglês PLC) é um sistema eletrônico, projetado para aplicações industriais que possui memória programável para armazenamento de instruções e que executa funções tais como lógica, seqüenciamento, temporizações e contagens para controlar através de suas entradas e saídas máquinas ou processos.

A estrutura geral de um PLC, segundo a IEC 61131-1 (INTERNATIONAL..., 2003) é apresentada na figura 4. As funções comunicam entre si e com o processo ou equipamentos controlado.

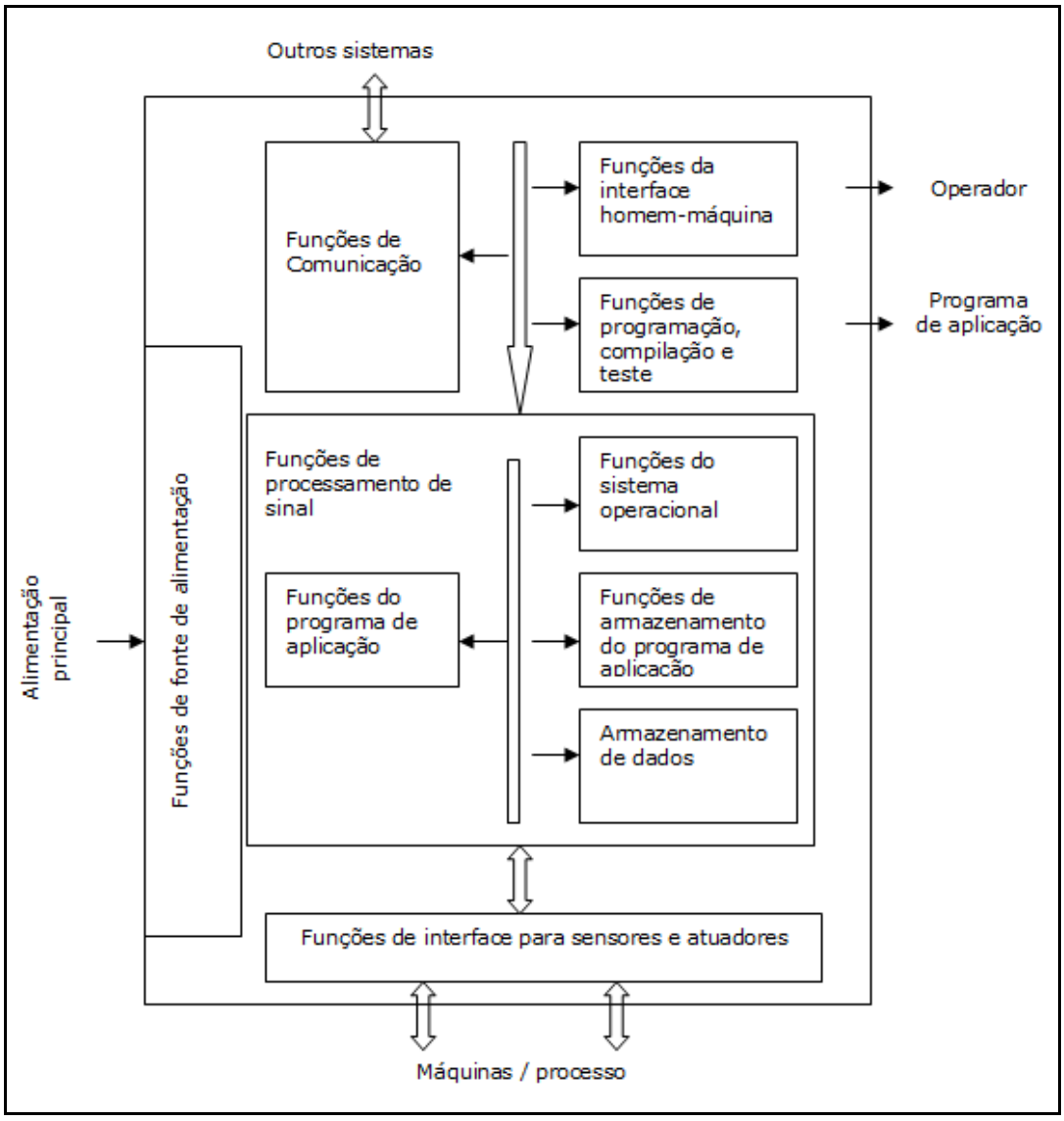

Figura 4: Estrutura funcional básica de um PLC
Fonte: adaptado de IEC 61131-1 (INTERNATIONAL..., 2003)

Segundo a IEC 61131-1 (INTERNATIONAL…, 2002), a função da CPU consiste da execução das funções do programa de aplicação e do armazenamento do programa de aplicação, de dados e do sistema operacional. A CPU processa sinais obtidos dos sensores, assim como dados internos e gera sinais para os atuadores ou para posições de memória. As interfaces com os sinais de entrada e de saída do PLC compatibilizam os sinais externos com os níveis de sinais processados pelo PLC. Enquanto as funções de comunicação executam a troca de dados com outros sistemas ou equipamentos, a interface homem máquina provê interação do operador com o processo ou máquina. A geração, carga, monitoramento, teste e compilação são executadas por funções específicas, assim como a alimentação elétrica do PLC.

No caso de aplicações de PLC em SIS, devem ser aplicadas as normas específicas tais como a IEC 61508 (INTERNATIONAL..., 2010). É escopo da citada Norma tratar de sistemas elétricos, eletrônicos e eletrônicos programáveis (E/E/PE) quando estes são utilizados em funções de segurança, bem como orientar a elaboração de padrões para setores específicos.

Para aplicação de SIS nas indústrias de processo a IEC 61511-1 (INTERNATIONAL..., 2003) estabelece os requisitos para especificação, projeto, instalação e manutenção de SIS, com o objetivo de tornar ou manter o processo em um estado seguro.

A figura 5 apresenta a arquitetura de SIS que segue a seguinte hierarquia: *hardware* e *software* empregados na medição das condições de processo (sensores), na execução de lógica e na atuação no processo (elementos finais), conforme a IEC 61511-1 (INTERNATIONAL..., 2003). Tanto os sensores e elementos finais quanto o resolvedor de lógica podem ser programáveis ou não e sua especificação deve ser feita de modo a alcançar o SIL requerido para a SIF.

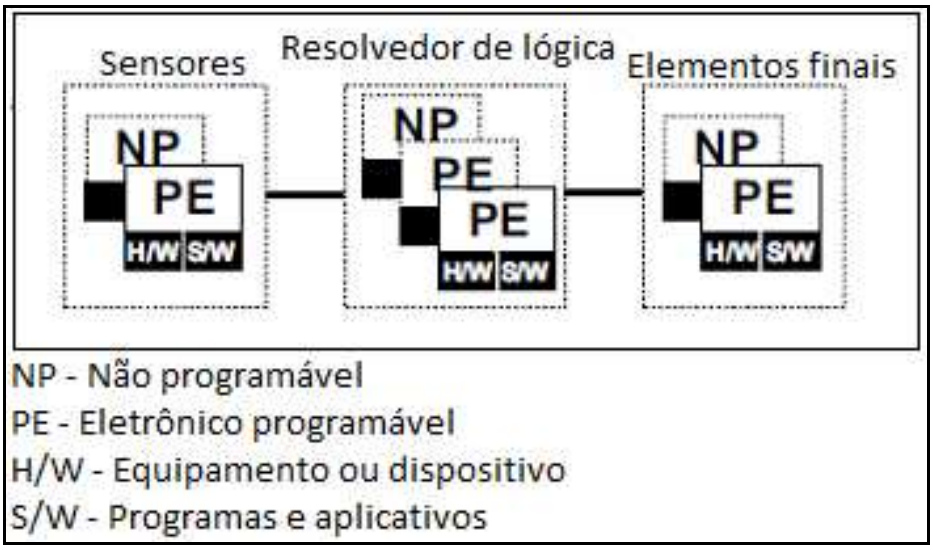

Figura 5: Exemplo de arquitetura de SIS
Fonte: adaptado de IEC 61511-1 (INTERNATIONAL..., 2003)'

2.6 REGULAMENTOS

Perdas de vidas humanas, de instalações, de equipamentos e de produção bem como a contaminação do meio ambiente contribuíram para a evolução das normas, regulamentos e para o desenvolvimento de sistemas de segurança, segundo Finkel et al (2006). Além destes fatores, danos à imagem e eventuais multas representam elevados custos que viabilizam os custos do ciclo de vida do SIS (GRUHN; CHEDDIE, 2006).

Gruhn e Cheddie (2006) afirmam que o desenvolvimento de padrões pela indústria tem como objetivo evitar a intervenção do governo e teve início após a ocorrência de vários desastres em plantas de processo americanas, nas décadas de 80 e 90. Destacam também os padrões utilizados pela indústria:

- Programmable Electronic Systems In Safety Related Applications, Parts 1 & 2, U.K. Health & Safety Executive: este foi o primeiro padrão sobre o tema, publicado em 1987.
- Guidelines for Safe Automation of Chemical Process, AIChE: este padrão cobre o projeto de SDCD e SIS, e foi elaborado pelo Center for Chemical Process Safety – CCPS, entidade criada pelo AIChE depois do acidente em Bopal, na India.
- Boiler and Combustion Systems Hazard Code, National Fire Protection Association NFPA 85: considerado como o padrão mais reconhecido no mundo para segurança de sistemas de combustão.
- Recomended Practice for Instrumentation and Control Systems for Fired Heaters and Steam Generator, API RP 556; o documento se apresenta como aplicável de forma integral em plantas químicas, plantas de gasolina e instalações similares.
- Recommended Practice for Design, Installation and Testing of Basic Surface safety Systems for Offshore Production Platforms, API RP 14C: práticas recomendadas prescritivas *(proven practices)* elaboradas para engenheiros de projeto e equipes de operação.
- Process Safety Management of Highly Hazardous Chemicals OSHA 29 CFR 1910.119: a OSHA reconheceu a ANSI/ISA-84.00.01-1996 como

um conjunto de boas práticas para SIS e que a conformidade com este padrão equivale à aderência aos requisitos de Gerenciamento de Segurança de Processo da OSHA para SIS.

- Standard Criteria for Safety Systems for Nuclear Power Generating Systems IEEE 603-2009: estabelece os critérios mínimos de projeto e funcionamento para sistemas de segurança em centrais nucleares.
- Identification of Emergency Shutdown Systems that are Critical to Maintaining Safety in Process Industry ANSI/ISA 91.00.01-2001: este padrão inclui definições de BPCS, sistemas de parada de emergência e controle crítico de segurança. Controles do tipo Safety Critical Control são aqueles que não possuem proteção de retaguarda, ou seja, cuja falha resultaria em evento perigoso.
- Functional Safety – Safety Related Systems, IEC 61508: este padrão cobre o uso de relés, estado sólido e sistemas programáveis, incluindo dispositivos de campo. Este padrão se aplica à todas as indústrias (transportes, médica, nuclear, processo, etc) e foi elaborado para orientar o desenvolvimento de padrões específicos.
- Functional Safety: Safety Instrumented Systems for the Process Industry Sector, ISA 84.00.01-2004 Parts 1 &3 (IEC 61511 Mod). A IEC desenvolveu a IEC 61511 a partir da ANSI/ISA-84.01-1996. Posteriormente a ISA adotou a IEC 61511, acrescentando cláusulas regulatórias oriundas da versão escrita em 1996.

