ESCOLA POLITÉCNICA DA UNIVERSIDADE DE SÃO PAULO

Projeto de Conclusão do Curso

Controle de Sistemas Instrumentados de Segurança (SIS) para o Caso de uma Estação de Compressão de Gás

Robson Naoto Sassaki Hirata

Rodolfo Saraiva Pini

São Paulo

2010

Robson Naoto Sassaki Hirata

Rodolfo Saraiva Pini

Controle de Sistemas Instrumentados de Segurança (SIS) para o Caso de uma Estação de Compressão de Gás

Monografia apresentada junto ao Curso de Engenharia Mecatrônica da Escola Politécnica da USP, na área de controle e automação, como requisito para a graduação.

Área de concentração: Engenharia Mecatrônica

Orientador: Prof. Dr. Diolino José dos Santos Filho

São Paulo

2010

FICHA CATALOGRÁFICA

Hirata, Robson Naoto Sassaki
Controle de sistemas instrumentados de segurança (SIS) para o caso de uma estação de compressão de gás / R.N.S. Hirata, R.S. Pini. -- São Paulo, 2010.
p.

Trabalho de Formatura - Escola Politécnica da Universidade de São Paulo. Departamento de Engenharia Mecatrônica e de Sistemas Mecânicos.

1. Instrumentação de sistemas (Segurança) 2. Redes de Petri 3. Sustentabilidade I. Pini, Rodolfo Saraiva II. Universidade de São Paulo. Escola Politécnica. Departamento de Engenharia Mecatrônica e de Sistemas Mecânicos III. t.

DEDICATÓRIA

Aos nossos pais, que nos deram toda formação de nossos valores e o suporte necessário para o alcance dos resultados obtidos.

AGRADECIMENTOS

Ao Prof. Dr. Diolino José dos Santos Filho, nosso orientador neste trabalho, por todo o suporte, paciência, atenção e confiança fornecidos, bem como por todo o conhecimento compartilhado e o tempo demandado à orientação.

A Reinaldo Squillante, mestrando da Escola Politécnica da USP e colaborador deste trabalho, por todo o compartilhamento de idéias e fornecimento de informações necessárias, referentes ao Estudo de Caso desenvolvido.

A todos aqueles que colaboraram direta e indiretamente da realização deste trabalho.

RESUMO

Atualmente, com a necessidade de se desenvolver soluções em engenharia que sejam aderentes aos princípios de sustentabilidade, faz-se necessária a aplicação de procedimentos para o desenvolvimento de sistemas de controle de plantas industriais que evitem acidentes que causam riscos ambientais e ao próprio ser humano. Neste sentido, tem sido proposto o conceito de Sistemas Instrumentados de Segurança (SIS) como uma forma de garantir níveis de risco aceitáveis para operação dos sistemas no contexto atual. Quanto maior a complexidade de um sistema, maior é a probabilidade de haver riscos não previstos em sua modelagem, e é nestes riscos que o SIS atua, visando a evitar e/ou mitigar suas conseqüências, aumentando assim, o nível de segurança do sistema. Este trabalho pretende contribuir para o desenvolvimento de algoritmos de controle necessários para executar os processos e as lógicas adicionais de controle para manter o processo seguro, aplicados ao estudo de caso de uma Estação de Compressão de Gás. Propõe-se uma nova abordagem, baseada na inserção de módulos de Diagnose e Tratamento de Falhas das Funções Instrumentadas de Segurança (SIF's). Estes módulos permitem uma maior confiabilidade dos algoritmos, que serão implementados em Rede de Petri (RdP), pois é um modelo matemático formal que permite uma análise global do SIS, pois utiliza os conceitos de estados locais e estado global. Propõe-se ainda a transcrição destes modelos para as linguagens de acordo com a norma IEC 61131-3.

Palavras-chave: Sistemas Instrumentados de Segurança (SIS), Diagnose, Tratamento de Falhas, IEC 61508, IEC 61131-3, Rede de Petri.

ABSTRACT

Currently, due to the demand for the development of Engineering solutions that are adherent to the principles of sustainability, it is necessary to apply procedures to the development of control systems for industrial plants to prevent accidents that cause environmental hazards and harm the human being. Thus, it has been proposed the concept of SIS (Safety Instrumented Systems) as a way to ensure acceptable risk levels for operating systems in the current context. The more complex a system, the higher is the likelihood of unpredictable risks in its modeling, and it is on these risks that the SIS has to act in order to avoid and/or mitigate their consequences, thus increasing the security level of the system. This work aims to develop control algorithms required to perform the procedures and additional logic control to keep the process safe, applied to the case of a Gas Compression Station. It is proposed a new approach based on the inclusion of modules of Diagnosis and Treatment of faults to the Safety Instrumented Functions (SIF's). These modules provide higher reliability to the algorithms that will be implemented in Petri Net (PN), that is a mathematical formal model that provides a global analysis to the SIS. It is still proposed the transcription of these models to languages according to the standard IEC 61131-3.

Keywords: *Safety Instrumented Systems (SIS), Diagnosis, Treatment of faults, IEC 61508, IEC 61131-3, Petri Net.*

SUMÁRIO

ÍNDICE DE FIGURAS

ÍNDICE DE TABELAS

1. INTRODUÇÃO

O cenário atual exige, mais do que nunca, que as plantas industriais busquem a otimização da produtividade, ou seja, os recursos devem ser utilizados de forma racional para evitar-se desperdício, ociosidade e acidentes que comprometam a sustentabilidade. Estes são os pré-requisitos que determinam competitividade no século XXI.

Para atender a essas exigências, uma das soluções adotadas prevê a automatização dos processos industriais. Neste contexto, os sistemas foram se tornando cada vez mais complexos até o patamar atual.

Tendo em vista o grau crescente desta complexidade, aumentou também a dificuldade em se modelar tais sistemas de forma a prever todos os estados alcançáveis durante a execução dos processos. Dessa forma, podemos dizer que em qualquer sistema, por mais moderno que seja, existem riscos inerentes de ocorrer um acidente.