2.7 SIS - REQUISITOS

Nesta seção são abordados requisitos de SIS, tais como confiabilidade, diagnósticos, disponibilidade e redundâncias.

2.7.1 Parada segura

Finkel et al (2006) afirmam que há vários conceitos errôneos amplamente difundidos em relação à SIS. Por exemplo, nem todo processo reverte a uma condição segura quando é cortada a alimentação elétrica, pois podem ser necessários equipamentos para circulação de fluido de refrigeração ou de purga de gases inflamáveis.

Segundo a IEC 61511-1 (INTERNATIONAL..., 2003), para toda função de segurança deve ser identificado um estado seguro que é aquele onde foram eliminados os riscos considerados inaceitáveis. Como resultado desta análise é estabelecido na fase de projeto o conjunto de ações a serem desencadeadas quando os limites forem excedidos, para cada cenário.

2.7.2 Confiabilidade

Devido à freqüência das variações e das atuações constatadas no controle contínuo, eventuais anomalias são rapidamente detectadas. No caso de SIS, a maior parte dos sistemas permanecem passivos, até que seja demandada sua atuação. FINKEL et al (2006) afirmam também que determinados instrumentos permanecem longos períodos sem demanda, tendo sua atuação verificada somente nas rotinas de testes periódicos estabelecidas no projeto do SIS.

Cita também que um sistema de controle tem dois estados possíveis: ou está funcionando corretamente ou caso apresente falha estará em manutenção. No caso de SIS além da condição normal o sistema pode apresentar falha segura ou falha oculta. Enquanto falhas seguras levam o sistema para a condição de segurança e resultam em perda de produção, falhas ocultas (inseguras) farão com que o SIS, quando demandado, não atue conforme projetado podendo resultar em acidente. Esta distinção entre as características dos sistemas de controle e de segurança leva a requisitos mais severos para o ciclo de vida do SIS (FINKEL et al, 2006).

2.7.3 Diagnósticos

São necessários para detectar falhas perigosas que poderiam impedir o SIS de realizar suas funções. A capacidade que um sistema ou subsistema possui para detecção automática de falhas pelo sistema representa o nível de cobertura do diagnóstico. Para estimar o nível de cobertura de diagnósticos, bem como dos modos de falha e seus efeitos, foi desenvolvida a técnica Failure Modes, Effects and Diagnostic Analysis – FMEDA (GRUHN; CHEDDIE, 2006).

2.7.4 Disponibilidade

Para evitar confusão causada por ranges típicos da ordem de 99% a 99,9999%, em termos de segurança normalmente se usa o complemento da disponibilidade, que é expressa pela probabilidade de falha sob demanda (PFD). O manuseio de números muito baixos pode ser contornado pela utilização do Fator de Redução de Risco – RRF que numericamente é o inverso do PFD (GRUHN; CHEDDIE, 2006).

2.7.5 Redundâncias

Gruhn e Cheddie (2006) afirmam que sistemas duais podem não ser melhores que sistemas únicos, assim como os triplos podem ser piores que os duais. Sistemas redundantes podem ser muito seguros, no entanto os sistemas têm seu desempenho afetado pelas paradas indesejadas dos sistemas não redundantes, eventualmente potencializadas.

Finkel et al (2006) citam casos em que além de ser requerida segurança elevada, devem ser evitadas falhas espúrias, por estas acarretarem riscos e perdas de produção. Para tais casos fabricantes desenvolveram equipamentos eletrônicos de lógica redundante e múltiplos, com alto nível de diagnósticos.

Uma solução adotada pela indústria para tornar os sistemas mais seguros e ao mesmo tempo reduzir paradas indesejadas é a Triple Modular Redundancy – TMR. Estes sistemas, utilizados em resolvedores de lógica de SIS, são basicamente PLCs especializados triplicados e podem permanecer operando apesar de haver alguma falha, ou seja possuem tolerância a falhas. Nesta configuração, mostrada na figura 6, são utilizadas três CPUs que fazem votação 2oo3 (dois de três) para definir a ação (GRUHN; CHEDDIE, 2006).

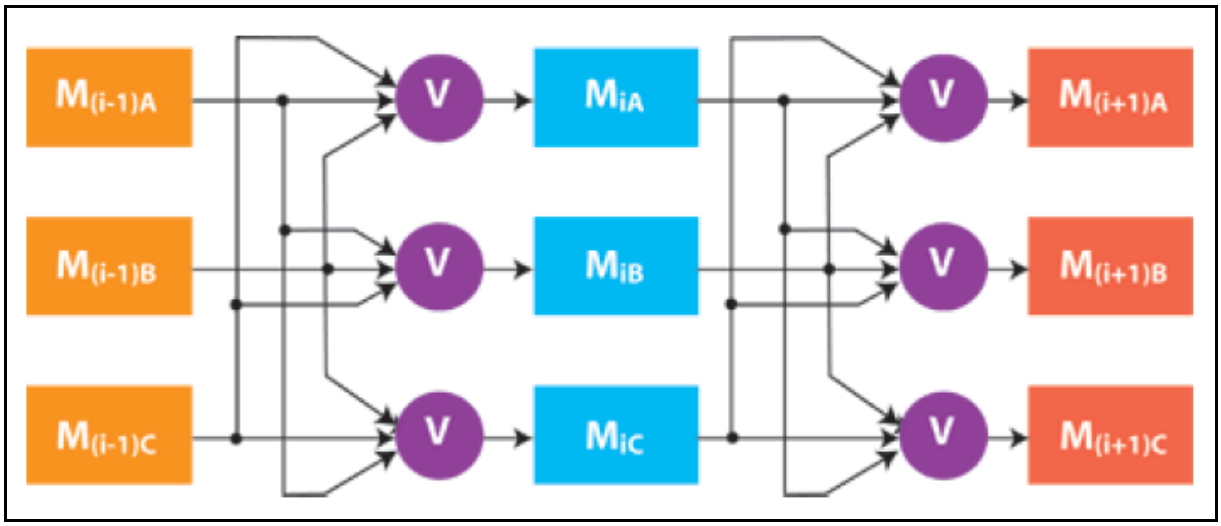

Figura 6: Configuração TMR
Fonte: Sheble (2012)

Para que um evento seja iniciado é necessária a indicação de dois dos três sensores simultaneamente, assim como é verificada a ocorrência de pelo menos duas saídas coincidentes dos resolvedores de lógica para a efetiva atuação dos elementos finais. Face os avanços dos sistemas programáveis, uma série de funcionalidades estão disponíveis via configuração.

Além da tolerância à falhas, que é a capacidade de um sistema ou subsistema realizar as funções requeridas na presença de um número limitado de componentes em falha (MITCHELL; HERENA, 2010), a configuração TMR permite a operação segura, ainda que em modo degradado, com a retirada de operação temporária de um dos ramos seja em falha ou para intervenção da manutenção.

Segundo BECKMAN (1998) os diagnósticos funcionais apresentam notáveis vantagens por serem confiáveis e determinísticos. Na configuração TMR é realizada, com o auxílio do diagnóstico a verificação de eventuais discrepâncias e realizada a votação em cada ciclo de execução do programa.

3 CICLO DE VIDA DO SIS

Gruhn e Cheddie (2006) indicam que além da proteção das pessoas devem ser consideradas as perdas de produção, danos a equipamentos e instalações e contaminações do meio ambiente para justificar a instalação de SIS. Complementarmente devem ser analisados os níveis de integridade de segurança selecionados, a confiabilidade requerida e os custos do ciclo de vida do SIS. Modelos de confiabilidade e análise de custo do ciclo de vida são indicados como ferramentas para justificar o projeto e a instalação de SIS.

A IEC 61511-1 (INTERNATIONAL..., 2003) requer que sejam definidos, para todas as fases do ciclo de vida do SIS, critérios, técnicas, medidas e procedimentos para gerenciar o processo, assegurar a integridade de segurança e garantir que os requisitos do SIS sejam alcançados nos diferentes modos de operação.

Para visualizar um exemplo completo de aplicação das fases do ciclo de vida pode ser consultada a ISA-TR84.00.04-2005 Part 2 (INSTRUMENTATION..., 2005), que apresenta uma planta de produção de PVC.

As pequenas alterações propostas por Finkel et al (2006), Gruhn e Cheddie (2006), Mitchell e Herena (2010) não alteram a essência do ciclo de vida indicado na IEC 61511-1 (INTERNATIONAL..., 2003), apresentado neste capítulo.

3.1 AVALIAÇÃO DE PERIGOS E REDUÇÃO DE RISCOS

Finkel et al (2006) relatam a evolução dos SIS nas últimas décadas, motivado pela investigação de acidentes e da consciência de que acidentes podem e devem ser evitados.

Os processos produtivos devem ser projetados para serem inerentemente seguros. Entretanto nos processos produtivos industriais estão presentes quantidades de energias e variedade de substâncias que representam risco às instalações, à saúde das pessoas ou ao meio ambiente (MITCHELL; HERENA, 2010).

Com o objetivo de trazer o risco inerente do processo para os limites considerados toleráveis, são acrescentadas camadas de proteção que têm seus fatores de redução de risco adicionados, conforme a figura 7 (N 2595, COMISSÃO..., 2011).

Na identificação e avaliação dos riscos do processo, são mapeados os eventos que podem resultar em situações perigosas e os requisitos para a redução de risco. Tal objetivo pode ser obtido por meio de controles administrativos, sistemas de proteção mecânica, de monitoramento e controle, e SIS utilizados em conjunto ou isoladamente, conforme a IEC 61511-1 (INTERNATIONAL..., 2003).