É neste contexto que surge uma grande preocupação com a preservação tanto da segurança humana, quanto da proteção ao meio ambiente, tendo em vista os princípios de sustentabilidade. Desta forma, surgiram diversas normas ambientais e de segurança, a fim de impedir que riscos mais graves ocorram e de regulamentar os processos, obrigando os profissionais envolvidos a se conscientizarem da importância dos sistemas de segurança.

Além disso, pode-se ter claramente a noção do quanto tais riscos são danosos também às empresas responsáveis, uma vez que envolve custos elevados quando não são evitados ou mitigados a tempo, gerando um acidente que pode envolver muitas vezes reparos astronômicos à planta, além de custos de indenização, multas ambientais, entre outros, sem contar o prejuízo que isto pode causar à imagem da companhia.

Assim, surgiu o conceito de Sistemas Instrumentados de Segurança (SIS) que são projetados especificamente para desempenhar funções que mantêm um estado

seguro de processo quando condições perigosas ou não aceitáveis são detectadas, garantindo assim a integridade das pessoas, da planta e evitando impactos ambientais (LUNDTEIGEN, 2009).

1.1. HISTÓRICO DE ACIDENTES

Ao longo de muitos anos, o petróleo vem sendo utilizado em uma escala cada vez maior, sendo crescentes também sua aplicabilidade e importância a cada dia, tanto que muitos até o chamam de “ouro preto” e é difícil imaginar como seriam as nossas vidas sem o petróleo, extraído dos poços que podem estar em terra firme ou sob os oceanos, e seus derivados, produzidos nas mais diversas refinarias.

Devido à crescente demanda, a produção tem sido ampliada num ritmo intenso, acelerando a complexidade dos sistemas. Neste processo, toda a cadeia de produção vem sendo pressionada a cumprir performances de pico, operando nos limites de sua capacidade instalada e de vida útil.

Este quadro é agravado quando medidas de segurança como manutenção preventiva e reformas estruturais de instalações de alto risco não são projetadas adequadamente numa planta deste tipo. Historicamente, ao longo da exploração do petróleo e de gases, diversos acidentes já ocorreram, causando perda de vidas humanas, desastres ambientais e imensos prejuízos.

Infelizmente, ainda acontecem sérios acidentes. No ano de 1979, dezenas de milhões de litros de petróleo vazaram para o Golfo do México após explosões no poço de perfuração da *Ixtoc*. Várias tentativas de estancar o vazamento falharam e até hoje é considerado como sendo o pior da história nesta região. Foram necessários dez meses para deter o vazamento.

A história se repete. Um exemplo recente é o desastre na plataforma de petróleo de extração *Deepwater Horizon*, no Golfo do México, no dia 20 de Abril de 2010. Este acidente já levantou questões no âmbito político e legal e está alavancando a implementação de normas mais rígidas de segurança. E é um alerta para o Brasil em um momento que são feitas discussões a respeito dos royalties do

petróleo na camada do pré-sal, pois as condições de exploração neste caso são mais adversas.

Estes são alguns exemplos que revelam a importância dos cuidados com a segurança nos processos complexos que envolvem grandes riscos.

1.2. OBJETIVO

O objetivo deste trabalho é propor um método para desenvolver o controle de SIS baseado na descrição das Funções Instrumentadas de Segurança (SIFs), definidas pelo estudo HAZOP (*Hazard and Operability* - CRUZ-CAMPA, 2009), separando a lógica de diagnóstico da lógica de tratamento de falhas críticas e aplicar este método em um estudo de caso de uma estação de compressão de gás.

Esta proposta foi elaborada para contribuir para a análise do controle do SIS, permitindo a verificação de conflitos entre SIFs para o tratamento de falhas em sistemas complexos.

1.3. METODOLOGIA

Este projeto seguiu uma metodologia dividida em três principais etapas:

- Revisão bibliográfica dos conceitos fundamentais relacionados ao contexto do trabalho.
- Geração de modelos para a representação do problema.
- Utilização de ferramentas computacionais para validação das soluções propostas.

Na primeira etapa, de revisão bibliográfica, foi feita uma análise do contexto atual apresentado na introdução, bem como um estudo dos conceitos relacionados ao SIS através da leitura de artigos e das normas relacionadas ao tema. Seguindo a fase de estudos, algumas metodologias de análise de risco mais adotadas na indústria foram verificadas.

Na segunda etapa, passou-se estudar técnicas de modelagem para a representação das SIF’s através do desenvolvimento de modelos de controle em

Rede de Petri (RdP). Feito isso, buscou-se um exemplo de aplicação para realizar o estudo de caso, decidindo-se por uma Estação de Compressão de Gás.

Por fim, na terceira etapa, a partir do uso de ferramentas computacionais, o HPSim, os modelos foram analisados, realizando-se uma série de simulações e de forma iterativa obteve-se os modelos finais de controle. Com o uso do CoDeSys foi possível obter os programas de controle em LD.

2. SISTEMAS INSTRUMENTADOS DE SEGURANÇA

O objetivo deste capítulo é fornecer uma visão geral do que é o SIS e, então, apresentar uma metodologia para o projeto de SIS para que os requisitos de segurança sejam atingidos.

A implantação de um Sistema Instrumentado de Segurança é uma medida de segurança que constitui uma das camadas de proteção independentes previstas na norma IEC 61508 para manter a operação de uma planta ou processo em um nível aceitável de risco. Esta condição só é possível de ser atingida se todas as medidas de redução de risco forem planejadas de forma adequada, pois medidas isoladas ou mal gerenciadas não previnem contra a maioria dos acidentes.

Neste ponto é importante definir o que vem a ser risco no contexto do presente trabalho.