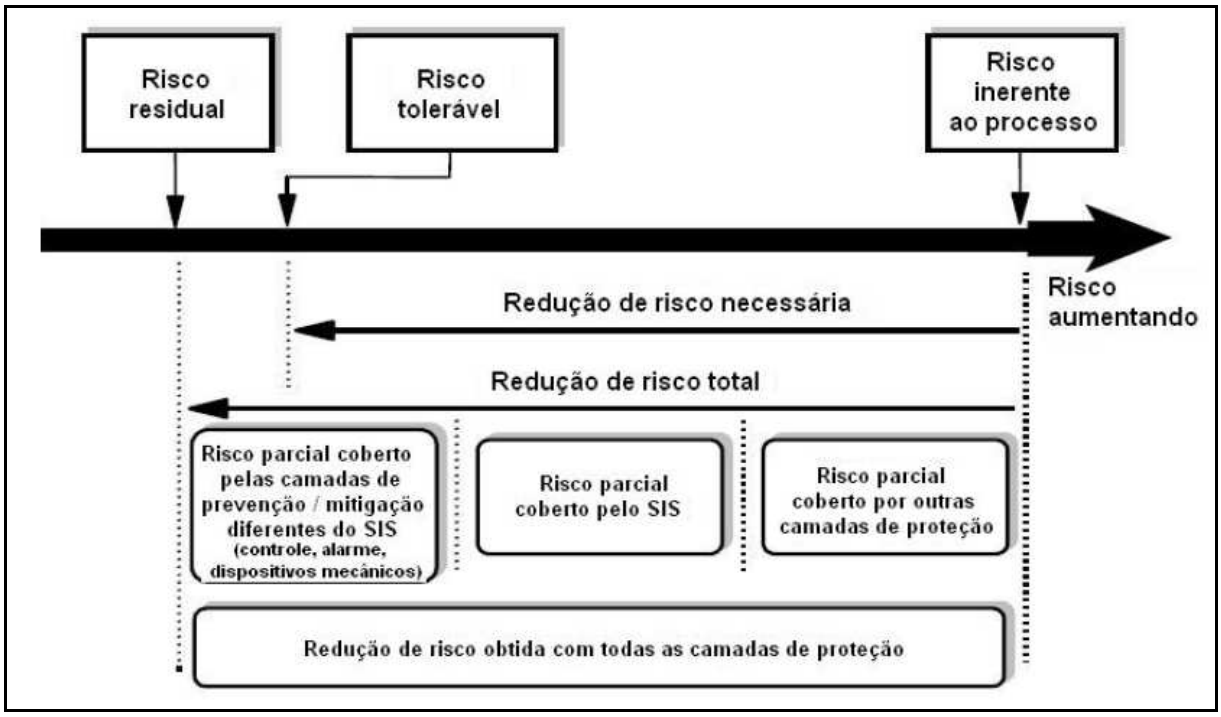

Figura 7: Redução de risco
Fonte: N 2595 (COMISSÃO..., 2011)

Após a redução de risco obtida pela inclusão de camadas independentes de proteção, o remanescente é conhecido como risco residual. Finkel et al (2006) afirmam que um paradigma que está mudando é a busca pela segurança absoluta e que neste contexto foi disseminada a metodologia As Low As Reasonably Practicable – ALARP (Tão Baixo Quanto Razoavelmente Praticável).

Segundo Gruhn e Cheddie (2006) o ALARP se baseia em três níveis de risco (inaceitável, tolerável e aceitável) e seus aspectos econômicos associados. Riscos considerados inaceitáveis devem ser reduzidos a níveis adequados. Os

riscos toleráveis devem ser reduzidos até o ponto em que a relação custo benefício permaneça favorável. Riscos considerados aceitáveis devem ser acompanhados para assegurar que permaneçam nesta região, não demandando ações adicionais.

3.2 ALOCAÇÃO DE FUNÇÕES DE SEGURANÇA

A IEC 61511-1 (INTERNATIONAL..., 2003) determina a avaliação de falhas dependentes, assim como de causas e modos de falha comuns entre camadas de proteção e estabelece como objetivos desta fase identificar as SIFs e determinar para estas o SIL requerido. A figura 8 mostra o relacionamento entre as SIFs e as demais funções de segurança.

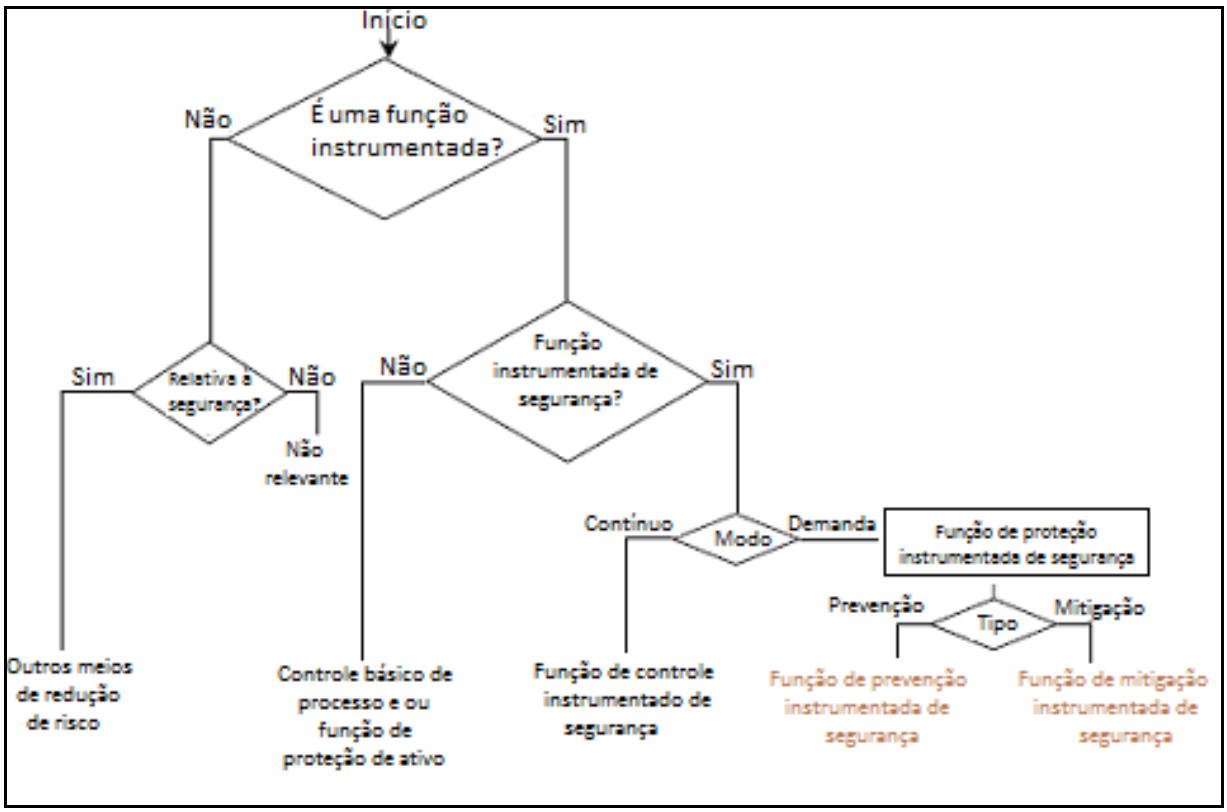

Figura 8: Relacionamento entre SIFs e outras funções
Fonte: adaptado de IEC 61511-1 (INTERNATIONAL..., 2003)

A alocação de funções de segurança para camadas de proteção específicas tem como propósito o controle, a prevenção ou mitigação de perigos do processo e

seus equipamentos. O estabelecimento do SIL de uma Função Instrumentada de Segurança depende da redução de risco requerida por esta função.

3.3 ESPECIFICAÇÃO DOS REQUISITOS DE SEGURANÇA DO SIS

Gruhn e Cheddie (2006) informam que na análise de 34 acidentes causados diretamente por falhas em sistemas de segurança e controle em diversas indústrias, especificações incorretas ou incompletas causaram 44% dos acidentes.

De acordo com a IEC 61511-1 (INTERNATIONAL..., 2003) os requisitos de segurança devem ser claros, precisos, verificáveis, exeqüíveis e possíveis de manter para todo o ciclo de vida do SIS. Devem conter as descrições dos modos de operação da planta e do monitoramento do processo pelo SIS, assim como a duração dos eventos e os tempos de resposta requeridos.

Pontos de ajuste, requisitos específicos do *hardware* e *software* de segurança e a sistemática para controle de alterações no SIS (desvios e inibições) são elementos a serem especificados. Para os modos de falha identificados devem ser estabelecidos intervalos de testes funcionais compatíveis com a redução de risco especificada.

3.4 PROJETO E CONSTRUÇÃO DO SIS

A IEC 61511-1 (INTERNATIONAL..., 2003) estabelece requisitos para projeto de um ou múltiplos SIS para atingir o desempenho especificado. Onde o SIS é utilizado para implementar funções de segurança e de controle, todo o *hardware* e *software* que possam afetar negativamente qualquer SIF em condições normais ou de falha deve ser tratado de forma a atingir o maior SIL requerido, devendo ser verificado por meio de cálculos.

O projeto deve prever facilidades para a realização dos testes, parciais ou totais. Nos casos em que os intervalos para paradas de manutenção da planta de processo são maiores que os intervalos de teste das SIFs, testes *on line* são

necessários. Imposição de valores às entradas ou saídas não devem ser usadas como parte do *software* de aplicação ou do procedimento de manutenção.

Para subsistemas que não falham de forma segura, em caso de falta de energia elétrica, devem ser previstas fontes de energia confiáveis e redundantes (baterias ou UPS), além de medidas como, monitoramento, diagnóstico, alarme, comunicação, proteção e comutação automática de fontes de energia.

Os componentes do SIS podem ser selecionados com base em aplicações anteriores desde que sua efetividade seja comprovada por meio de documentação compatível com a complexidade da aplicação e atendimento aos requisitos de projeto e normativos.

Os sensores, resolvedores de lógica e elementos finais devem ter uma tolerância mínima à falhas de *hardware*, ou seja, continuar operando ainda que na presença de uma ou mais falhas. Este parâmetro representa a mínima redundância do sistema ou componente. A adequação dos componentes selecionados para aplicação em SIS com SIL 1, 2 ou 3 deve ser comprovada pelos fabricantes, com apresentação da documentação certificada relativa ao *hardware* e *software* embarcados.

Os dispositivos de campo devem ser selecionados e instalados visando a minimização de falhas durante o ciclo de vida. Condições ambientais como corrosão, intempéries, temperatura e pressão extremas, sólidos em suspensão, condensação, obstrução, dentre outras devem ser previstas e medidas preventivas adequadas e suficientes adotadas.

Cada elemento de campo deve ter sua fiação individual para a entrada ou saída do SIS, exceto quando se tratar de múltiplos sensores discretos ligados em série monitorando a mesma variável ou múltiplos elementos finais conectados à uma única saída ou um barramento de comunicação digital.

Sensores inteligentes devem ser protegidos para prevenir modificações não autorizadas ou inadvertidas, considerando os fatores humanos.

As interfaces de comunicação e homem-máquina podem incluir, mas não se limitar às interfaces de operação, de manutenção, de engenharia e de comunicação. Onde a interface for feita pelo BPCS, deve ser considerada a imunidade às falhas deste sistema.

O projeto do SIS deve ser feito de forma a minimizar a necessidade de modificações temporárias (inibições ou desvios) enquanto a unidade de processo

está em partida ou em operação. Eventuais desvios das funções de segurança (*bypass*) devem ser controlados por meio de senhas de acesso e não devem impedir o funcionamento dos alarmes e a parada iniciada manualmente.

O projeto deve assegurar que qualquer falha das interfaces de manutenção, de engenharia ou com outros sistemas não comprometa a capacidade do SIS de manter ou levar o processo para um estado seguro.

A interface de comunicação deve ser robusta para manter o desempenho do SIS, mesmo em ocorrência de falha e suportar variações bruscas de energia sem provocar falhas perigosas.

3.5 INSTALAÇÃO, COMISSIONAMENTO E VALIDAÇÃO DO SIS

A IEC 61511-1 (INTERNATIONAL..., 2003) recomenda a realização de testes de aceitação do *software* e do resolvedor de lógica no fabricante, com o objetivo de identificar eventuais falhas e verificar o atendimento às especificações.

Todos os componentes do SIS deverão ser instalados e testados conforme estabelecido nos documentos de projeto e o comissionamento deve ser conduzido com o foco na validação final do sistema.

Os registros referentes ao comissionamento do SIS devem atestar os resultados dos testes e que os objetivos e critérios definidos na fase de projeto foram alcançados, bem como registrar e justificar eventuais insucessos para análise e providências.

Na fase de validação do SIS são verificados, através de inspeção e testes do SIS instalado e comissionado, o atendimento aos requisitos da especificação de segurança. O desempenho do SIS deve ser avaliado em todos os modos relevantes de operação do processo e equipamentos associados.

3.6 OPERAÇÃO E MANUTENÇÃO DO SIS

Procedimentos de operação e manutenção do SIS devem ser desenvolvidos, contendo as rotinas especificadas no projeto, o monitoramento das falhas do sistema e das taxas de demanda, a revalidação e os diagnósticos.

As equipes de operação e de manutenção do SIS devem receber treinamento e reciclagem adequados para realização de suas atividades.

O SIS deve ser testado por completo, incluindo os sensores, resolvedor de lógica e elementos finais com a freqüência definida no projeto objetivando manter a PFD média especificada. Deve ser observado que diferentes partes do SIS podem requerer intervalos de teste específicos e isto deve estar refletido no plano de manutenção.

Procedimentos de testes escritos devem ser desenvolvidos para cada SIF para revelar falhas perigosas não detectadas pelo diagnóstico. Para determinar as falhas não detectadas, que precisam ser testadas, podem ser utilizadas as técnicas de análise dos modos de falha e efeitos, exame da árvore de falhas e manutenção centrada em confiabilidade.

Periodicamente deve ser reavaliada a freqüência de testes, considerando os dados históricos de testes, a experiência com a planta, a degradação do *hardware* e a confiabilidade verificada do *software*.

O SIS deve passar por inspeção periódica para avaliar deterioração das instalações e assegurar que não foram executadas mudanças não autorizadas. Devem ser mantidos registros referentes aos testes funcionais e inspeções realizados.

Gruhn e Cheddie (2006) citam estudo em que 15% dos acidentes analisados foram causados por problemas na operação e manutenção do SIS. Introdução de defeitos durante a execução de testes ou intervenções da manutenção, bem como o uso de procedimentos não específicos para SIS são indicados como possíveis causas da falha.

3.7 MODIFICAÇÕES DO SIS

As interfaces do SIS devem ser projetadas para evitar mudanças não autorizadas no *software*. Modificações no SIS devem ser planejadas, revisadas e aprovadas antes de sua implementação.

Devem ser investigados impactos no SIS (confiabilidade, modos, freqüência e probabilidade de falhas) decorrentes de alterações realizadas em sistemas com os quais possua interface.

Procedimentos para controle e autorização de mudanças devem ser implementados antes de realizar qualquer alteração no SIS. Deve ser analisado o impacto na segurança funcional em decorrência da modificação proposta.

3.8 DECOMISSIONAMENTO

Antes de retirar definitivamente de operação um SIS, ou seja de realizar o decomissionamento, devem ser identificados os riscos e salvaguardas afetados pela intervenção, definidas as medidas de controle, planejadas as atividades e obtidas as autorizações necessárias.

Devem ser analisados possíveis impactos na segurança funcional de sistemas ou instalações próximas ou que tenham interface com o SIS.

3.9 VERIFICAÇÃO DO SIL

O objetivo da verificação é demonstrar por meio de revisão, análise e testes que os resultados obtidos satisfazem os requisitos definidos para as fases do ciclo de vida. Eventuais irregularidades precisam ser tratadas de forma sistematizada, a ser estabelecida na fase de planejamento.

A seleção de técnicas e métricas para a verificação do processo dependem dentre outros fatores, do grau de complexidade, ineditismo do projeto ou da tecnologia e do SIL requerido.

3.10 AVALIAÇÃO DA SEGURANÇA FUNCIONAL DO SIS

Para avaliação da segurança funcional do SIS a IEC 61511 (INTERNATIONAL..., 2003) estabeleceu um sistema de gerenciamento que contempla todas as fases do ciclo de vida do SIS.

A política e a estratégia para atingir a segurança devem ser identificadas junto com os meios para medir a eficácia. Os resultados desta avaliação, quando realizada, devem ser comunicados dentro da organização.

Devem ser estabelecidos procedimentos para avaliação multidisciplinar da segurança funcional do SIS, com o objetivo de verificar se o SIS atingiu o nível de integridade de segurança e a segurança funcional especificados.

4 TECNOLOGIA, TOPOLOGIA E APLICAÇÕES

Neste capítulo serão abordadas as diversas tecnologias utilizadas, destacando os avanços e etapas já vencidas no desenvolvimento da tecnologia Foundation Fieldbus para aplicação em SIS. Topologias típicas de sensores e de elementos finais, com a apresentação de um exemplo conceitual de SIS em um processo, também serão apresentados.

4.1 TECNOLOGIA

Gruhn e Cheddie (2006) citam uma variedade de tecnologias a serem aplicadas em SIS. A decisão sobre que tecnologia utilizar deve considerar principalmente os custos do ciclo de vida, tamanho, complexidade, requisitos de comunicação e nível de risco dos sistemas:

- pneumáticos: são mais indicados para pequenas aplicações que tenham pouca disponibilidade de energia elétrica;
- de relés: são geralmente usados em aplicações pequenas e simples;
- de estado sólido: (sistemas que utilizam cabos e que não utilizam *software*) apresentam custos altos e limitada flexibilidade. São utilizados em aplicações simples, pequenas e com alto nível de integridade de segurança;
- baseados em *software*: oferecem vários recursos e têm aplicação mais ampla.

4.2 TECNOLOGIA FOUNDATION FIELDBUS

A arquitetura aberta, não proprietária, Foundation Fieldbus – FF utiliza um protocolo de comunicação para sistemas de instrumentação e controle em que cada

dispositivo tem sua própria inteligência e comunica por um sistema de comunicação digital, serial e bi-direcional.

A rede H1 é utilizada para controle de processos, interface no nível de campo e integração de dispositivos, com velocidade de 31,25kbit/s. Projetada para ter sinal e alimentação em um mesmo par trançado, torna opcional o uso de fibra óptica e suporta aplicações de segurança intrínseca.

A High Speed Ethernet – HSE, que possui velocidade de 100Mbit/s, é projetada para dispositivos, subsistemas e integração com os sistemas empresariais (FIELDBUS FOUNDATION, 2012 a).

Um exemplo de arquitetura FF é apresentado na figura 9. Nas aplicações com dispositivos FF, a lógica de controle pode ser configurada no próprio sensor ou no atuador o que permite a continuidade operacional mesmo com a perda de comunicação com o sistema de controle central.

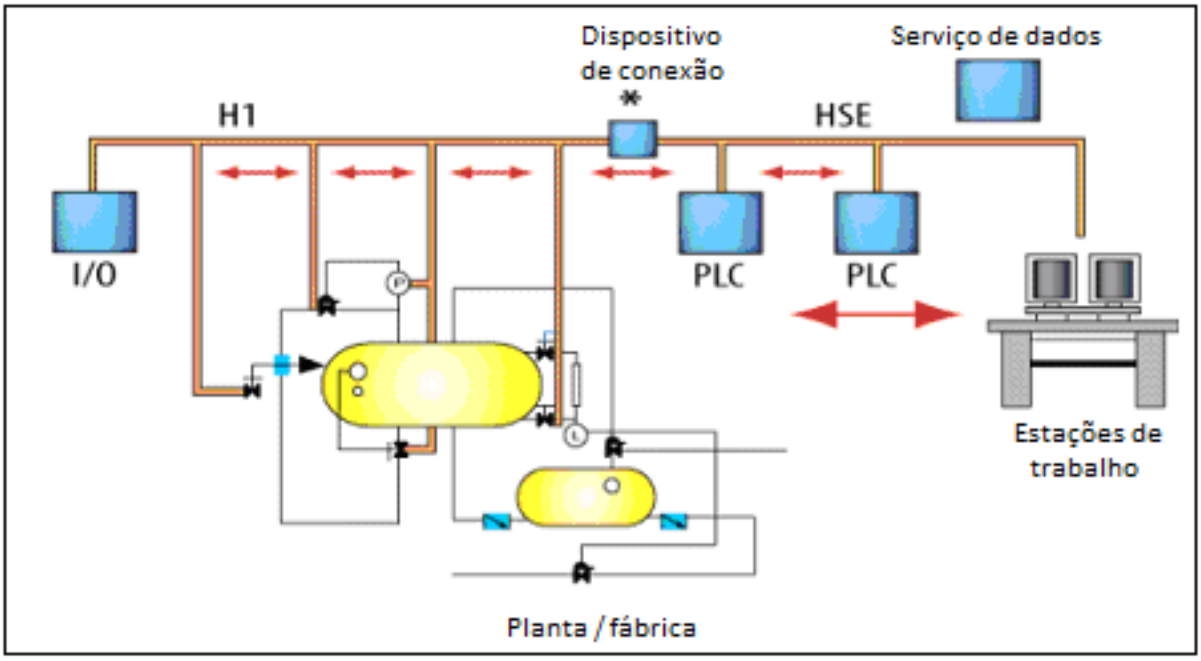

Figura 9: Exemplo de arquitetura de rede com dispositivos FF
Fonte: adaptado de Fieldbus Foundation (2012 b)

4.3 PROJETO FF-SIF

Em outubro de 2002 foi aprovado o desenvolvimento da especificação do projeto FF-SIF (Funções Instrumentadas de Segurança da Fieldbus Foundation). Decorridos dois anos, a Fieldbus Foundation finalizou a especificação preliminar para o desenvolvimento do FF-SIF e em 2005, testes de laboratório realizados por uma consultoria independente validaram as especificações. Posteriormente foi obtida a aprovação final para o tipo de protocolo junto ao TÜV. O projeto inclui o desenvolvimento de práticas e recomendações, treinamento, ferramentas de teste e demonstrações de campo de SIS com tecnologia FF (FIELDBUS FOUDATION, 2012 c).

No artigo intitulado Fieldbus Myths Busted (FIELDBUS FOUNDATION, 2012 d) é relatado que as especificações do FF-SIF foram aprovadas pelo TÜV em 2006, em conformidade com a IEC 61508 (INTERNATIONAL..., 2010) para aplicações até SIL3. Com a aprovação da especificação, fornecedores começaram a desenvolver produtos FF para aplicação em SIS e empresas de petróleo como Aramco e Shell iniciaram testes de sistemas com dispositivos e resolvedores de lógica FF-SIF. A rede H1 não foi alterada para a implementação de SIS, mas foram incrementadas as funções de diagnóstico e a capacidade de detecção de falhas. No citado artigo, são citados como vantagens do FF-SIF a entrada em operação mais rápida e a redução dos custos de instalação.