Definição 1. Segundo a norma IEC 61511-1, risco é uma combinação da frequência (ou probabilidade) de um evento perigoso ocorrer e da severidade das consequências do mesmo.

2.1. CAMADAS DE PROTEÇÃO

A estratégia de prevenção de acidentes começa no projeto da instalação que deve ser inerentemente segura. Entretanto, alguns processos se tornam perigosos em determinadas situações que saem de controle, como elevadas temperaturas ou altas pressões. Além disso, quando se trata de substâncias inflamáveis e/ou tóxicas, nem sempre a instalação inerentemente segura justifica os elevados custos

associados. Para estes casos, outras medidas de segurança foram desenvolvidas e as principais delas estão representadas na Figura 1.

Camadas de proteção são dispositivos, sistemas ou ações capazes de prevenir um cenário de consequências indesejáveis. Elas são independentes do evento inicial e da ação ou falha de qualquer outra camada de proteção associada a este cenário e podem ser classificadas como:

a) **Camadas de prevenção:** são projetadas para impedir a ocorrência de situações perigosas. Envolvem:

- Concepção e projeto de procedimentos de controle para prevenir ou reduzir desvios de processos;
- Sistema de controle básico do processo que, por si só, oferece uma segurança significativa através de um projeto adequado de controle;
- Alarmes críticos de alerta ao operador;
- SIS;
- Etc.

b) **Camadas de mitigação:** são aquelas que reduzem as consequências após a ocorrência de um evento perigoso.

- Proteção ativa: sistemas de alívio (válvulas de alívio, discos de ruptura);
- Proteção passiva: sistemas de contenção (diques);
- Planos de emergência para minimizar impacto à planta e à comunidade;
- Etc.

Figura 1 - Camadas de Proteção. Fonte: Adaptado de IEC 61511-1.

2.2. LAYOUT BÁSICO DO SIS

Um Sistema Instrumentado de Segurança (SIS) é constituído por sensores, um ou mais controladores programáveis de segurança (logic solvers) e atuadores, por vezes chamados de elementos finais por alguns autores (LUNDTEIGEN, 2009).

Seu propósito é a monitoração e detecção de eventos potencialmente perigosos no processo industrial, como vazamentos de gás e altas pressões, por exemplo, e alarmar ou executar ações pré-programadas para a prevenção de acidentes ou mitigação de suas consequências aos seres humanos, meio-ambiente e equipamentos a partir do uso de tecnologias modernas como equipamentos elétricos, eletrônicos e eletrônicos programáveis (E/E/EP), conforme ilustrado na Figura 2.

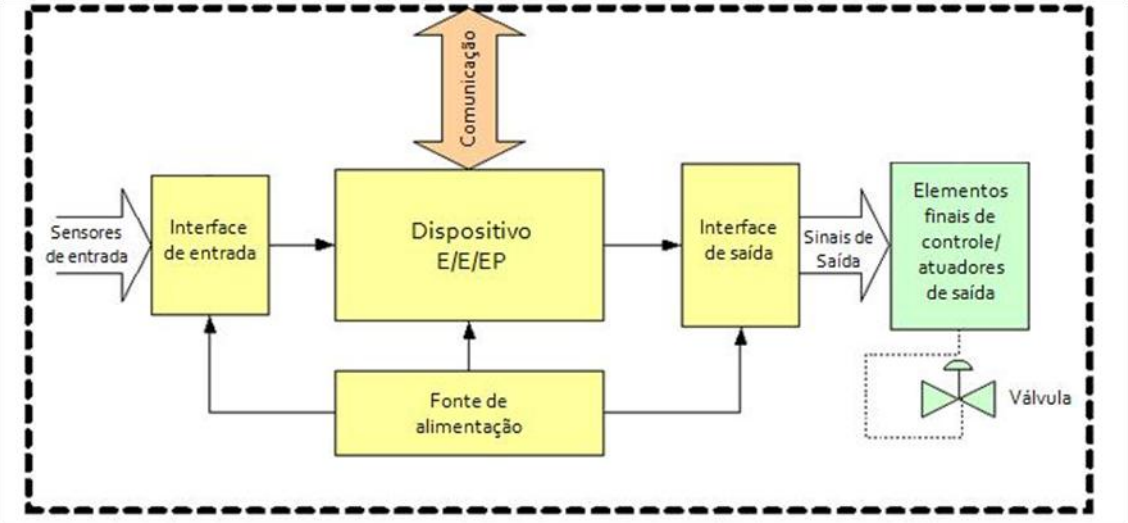


Figura 2 - Exemplo de Estrutura Básica do SIS para o Controle de uma Válvula. Fonte: Adaptado de IEC 61508.

Em um processo industrial, o equipamento de segurança deve ser instalado separadamente do equipamento de controle. Esta separação é necessária para que o SIS possa executar sua função de segurança independentemente do estado do controlador, ainda que este sofra alguma falha.

O equipamento de controle é chamado de Sistema de Controle Básico de Processo (SCBP) e utiliza Controladores Programáveis (CP) para a execução do controle. Dentre suas utilidades estão a leitura de sensores, as funções de controle e o seqüenciamento de eventos, além da geração de comandos para atuadores. Este sistema tem o objetivo de controlar o processo para cumprir as ordens de produção e, quando o risco é muito alto, o acúmulo de funções não é recomendável.

A Figura 3 abaixo ilustra esta configuração de forma esquemática.