Devido ao estágio atual da tecnologia, ainda em desenvolvimento, as referências são bastante escassas, se limitando a alguns artigos publicados no sitio da Fieldbus Foudation e de empresas que participam do grupo de trabalho.

Shaiwale (2012), da empresa Hima publicou em dezembro de 2011 as informações mais recentes sobre o estágio do projeto FF-SIF disponibilizadas no sítio da Fieldbus Foundation. Como uma justificativa para o desenvolvimento da tecnologia FF para SIS apresenta o fator de cobertura de diagnóstico, expresso pela relação entre as taxas de falhas perigosas detectáveis pelo diagnóstico e o total de falhas perigosas. De forma qualitativa a distribuição das falhas seguras e perigosas, detectáveis e não-detectáveis é apresentada na figura 10. Apesar da maior parte das falhas serem seguras ou detectáveis, devem ser destacadas as falhas perigosas não detectáveis.

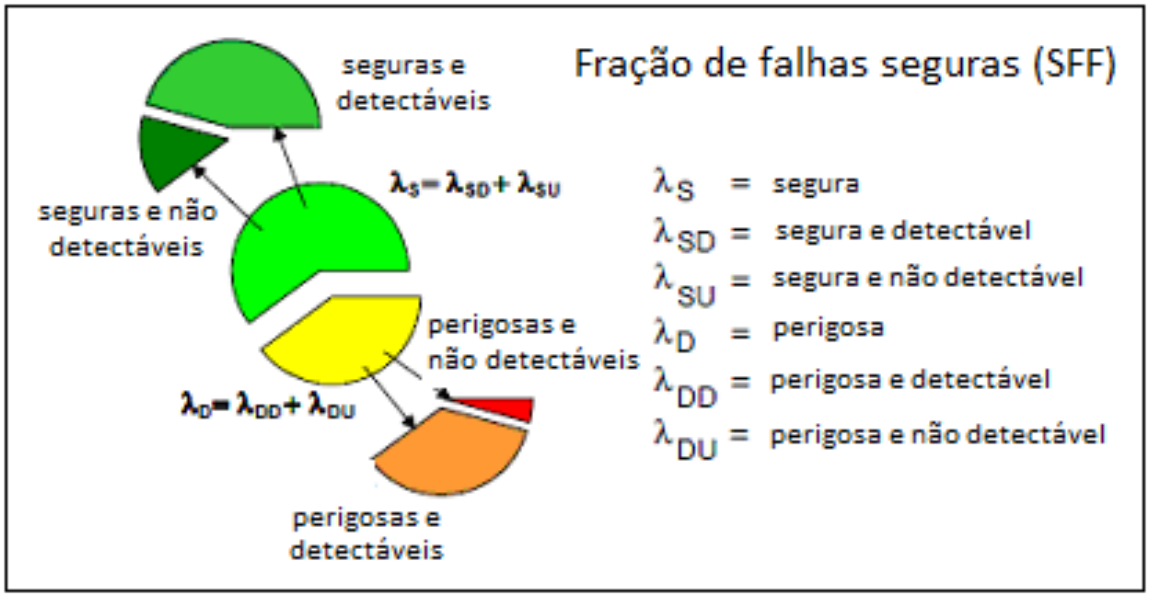

Figura 10: Falhas seguras, perigosas, detectáveis e não detectáveis
Fonte: adaptado de Shaiwale (2012)

Assim como Gruhn e Cheddie, Shaiwale (2012) destaca que a porcentagem de falhas é de cerca de 8% nos resolvedores de lógica e de 92% em elementos de campo (sensores e elementos finais). Divergem, no entanto quando tratam de elementos finais, pois para Gruhn e Cheddie estes contribuem com 50% das falhas e para Shaiwale representam 65% do total de falhas.

No caso de válvulas de controle a tecnologia FF-SIF permite pequenas movimentações da haste para diagnóstico *(Partial Stroke Test)*, contribuindo para uma redução na PFD, conforme a figura 11.

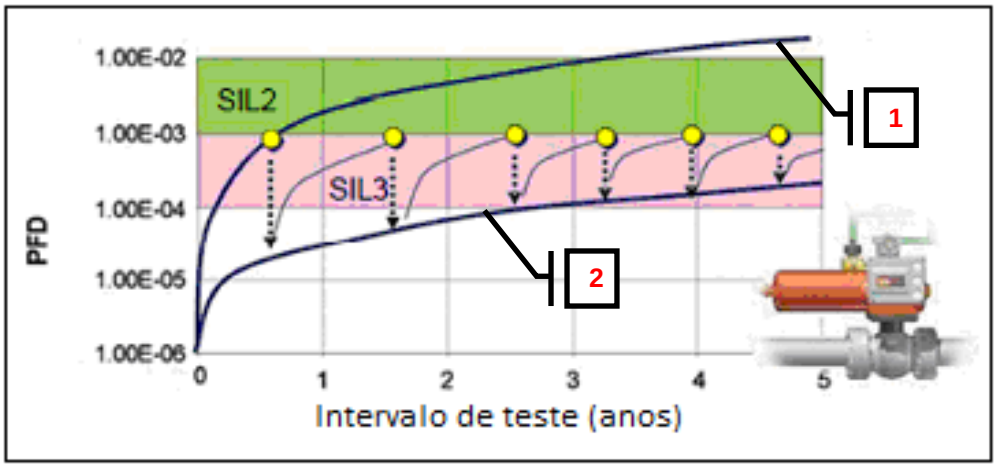

Figura 11: Redução de PFD em válvulas devido ao Partial Stroke Test
Fonte: adaptado de Shaiwale (2012)

A curva 1 mostra o aumento previsto da PFD, sem a rotina de testes. Em cerca de seis meses a PFD seria tal que degradaria a função de segurança do nível SIL 3 para SIL2 e em cerca de três anos sofreria nova degradação. A curva 2 mostra que com a realização de testes periódicos é possível reduzir a PFD, permitindo que a mesma malha de intertravamento atenda aos requisitos de um SIL maior.

Segundo Shaiwale (2012), algumas das razões para a utilização da tecnologia FF para SIS são:

- Melhoria do diagnóstico em dispositivos de campo;
- Redução da probabilidade de falhas perigosas não-detectadas;
- Aumento nos intervalos de teste;
- Aumento na disponibilidade e lucratividade dos processos;
- Redução de paradas espúrias;
- Integração mais fácil e barata com gerenciamento de ativos;
- Redução da quantidade de cabos e de painéis.

Shaiwale (2012) apresenta as configurações dos sistemas FF-SIF, que estão sendo testadas pela Chevron (figura 12), Aramco (figura 13) e Shell (figura 14). Com o intuito de desenvolver a tecnologia as configurações implementadas para teste em campo contam com a participação de diversos fabricantes de *hardware* e *software*.

No caso da Chevron foram utilizados sensores da ABB, Emerson, Smar, Siemens e Magnetrol monitorando pressão e nível. Os elementos finais (válvulas) foram da Emerson e da Westlock. Os resolvedores de lógica, o configurador e o sistema de gerenciamento de ativos e a ferramenta de diagnóstico foram desenvolvidos pela Emerson.

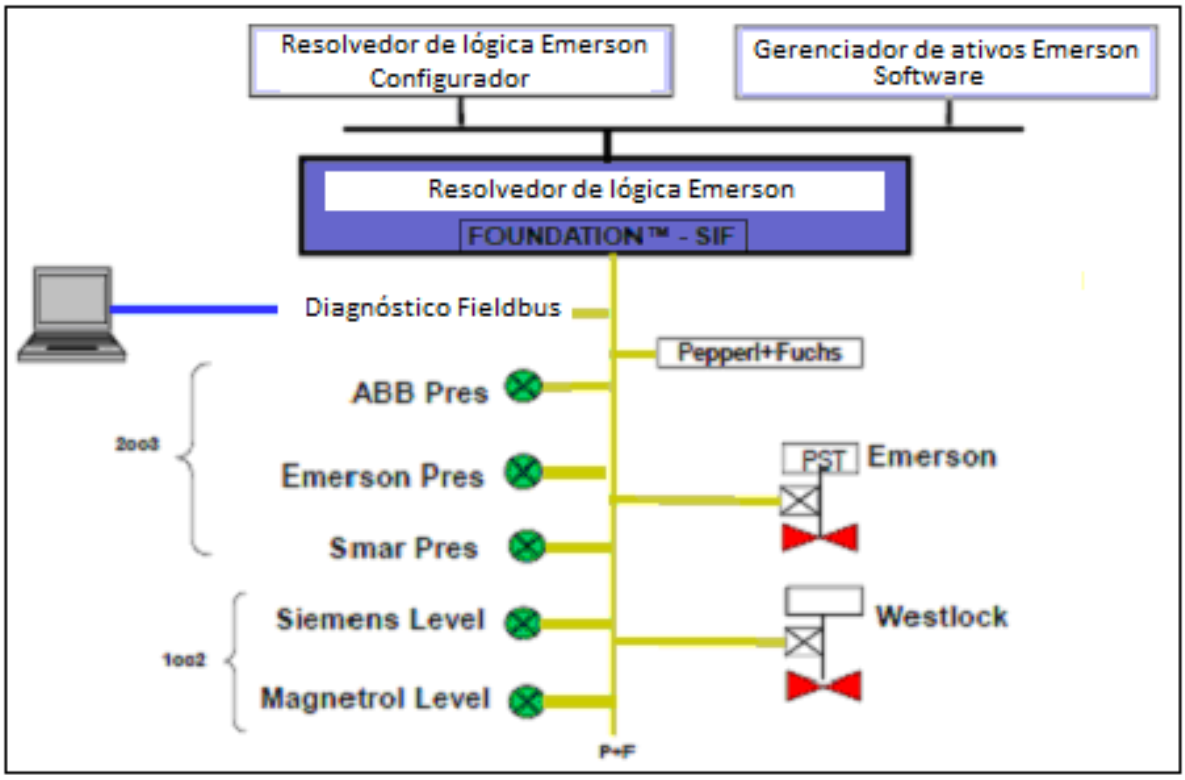

Figura 12: Sistema FF-SIF com PLC da Emerson - Chevron em Houston
Fonte: adaptado de Shaiwale (2012)

Na aplicação implantada na Saudi Aramco, foram utilizados resolvedores de lógica, BPCS, gerenciamento de ativos e sensores da Yokogawa. Também participaram a Metso, Pepperl Fuchs, Fisher, Magnetrol, Smar e outros fornecedores.

Saudi Aramco, segundo Shaiwale (2012), planeja a instalação de FF-SIF no Projeto Juaymah para mostrar os benefícios da tecnologia e ampliar a capacidade de diagnóstico e testes locais. Uma segunda aplicação estaria sendo planejada com a substituição de um sistema de bloqueio de emergência por um sistema com novas válvulas (Smart ZV), equipadas com atuadores pneumáticos e posicionadores inteligentes FF-SIF.

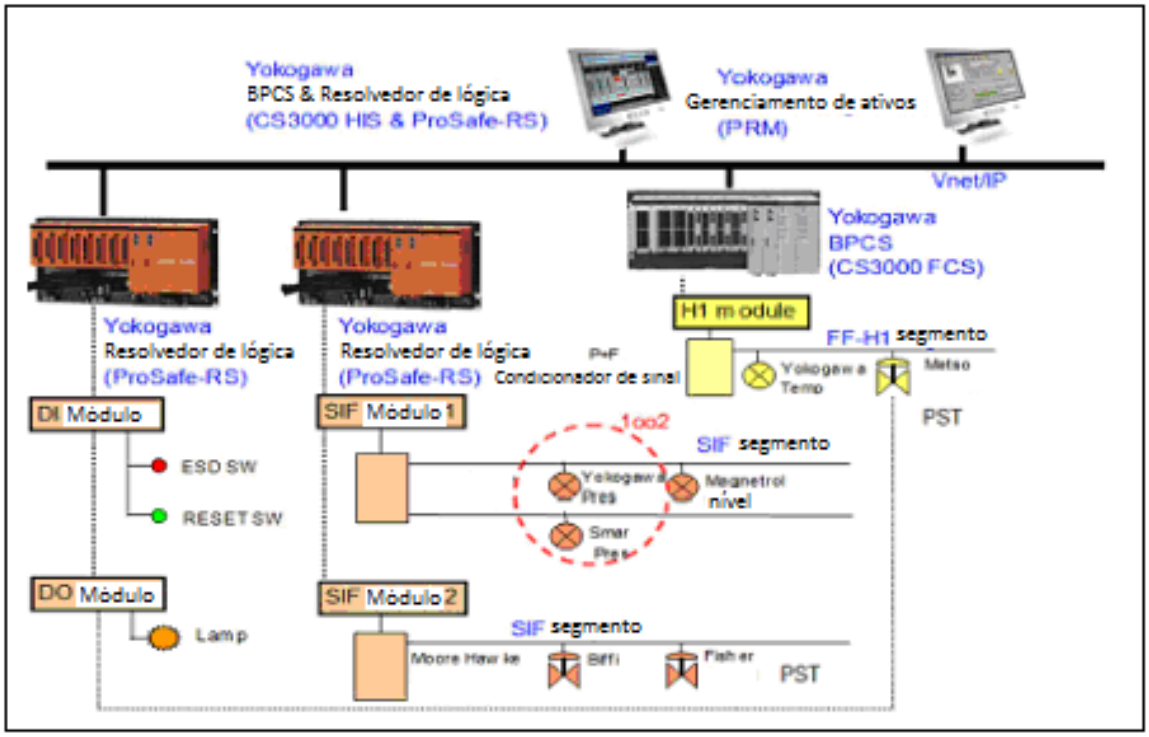

Figura 13: Sistema FF-SIF com PLC da Yokogawa – Aramco em Dhahran
Fonte: adaptado de Shaiwale (2012)

Na aplicação implantada na Shell GS foi utilizado PLC da Hima, BPCS e gerenciamento de ativos da Yokogawa. Elementos iniciadores e finais foram fornecidos pela Emerson, Smar, Westlock, Siemens, Magnetrol, Yokogawa, Metso, Endless Hauser.

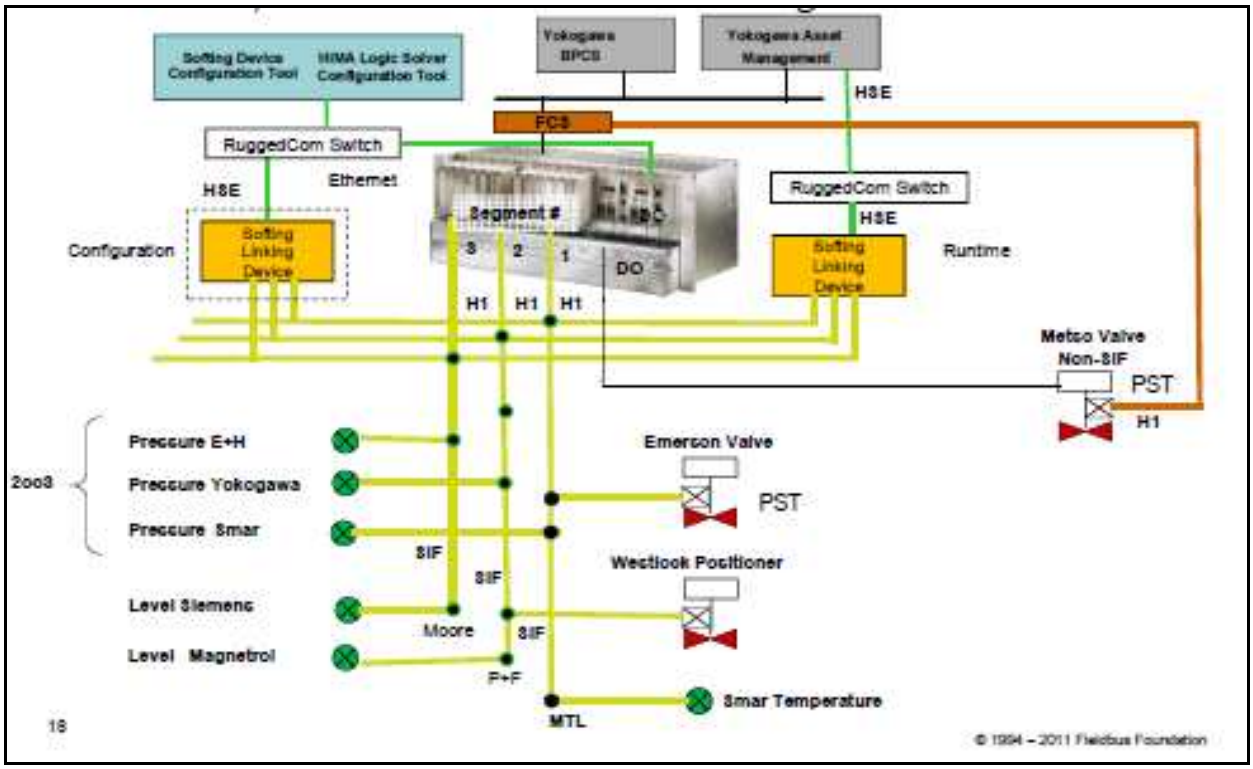

Figura 14: Sistema FF-SIF com PLC da HIMA – Shell GS em Amsterdã
Fonte: Shaiwale (2012)

Segundo Shaiwale (2012), a Shell Global Solutions aguarda a disponibilização de dispositivos certificados para a instalação no projeto NAM na Holanda, sendo que a primeira onda de produtos é esperada para o ano de 2012.

4.4 TOPOLOGIA E APLICAÇÕES

Gruhn e Cheddie (2006) afirmam que o projeto conceitual do SIS deve ser realizado de acordo com os padrões relevantes da indústria e apresentam resumo das práticas relacionadas à arquitetura, para seleção de *hardware* e *software*:

- SIL 0
    - Sensores: não é requerida redundância.
    - Resolvedores de lógica: pode ser configurado em sistemas de controle, tal como o SDCD, ou PLCs industriais não redundantes.
    - Elementos finais: não é requerida redundância.

- SIL 1:
    - Sensores: não é requerida redundância.
    - Resolvedores de lógica: pode ser especificado ou relé lógico ou PLC não redundante.
    - Elementos finais: não é requerida redundância.
- SIL 2:
    - Sensores: a redundância deve ser aplicada somente se for requerido durante os cálculos de PFD média.
    - Resolvedores de lógica: PLC de segurança é requerido.
    - Elementos finais: aplicar redundância se requerido pelos cálculos de PFD média.
- SIL 3:
    - Sensores: devem ser redundantes, podendo ter votação 1oo2 ou 2oo3 dependendo dos requisitos de paradas espúrias.
    - Resolvedores de lógica: devem ser utilizados PLCs de segurança redundantes.
    - Elementos finais: é requerida votação 1oo2.
- SIL 4

Segundo a IEC 61.511-1 (INTERNATIONAL..., 2003), funções de segurança SIL 4 são raras na indústria de processo e devem ser evitadas devido à dificuldade em alcançar e manter este nível de integridade. Deve ser avaliada a adoção de camadas de proteção não instrumentadas ou aumentar a segurança intrínseca do processo de forma a evitar malhas SIL 4.

Sistemas com SIL 4 possuem os mais rigorosos requisitos e devem suportar até duas falhas simultâneas de *hardware*, mantendo sua capacidade de atuar em eventual demanda.

- Sensores: devem ser redundantes e sua configuração dependerá de projeto específico.
- Resolvedores de lógica: devem ser utilizados PLCs de segurança redundantes e com *hardware* diferente. O uso de *hardware* diverso somente pode ser dispensado onde for comprovado a obtenção do SIL 4 sem sua adoção.
- Elementos finais: devem ser redundantes e sua configuração dependerá de projeto específico.

Ilustrando as votações citadas, as figuras 15 e 16 apresentam possíveis configurações para elementos finais com o objetivo de atingir a redundância requerida, conforme a ISA-TR84.00.02-2002 - Part 2 (INSTRUMENTATION..., 2002). Assim como os exemplos podem ser extrapolados para os sensores, no caso de acionamento de elementos finais elétricos, são válidos os mesmos arranjos, substituindo as válvulas por contatos elétricos.