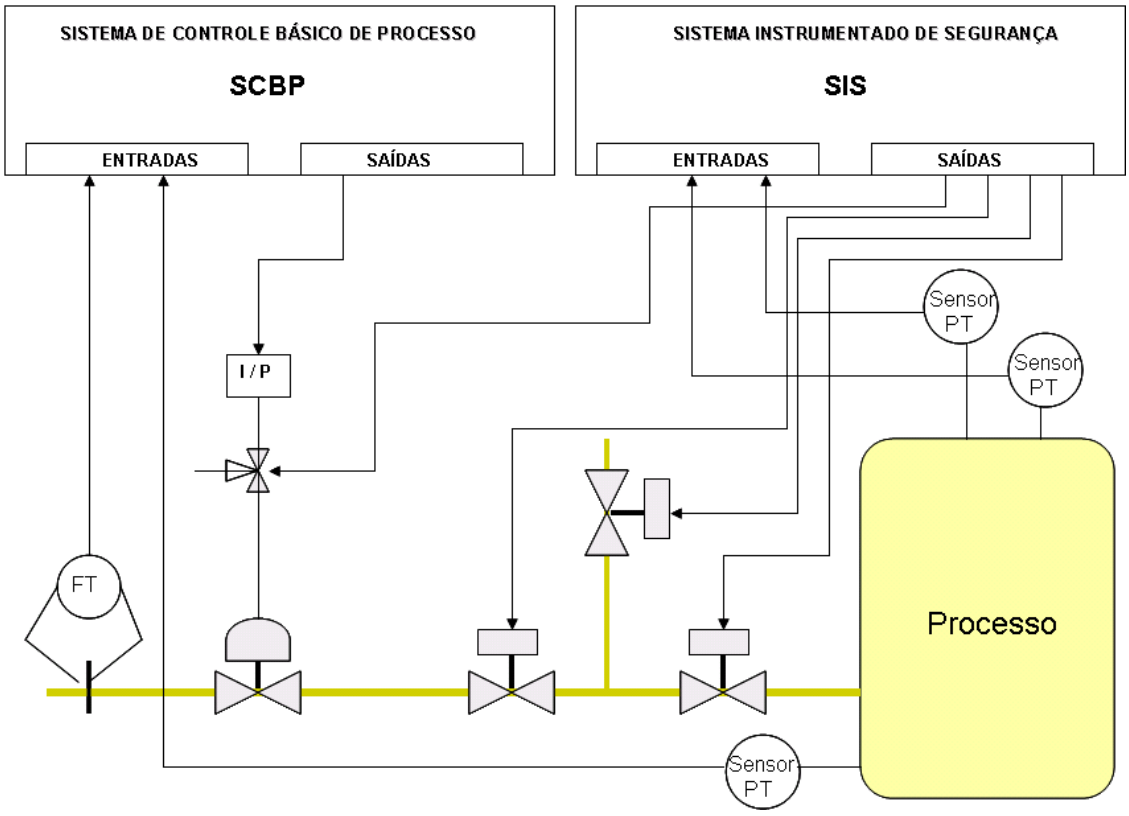


Figura 3 - Separação entre o SCBP e o SIS. Fonte: Adaptado de GOBLE, W.M, 1998.

2.2.1. SIF (Funções Instrumentadas de Segurança)

Sistemas Instrumentados de Segurança, sistemas de shutdown de emergência, sistemas de fogo e gás e intertravamentos de segurança são sistemas que implementam uma ou mais Funções Instrumentadas de Segurança (SIF – *Safety Instrumented Function*).

Definição 2. Uma Função Instrumentada de Segurança (SIF) tem como finalidade detectar uma condição perigosa específica, decorrente da violação de pré-condições e, automaticamente, realizar ações de controle apropriadas para mover o processo para um estado seguro.

2.2.2. SIL (Níveis de Integridade de Segurança)

O conceito de Nível de Integridade de Segurança (SIL – *Safety Integrity Level*) foi introduzido durante o desenvolvimento da norma IEC 61508, direcionada aos sistemas instrumentados que têm que realizar uma função de segurança, a fim de

estabelecer o nível de exigência de uma SIF. Ao todo, são quatro ordens de magnitude de níveis de redução de risco. O SIL 1 tem o menor nível de redução de risco, enquanto o SIL 4 tem o maior nível. Quando se diz que o SIL é de magnitude 0, significa que a implantação de um SIS não é necessária para manter as atividades em um estado seguro, bastando a implantação de sistemas de proteção mais simples.

Tais níveis são baseados no conceito de Probabilidade de Falha sob Demanda (PFD) e de Fator de Redução de Risco (FRR).

Definição 3. O Fator de Redução de Risco (FRR) é definido como a razão entre o risco inerente ao sistema e o risco aceitável. Desta forma:

$$\text{FRR} = \frac{\text{Risco Inerente}}{\text{Risco Aceitável}}$$

Definição 4. A Probabilidade de Falha sob Demanda (PFD), importante para medir a capacidade de redução de risco de um SIS, é definida como:

$$\text{PFD} = \frac{1}{\text{FRR}}$$

Na Tabela 1, a seguir, pode-se verificar quais são estes níveis, e em seguida a descrição dos conceitos citados.

Tabela 1 – Níveis de Integridade de Segurança

Nível de Integridade de Segurança (SIL)	Probabilidade de Falha sob Demanda (PFD)	Fator de Redução de Risco (FRR)
4	0,0001 – 0,00001	10000 – 100000
3	0,001 – 0,0001	1000 – 10000
2	0,01 – 0,001	100 – 1000
1	0,1 – 0,01	10 – 100

Se o FRR é maior que 1, significa que o risco inerente é maior que o risco aceitável e, portanto, deve-se reduzir tais riscos, de forma que o sistema atinja um nível de segurança maior.

A PFD é estimada a partir das experiências dos profissionais que atuam na planta e dos registros históricos, enquanto o risco inerente pode ser determinado seguindo uma metodologia de análise de risco. Já o risco aceitável depende de políticas de gestão de cada empresa e das legislações vigentes em cada região.

2.3. ANÁLISE DE RISCO

Uma análise de risco pode variar desde uma análise de triagem até um estudo detalhado das ameaças e operabilidade, dependendo da complexidade das operações e da severidade dos riscos envolvidos.

O segundo caso envolve um rigoroso exame do processo por uma equipe multidisciplinar composta por engenheiros de processo, mecânicos, elétricos e de instrumentação e também especialistas em segurança e representantes administrativos.

Relações de causa e efeito são consideradas e riscos quantificados para todas as funções de processo e operações. Primeiramente, é importante avaliar os eventos perigosos sem considerar a camada de proteção SIS. Se neste caso o estudo determina que as medidas de segurança sejam insuficientes para proteger contra danos potenciais, o SIS é recomendado (Figura 4). E então, devem ser determinadas quais serão as SIFs necessárias e o SIL exigido para cada uma delas.

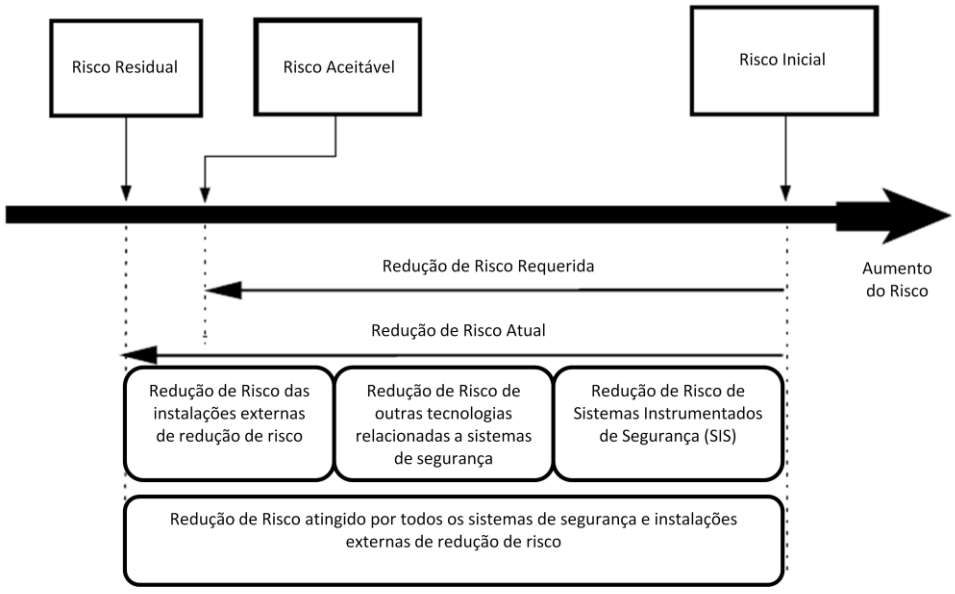


Figura 4 - Redução de riscos – conceitos gerais. Fonte: adaptado da figura A.1 – IEC 61508-5.

A seguir são apresentadas imagens relacionadas ao contexto de riscos e suas classificações. A Tabela 2 define a severidade das conseqüências de um evento e a Tabela 3 apresenta uma forma mais prática de determinar a magnitude da freqüência com a qual um evento perigoso ocorre.

Por sua vez, a Tabela 4 apresenta a classificação dos riscos de acordo com a norma IEC 61508. Fazendo uma associação desta com a Figura 5, pode-se associar facilmente os riscos de grau I e IV nas extremidades do diagrama, enquanto os de grau II e III se localizam na zona de critério variável.

Tabela 2 - Severidade das conseqüências de um evento. Fonte: Adaptado de CRUZ-CAMPA, 2009.

Severidade	Receptor	Descrição dos efeitos potenciais
Categoria 5: Catastrófico	Pessoal	Fatalidade ou invalidez permanente
	Comunidade	Um ou mais lesões severas
	Meio Ambiente	Liberação significativa com sério impacto e possível impacto imediato e a longo prazo
	Equipamentos	Total ou quase total destruição de uma ou mais áreas de processo
Categoria 4: Grave	Pessoal	Um ou mais lesões severas
	Comunidade	Um ou mais lesões leves
	Meio Ambiente	Liberação significativa com sério impacto
	Equipamentos	Danos significativos de uma ou mais áreas de processo
Categoria 3: Crítico	Pessoal	Uma lesão, não grave
	Comunidade	Reclamação de odor e barulho da vizinhança
	Meio Ambiente	Liberação que deve ser notificada as autoridades ou dentro dos limites da legislação
	Equipamentos	Alguns danos com pouca perda de produção
Categoria 2: Leve	Pessoal	Uma lesão leve
	Comunidade	Não afeta a comunidade
	Meio Ambiente	Deve ser registrado mas sem necessidade de comunicar as autoridades ou dentro dos limites da legislação
	Equipamentos	Danos leves sem perda de produção
Categoria 1: Negligível	Pessoal	Sem lesão
	Comunidade	Não afeta a comunidade
	Meio Ambiente	Deve ser registrado mas sem necessidade de comunicar as autoridades ou dentro dos limites da legislação
	Equipamentos	Danos leves sem perda de produção

Tabela 3 - Ordem de magnitude das freqüências. Fonte: Adaptado de CRUZ-CAMPA, 2009.

Ordem de Magnetude das frequências (eventos/ano)	Descrição qualitativa
1.000	Ocorre em todos os turnos
100	Ocorre semanalmente
10	Ocorre mensalmente
1	Ocorre anulamente
1/10	Grande chance de ocorrência numa vida útil da planta. Evento já ocorreu ao menos uma vez em alguma planta similar
1/100	Probabilidade média de ocorrência numa vida útil da planta. Grande chance de ocorrer o evento em 10 plantas similares
1/1.000	Probabilidade baixa de ocorrência numa vida útil da planta. Média probabilidade de ocorrer o evento em 10 plantas similares
1/10.000	Baixa probabilidade de ocorrer o evento em 10 plantas similares
1/100.000	Baixa probabilidade de ocorrer o evento em 100 plantas similares
1/1.000.000	Baixa probabilidade de ocorrer o evento em 1000 plantas similares
1/10.000.000	Chances quase nulas de ocorrer o envento