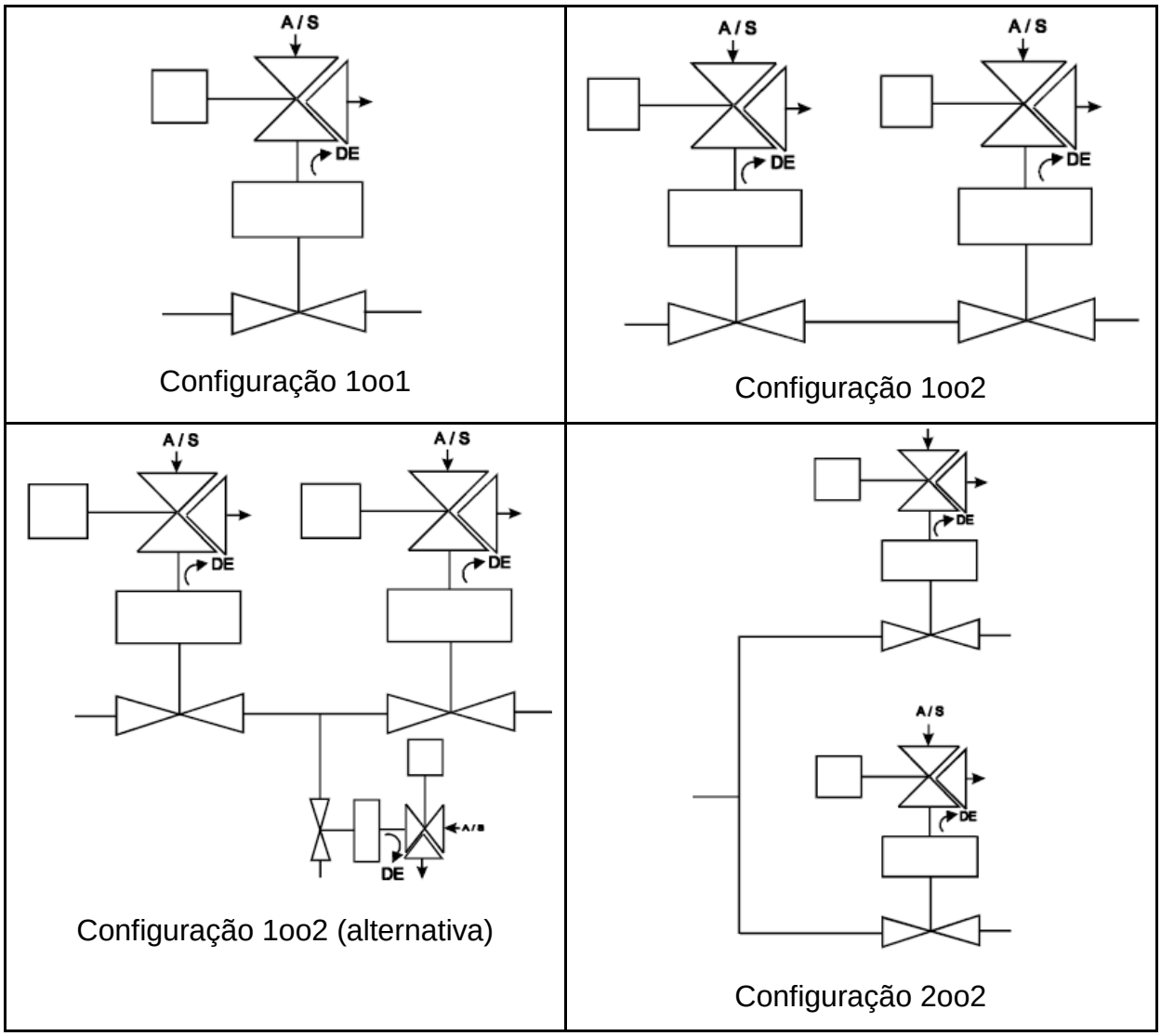

Figura 15: Configuração de elementos finais
Fonte: ISA-TR84.00.02-2002 - Part 2 (INSTRUMENTATION..., 2002)

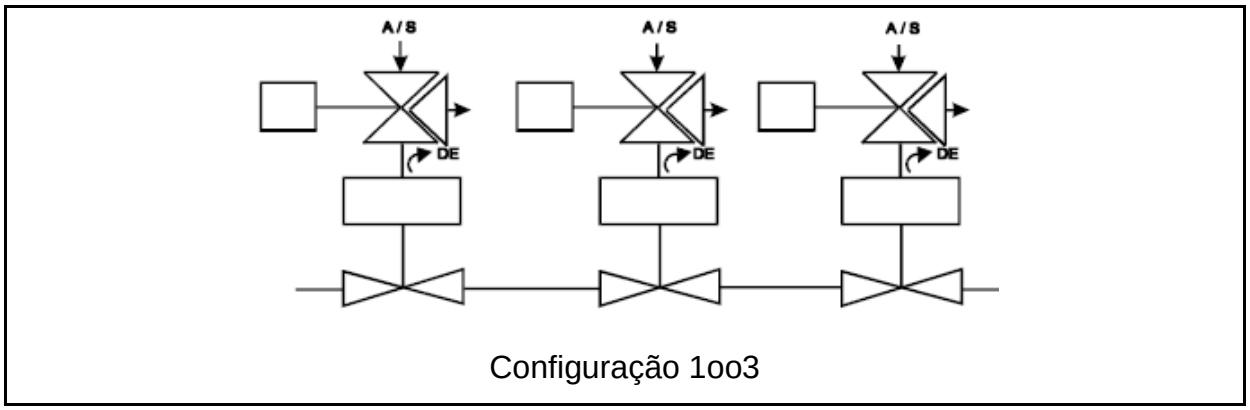

Figura 16: Configuração de elementos finais
Fonte: ISA-TR84.00.02-2002 - Part 2 (INSTRUMENTATION..., 2002)

Um diagrama de processo e a configuração do SIS para um exemplo de malha SIL 2 é apresentado nas figuras 17 e 18, segundo a ISA-TR84.00.02-2002 - Part 2 (INSTRUMENTATION..., 2002).

A figura 17 mostra os sensores de vazão com a configuração 2oo3 (votação 2 de 3), os transmissores de pressão, as chaves de temperatura e de nível com votação 1oo2 (1 de 2). Na configuração 2oo3 é necessário que dois sensores detectem a falha simultaneamente para que seja desencadeada a lógica do SIS. Uma vez acionada a função de segurança o resolvedor de lógica comanda as válvulas de admissão de produto no vaso. Na configuração apresentada, 1oo2, as duas válvulas são acionadas simultaneamente. O fechamento de uma das válvulas conduz o processo para um estado seguro, sendo que a segunda é a redundância da primeira válvula.

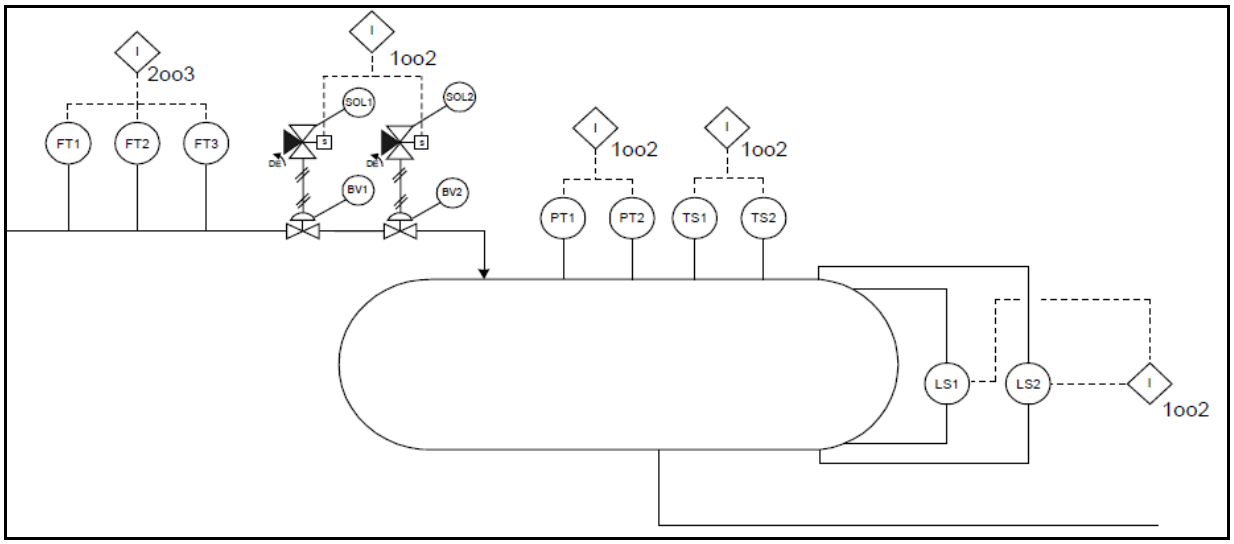

Figura 17: Exemplo de diagrama de processo
Fonte: ISA-TR84.00.02-2002 - Part 2 (INSTRUMENTATION..., 2002)

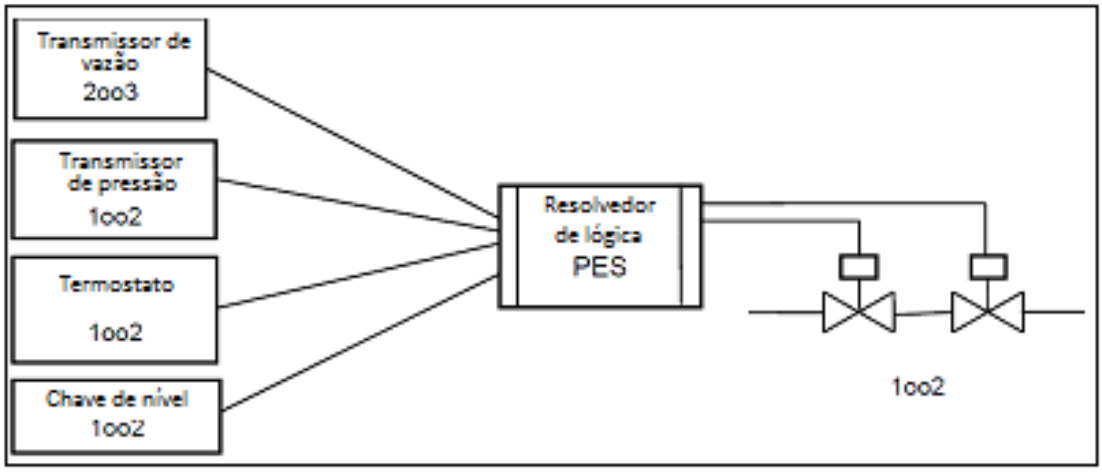

Figura 18: Exemplo de configuração de SIS (malha SIL 2)
Fonte: adaptado de ISA-TR84.00.02-2002 - Part 2 (INSTRUMENTATION..., 2002)

4.5 HIPPS

Sistemas como o High Integrity Pressure Protection System – HIPPS têm substituído dispositivos mecânicos especiais, permitindo como benefício adicional reduzir custos no dimensionamento de tubulação e equipamentos (GRUHN; CHEDDIE, 2006).

No HIPPS a malha de segurança, formada por iniciadores, elementos finais e resolvedor de lógica, executam a proteção contra sobrepressões. Todos os componentes devem ser do tipo falha segura, no modo desenergizado. Tipicamente é utilizada em aplicações onde são movimentadas grandes quantidades de líquidos. Nestes casos durante transitórios, tais como reduções bruscas de vazão, ocorrem elevações rápidas de pressão. No método tradicional, além do maior dimensionamento da tubulação e de equipamentos, são utilizadas válvulas de segurança para aliviar o fluxo, podendo também ser empregado o SIS como camada de proteção adicional. Entretanto, o alívio de vazão implica na necessidade de reservatório para armazenar o fluido o que nem sempre é viável. Em tais casos o HIPPS protege contra sobrepressão, por meio do rápido e confiável isolamento dos sistemas a serem protegidos da fonte causadora de risco. Com a aplicação do HIPPS, que propicia redução de risco de até SIL3, é evitado o sobredimensionamento e eventuais tanques são significativamente reduzidos em

volume. Na figura 19 pode-se observar que os elementos finais (válvulas) estão instalados em tubulação com classe de pressão (1500 libras) superior à protegida pelo HIPPS (600 libras).