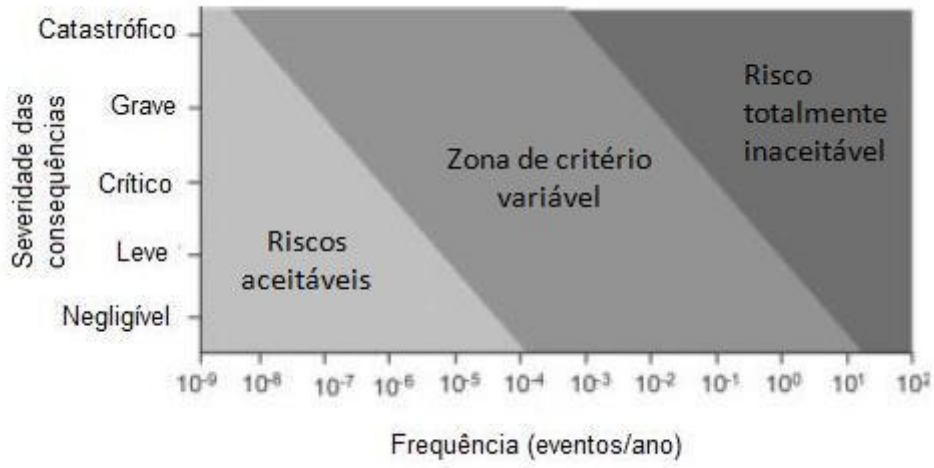


Figura 5 - Diagrama frequência x severidade para representar o critério de aceitação de risco. Fonte: CRUZ-CAMPA, 2009.

Tabela 4 - Classificação de Risco de Acidentes. Fonte: Adaptado de IEC 61508.

Classe de Risco	Interpretação
I	Risco intolerável
II	Risco indesejável, tolerável se a redução de risco é inviável
III	Risco tolerável se os custos para se reduzir os riscos não compensam os ganhos obtidos
IV	Risco negligível

2.3.1. HAZOP

A técnica HAZOP (*Hazard and Operability* – CRUZ-CAMPA, 2009) é um estudo de análise estruturada e sistemática que tem o objetivo de identificar riscos de uma instalação de processo, revisando metodicamente o projeto da unidade ou de toda a fábrica e ainda classificar a exigência por um SIS.

Esta técnica enfoca tanto problemas de segurança como problemas de operabilidade, que embora não sejam perigosos, causam perda de produtividade ou afetam a qualidade do produto.

HAZOP se aplica em qualquer estágio da vida de uma instalação desde que os fluxogramas de engenharia estejam disponíveis (P&ID – Diagramas de Tubulação e de Instrumentação). É, portanto, uma metodologia que identifica desvios operacionais na fase de projeto de novos sistemas ou quando se realiza modificações nas unidades já em operação.

A realização de um HAZOP de boa qualidade depende essencialmente da equipe composta por especialistas experientes e também das informações que devem ser precisas, detalhadas e atualizadas. Estas informações podem ser obtidas através de documentações. As principais são:

- Fluxogramas de engenharia (P&ID);
- Fluxogramas de processo e balanço de materiais;
- Memoriais descritivos, incluindo a filosofia do projeto;

- Folhas de dados de todos os equipamentos, inclusive de válvulas de controle, instrumentos, etc.;
- Dados de projeto, inclusive *set points* das válvulas de alívio, discos de ruptura, etc.;
- Especificações e padrões de materiais das tubulações;
- Diagramas lógicos de intertravamentos;
- Diagrama elétrico;
- Especificações das utilidades (vapor, água de refrigeração, ar comprimido, etc.);
- Entre outras.

A equipe deve ser formada por profissionais com diferentes conhecimentos e experiências para que juntos possam interagir e avaliar os problemas, encontrando soluções criativas e eficazes, evitando que riscos sejam omitidos do estudo. A equipe é estruturada, em geral, da seguinte forma:

- Líder da equipe: esta pessoa deve dominar o conhecimento da técnica HAZOP e conduzir o grupo para que a metodologia seja seguida;
- Engenheiros de processo, de fabricação e de produção: conhecem detalhes do projeto da instalação e da operação;
- Engenheiro de manutenção: conhece detalhes de equipamentos e lida com as falhas destes dispositivos no dia a dia;
- Engenheiro de automação: visto que os processos são automatizados, este profissional desempenha um papel importante.

Com os fluxogramas de engenharia em mãos, a equipe pode analisar os subsistemas identificando os pontos, chamados de nós, que podem apresentar desvios de processo. Feito isto, o grupo gera perguntas sistemáticas que são baseadas em palavras-guia para verificar os desvios possíveis do nó em questão.

Para cada desvio é necessário investigar todas as possíveis causas e suas conseqüências. Deve-se também verificar os recursos de que a instalação dispõe para detectar a ocorrência do desvio. A partir destes levantamentos, a equipe deve propor providências a serem tomadas.

Tabela 5 – Palavras-Guias.

PALAVRA-GUIA	SIGNIFICADO
não/nenhum	completa negação da intenção de projeto
menos/menor	redução quantitativa
mais/maior	aumento quantitativo
também	acréscimo qualitativo
parte de	decréscimo qualitativo
reverso	posição lógica da intenção de projeto
outro que	substituição completa

Sistema: Transferência de Produto Corrosivo do Caminhão para o Tanque				**Equipe:**		**Data:**
Parâmetro: vazão		**Nó:** 01				**Página:** 1/4
Palavra Guia	**Desvio**	**Causas**	**Detecção**	**Conseqüências**	**Providências**	
Mais	Mais Vazão	• Falha no arqueamento do tanque; • Caminhão com quantidade de produto maior do que o tanque comporta; • O tubo de inspeção não é vedado; • O dreno do tanque está entupido; • O dreno do tanque está mais alto do que o topo do tubo de inspeção.	Visual	• Transbordamento do tanque de ácido com perda de produto; • Danos a estrutura do tanque; • Danos aos equipamentos atingidos; • Geração de resíduos químicos; • Gastos na manutenção do tanque e equipamentos; • Gastos na descontaminação do local; • Projeção de ácido sobre o comando das bombas.	• Instalação de um medidor de nível para o tanque; • Instalação de chaves LSH e LSHH; • Envio da nota fiscal do Almoxarifado para o operador da ETA, para checar se a quantidade de ácido do caminhão é a quantidade requisitada; • Elevar o tubo de inspeção; • Vedar o tubo de inspeção com tampa rosqueada e juntas "o-ring"; • Relocar botoeiras de comando.	