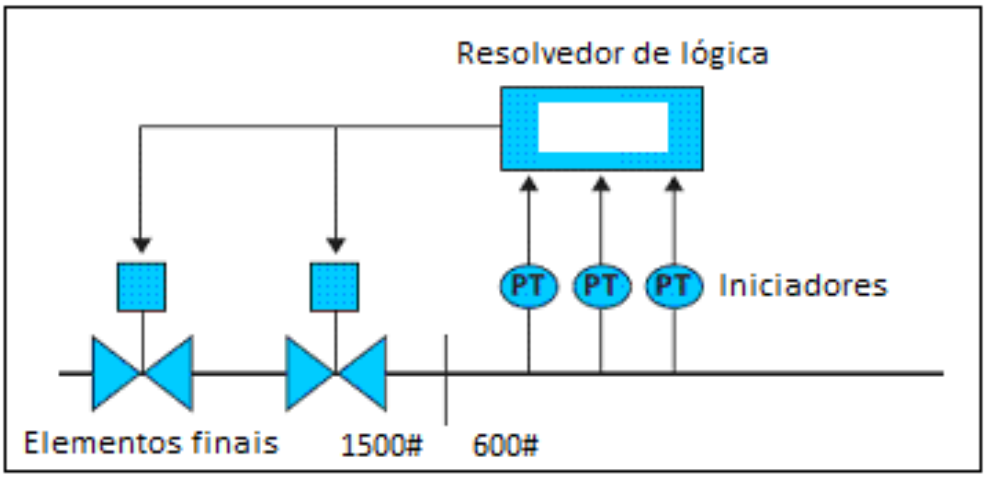

Figura 19: Malha de segurança típica do HIPPS
Fonte: adaptado de Mokveld Valves (2012)

5 CONSIDERAÇÕES FINAIS

Tipicamente os equipamentos e sistemas protegidos por SIS possuem significativos tempos de reparo e este se torna ainda maior no caso de reposição de componentes como rotores de turbinas, bombas e compressores de grande porte. As interrupções na produção, em caso de danos severos podem ter meses de duração o que torna acentuadas as perdas financeiras.

Um dos desafios é convencer os gerentes a investir em SIS, pois tais sistemas são frequentemente associados a interrupções no processo produtivo. Apesar do aparente conflito entre produção e segurança nas instalações industriais, Gruhn e Cheddie (2006, p. 25) citam estudo da Occupational Safety & Health Administration - OSHA, em que a regulação para gerenciamento de segurança de processo reduziu o número de acidentes em mais de 20% e resultou em aumento de produtividade das empresas.

SIS tem como função conduzir o processo à condição de segurança, sempre que demandado, reduzindo desgastes ou sobrecargas durante as paradas, e permitem restabelecer em menor tempo a operação normal das unidades de processo. A implantação de SIS nas empresas altera toda a sistemática utilizada pelas equipes de operação e manutenção, pois implementa novas rotinas e requer procedimentos, treinamentos, documentação e organização.

Para obter o desempenho especificado é fundamental que as funções e a integridade do SIS sejam preservadas. Durante a especificação de grandes ou complexos sistemas de segurança, os recursos necessários são disponibilizados e especialistas conduzem ou assessoram os trabalhos. No entanto, pouco efetivos são a especificação, o projeto, a construção e a instalação, se a operação e a manutenção não seguirem as especificações de projeto e se não houver um controle rigoroso de mudanças.

Aplicações menores frequentemente são implementadas pelas equipes em meio às rotinas da manutenção, sem a necessária avaliação dos riscos do processo ou da redução de risco necessária. Um intertravamento ou uma função de segurança, quando identificados não devem ser tratados como uma aplicação simples de *hardware* e *software* e sim analisadas conforme as normas técnicas

aplicáveis, que podem ser internacionais caso inexistam normas nacionais conforme prevê a NR 10.

Em indústrias químicas e petroquímicas o corpo técnico possui acesso fácil às normas técnicas e está familiarizado com sistemas de segurança e seus requisitos. Mesmo assim é possível constatar em congressos e em comunidades técnicas a implementação de SIFs sem os procedimentos adequados.

A visão geral do ciclo de vida do SIS, os conceitos sobre SIS, as abordagens de diferentes entidades normatizadoras, particularidades de intertravamento e controle, tecnologia, topologia e justificativas para instalação do SIS contribuirão para disseminar conceitos e aproximar leitores desta área de conhecimento, tal como estabelecido nos objetivos desta monografia.

A pesquisa realizada e a elaboração deste dossiê permitiram agrupar conceitos e regulamentações a serem considerados por profissionais que tenham alguma interface com funções instrumentadas de segurança. Adicionalmente este trabalho poderá ser utilizado como um guia para orientar a busca de conhecimento sobre SIS aos leitores, assim como guiou o autor.

Como sugestão para trabalhos futuros, considera-se relevante

- Diagnóstico de gestão de ciclo de vida de SIS;
- Diagnóstico de gestão de manutenção de SIS;
- Casos de estudo relativos ao ciclo de vida do SIS;
- Aplicação de métodos para determinação de SIL;
- Comparação entre métodos para definição do SIL das malhas;
- Análises de viabilidade técnica e econômica do ciclo de vida do SIS;
- Estudos de caso referentes à aplicação dos conceitos normativos sobre SIS.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT Catálogo**. Disponível em: < http://www.abntcatalogo.com.br/> Acesso em: 10 mar. 2012.

BECKMAN, Lawrence. **Determining the required safety integrity level for your process**. Houston: ISA Transactions 37 Elsevier, 1998.

CENTER FOR CHEMICAL PROCESS SAFETY – CCPS. **Layers of Protection Analysis**: Simplified Process Risk Assessment. 1st ed. New York: American Institute of Chemical Engineers – AIChE, 2001.

COMISSÃO DE NORMALIZAÇÃO TÉCNICA PETROBRAS. **N 2595**: Critérios de Projeto, Operação e Manutenção de Sistemas Instrumentados de Segurança em Unidades Industriais. rev. C. Rio de Janeiro: PETROBRAS, 2011.

CONSELHO NACIONAL DO MEIO AMBIENTE. **Resoluções do Conama**: Resoluções vigentes publicadas entre julho de 1984 e novembro de 2008. 2.ed. Brasília: Conama, 2008.

EMERSON PROCESS. **DeltaV SIS System Overview**. Disponível em: <http://www2.emersonprocess.com/en-US/brands/deltav/sis/differentiators/Pages/SystemOverview.aspx> Acesso em: 10 dez. 2012. a

EMERSON PROCESS. **DeltaV Overview**. Disponível em: <http://www2.emersonprocess.com/en-US/brands/deltav/differentiators/Pages/SystemOverview.aspx> Acesso em: 18 jun. 2012. b

FIELDBUS FOUNDATION. **Overview.** Disponível em: <http://fieldbus.famefoundry.com/index.php?option=com_content&task=view&id=23&Itemid=308>. Acesso em: 12 jun. 2012. a

FIELDBUS FOUNDATION. **Exemplo de arquitetura de rede com dispositivos FF.** Disponível em: <http://fieldbus.famefoundry.com/index.php?option=com_content&task=view&id=138&Itemid=314>. Acesso em: 12 jun. 2012. b

FIELDBUS FOUNDATION. **Fieldbus Foundation Launches End User Demonstration Project For Safety Instrumented Systems.** 2006. Disponível em:

<http://www.fieldbus.org/index.php?option=com_content&task=view&id=338&Itemid=281>. Acesso em: 21 maio 2012. c

FIELDBUS FOUNDATION. **MYTHS BUSTED.** Disponível em: <http://www.fieldbus.org/index.php?option=com_content&task=view&id=150&Itemid=326>. Acesso em: 21 maio 2012. d

FINKEL, Vitor S. et al. **Instrumentação Industrial**. 2.ed. Rio de Janeiro: Interciência, 2006.

GIL, Antonio C. **Como elaborar projetos de pesquisa**. 5. ed. São Paulo: Atlas, 2010.

GRUHN, Paul; CHEDDIE, Harry L. **Safety Instrumented Systems: Design, Analysis and Justification**. 2nd ed. Durham: ISA – Instrumentation, Systems, and Automation Society, 2006.

INTERNATIONAL ELECTROTECHNICAL COMMISSION. **IEC 60092-504**: Electrical Installation in Ships – Part 504: Control and Instrumentation. 3rd ed. Genebra: IEC, 2001.

INTERNATIONAL ELECTROTECHNICAL COMMISSION. **IEC 61131-1**: Programmable controllers – Part 1: General information. 2nd ed. Genebra: IEC, 2003.

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

INTERNATIONAL ELECTROTECHNICAL COMMISSION. **IEC 61511-1**: Functional safety – Safety instrumented systems for the process industry sector – Part 1: Framework, definitions, system, hardware and software requirements. 1st ed. Genebra: IEC, 2003.

INTERNATIONAL ELECTROTECHNICAL COMMISSION. **IEC 61511-3**: Functional safety – Safety instrumented systems for the process industry sector – Part 3: Guidance for the determination of the required safety integrity levels. 1st ed. Genebra: IEC, 2003.

INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS. **IEEE Std 493**: IEEE Recommended Practice for the Design of Reliable Industrial and Commercial Power Systems. 2nd ed. New York: IEEE, 2007.

INSTRUMENTATION, SYSTEMS, AND AUTOMATION SOCIETY, **ISA-TR84.00.02-2002 - Part 2**: Safety Instrumented Functions (SIF) - Safety Integrity Level (SIL) Evaluation Techniques – Part 2: Determining the SIL of a SIF via Simplified Equations. 1st ed. North Carolina: IHS, 2002.

INSTRUMENTATION, SYSTEMS, AND AUTOMATION SOCIETY, **ISA-TR84.00.04-2005 – Part 2**: Example Implementation of ANSI/ISA-84.00.01-2004 (IEC 61511 Mod). 1st ed. North Carolina: IHS, 2005.

MITCHELL, Kevin J; HERENA, Peter. **Safety Instrumented Systems Engineering Handbook.** 1st ed. Columbus: Kenexis Consulting Corporation, 2010.

MOKVELD VALVES. **Mokveld-HIPPS_application_leaflet_EN.** Disponível em: <http://www.mokveld.com/upload/product_document/Mokveld-HIPPS_application_leaflet_EN.pdf>. Acesso em: 29out.2012.

SHAIWALE, Lalit S. **Foundation Fieldbus in Safety Applications (SIF) - (Apresentação).** Disponível em: <http://www.fieldbus.org/images/stories/international/asiapacific/India/presentations/j2011_5_ff_in_safety_applications__sif_.pdf> Acesso em: 21 maio 2012.

SHEBLE, Nicholas. **More is always better when it's critical:** TMR is an old good idea that is only more valuable in the microprocessed era. Disponível em: <http://www.isa.org/InTechTemplate.cfm?Section=Features3&template=/ContentManagement/ContentDisplay.cfm&ContentID=30533> Acesso em: 18 jun. 2012.