(*) LSH – Level Switch High & LSHH – Level Switch High High

Figura 6 - Exemplo de uma planilha de HAZOP. Fonte: AGUIAR.

2.3.2. HAZOP: Indústria de Óleo e Gás

A técnica apresentada aqui é uma das diversas metodologias de análise de riscos e classificação de malhas de segurança para um projeto de SIS, utilizando

como base o HAZOP e normas como a IEC 61508 e IEC 61511, apresentadas mais à frente.

Uma malha de segurança é constituída pelo conjunto de um ou mais iniciadores (linhas de impulso, sensores e transmissores), pelo processador da lógica de controle de segurança, e por um ou mais atuadores (elementos finais de atuação e controle) com a função de prevenir determinado perigo.

Esta técnica é baseada no mapeamento e na determinação de malhas de segurança para a planta a ser analisada, fazendo uma abordagem qualitativa de engenharia de confiabilidade, para avaliação de seu nível de criticidade. Cada malha deve ser classificada segundo uma escala, que envolve diversos parâmetros a serem aqui apresentados, para assim, verificar sua eficiência e adequação na redução de riscos. Deve-se ainda determinar a necessidade de implementação de um SIS para o mesmo, além do SIL requerido para cada SIF em questão.

A primeira ação a ser tomada deve ser uma análise minuciosa da planta estudada. Primeiramente, é preciso considerar que diversas técnicas e mecanismos de proteção integrados aos equipamentos podem reduzir consideravelmente os riscos associados, sem a necessidade de implementação de um SIS, caso tal redução se mostre suficiente. Sendo assim, a etapa inicial deste processo exige que se averigúe a possibilidade de aplicação destes mecanismos para redução de risco.

Se, após a aplicação de tais técnicas, o grau de risco ainda permanecer maior que o aceitável, faz-se necessária a implementação de um SIS para atingir um nível aceitável (Figura 4).

É muito importante que se leve também em consideração fatores como a forma de operação e a localização de cada planta; por exemplo, se a planta é operada manualmente do campo ou remotamente, se a planta é isolada ou próxima a regiões habitadas, etc.

Cada malha deve ser analisada individualmente. Existem malhas mais simples, com apenas um iniciador e um atuador, porém há malhas com mais de um iniciador e/ou mais de um atuador. Nestes casos, deve-se fazer uma combinação

dos componentes para a análise e quando isto ocorrer, cada malha será analisada individualmente considerando que os demais componentes da arquitetura têm perfeitas condições operacionais.

Para o caso abaixo (Figura 7) em que há três iniciadores (I1, I2 e I3) e apenas um atuador (A1), considera-se que existem três diferentes malhas: I1 – A1, I2 – A1e I3 – A1.

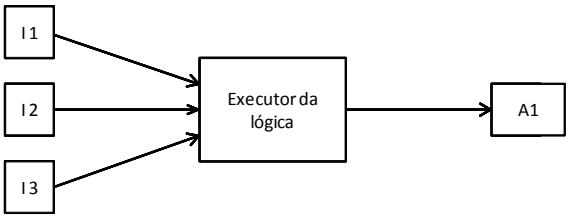


Figura 7 – Exemplo de Arquitetura com mais de um Iniciador.

Por sua vez, quando há um único iniciador e três atuadores, como abaixo (Figura 8), as malhas serão: I1 – A1, I1 – A2, I1 – A3. Neste caso específico, recomenda-se que seja feita uma análise para cada atuador isoladamente, considerando operação normal dos demais componentes, inclusive do iniciador, e ainda, mais um caso de falha apenas no iniciador, com atuadores em condições normais.

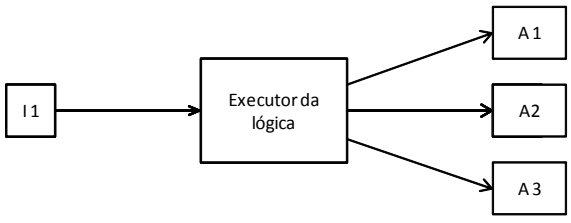


Figura 8 - Exemplo de Arquitetura com mais de um Atuador.

A classificação das malhas de segurança se divide de acordo com a possibilidade de ocorrência de falha sob demanda e de acordo com a possibilidade de ocorrência de falhas espúrias.

A) Possibilidade de Ocorrência de Falha sob Demanda

Esta classificação engloba três aspectos principais: conseqüências sobre a segurança pessoal, sobre a produção e equipamentos, e sobre o meio ambiente.

Primeiramente, é essencial que se faça uma análise prévia quanto à Freqüência sob Demanda, verificando qual é a freqüência com que a malha de segurança é requisitada. Esta análise é feita em todos os casos de classificação. Abaixo é apresentada a descrição deste quesito.

(W) Freqüência sob demanda:

W0 – Não classificada;
W1 – Muito baixa (uma em cada 10 ~ 100 anos);
W2 – Baixa (uma em cada 1 ~ 10 anos);
W3 – Relativamente alta (mais de uma por ano).

A seguir são descritos os aspectos citados anteriormente para a classificação para falha sob demanda.

A1) Segurança Pessoal

Para tal análise, uma das questões a serem levantadas é sobre o potencial de risco para o ser humano quando da falha sob demanda na malha.

(S) Potencial de risco ao ser humano:

S0 – Nenhum;
S1 – Lesões desprezíveis;
S2 – Lesões severas (morte de uma pessoa);

S3 – Morte de várias pessoas;

S4 – Catástrofe.

Outra questão, enquadrada apenas quando se tem nível S1 ou S2, é sobre o período de exposição humana na área em que o evento de risco pode ocorrer.

(A) Grau de presença humana:

A1 – Entre raramente e frequentemente;

A2 – Entre frequentemente e continuamente.

Por fim, apenas para os casos de nível S2, deve-se verificar ainda se é possível que a(s) pessoa(s) presente(s) na área evite(m) se expor ao evento de risco.

(G) Possibilidade de evitar a exposição ao risco:

G1 – Sobre certas condições;

G2 – Dificilmente possível.

Feitas tais considerações, deve-se relacioná-las através do diagrama abaixo, chegando assim, a uma classe de Malha de Segurança, da qual é possível extrair o SIL requerido.

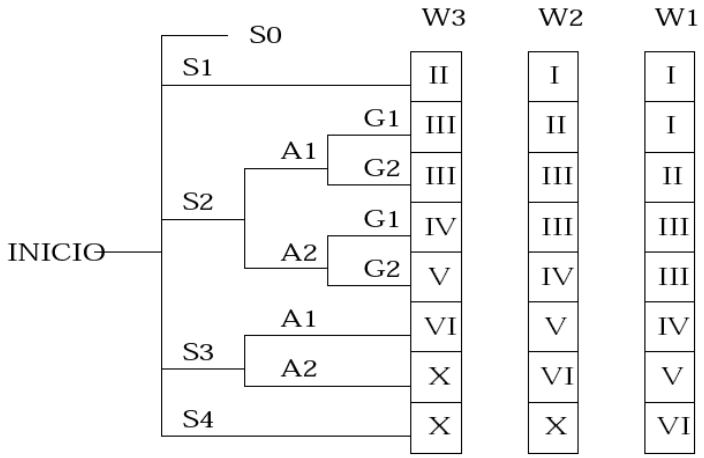


Figura 9 - Diagrama de Risco para Classificação de Malhas de Segurança - Segurança Pessoal.

Para verificação do SIL, é preciso consultar a Tabela 6, a seguir:

Tabela 6 - Relação Classe MS - PFD - SIL - Classe AK, de acordo com as normas IEC 61508 e DIN V 19250 .

Classe de MS	PFD	SIL	Classe AK
I	$\geq 10^{-1}$	-	-
II	$\geq 10^{-1}$	-	1
III	$\geq 10^{-2}$ - $<10^{-1}$	1	2-3
IV	$\geq 10^{-3}$ - $<10^{-2}$	2	4
V	$\geq 10^{-4}$ - $<10^{-3}$	3	5
VI	$\geq 10^{-4}$ - $<10^{-3}$	3	6
X	$\geq 10^{-5}$ - $<10^{-4}$	4	7-8

A2) Perda de Produção e Danos a Equipamentos

Aqui é analisado o potencial de perda de produção e equipamento. Os danos são discriminados de acordo com a necessidade de substituição de peças e dispositivos, custo de reparação, e prejuízo por indisponibilidade.

(L) Potencial de perda de produção e equipamento:

L0 – sem perturbações operacionais ou danos a equipamentos;

L1 – Pequenas perturbações operacionais ou danos reduzidos ao equipamento;

L2 – Moderadas perturbações operacionais ou danos moderados ao equipamento;

L3 – Grande perturbação operacional ou dano grave ao equipamento;

L4 – Perda de produção associada a dano em equipamento essencial.

Caso o resultado seja L0, não é exigida a implementação de uma malha de segurança.

O diagrama de associação de classificações neste caso é:

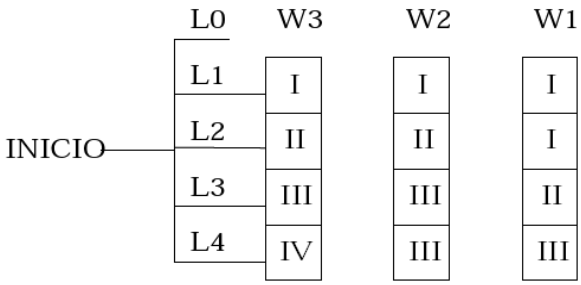


Figura 10 - Diagrama de Risco para Classificação de Malhas de Segurança - Perda de Produção e Danos a Equipamentos.

A3) Meio Ambiente

A classificação para esta categoria se dá de forma similar à anterior. São verificados os danos causados ao meio ambiente, segundo os critérios abaixo.

(E) Potencial de danos ao meio ambiente:

E0 – Sem liberação ou liberação sem conseqüências ao meio ambiente;
E1 – Liberação para dentro dos limites geográficos da companhia com conseqüências ambientais conhecidas;
E2 - Liberação para fora dos limites geográficos da companhia com conseqüências ambientais conhecidas;
E3 - Liberação para fora dos limites geográficos da companhia com conseqüências ambientais desconhecidas.

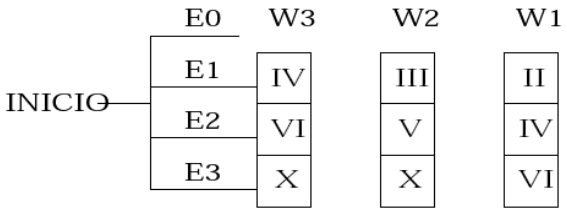


Figura 11 - Diagrama de Risco para Classificação de Malhas de Segurança – Meio Ambiente.

Malhas de segurança que atuam na prevenção de alívio para a atmosfera devem ser classificadas segundo esta categoria. Além disso, é preciso que se atenha às legislações locais, que definem os limites permissíveis, não para fins de

classificação, mas para que se atendam os requisitos legais. Outro fator importante é a imagem da empresa. Se após a classificação a companhia ainda entender que a sua imagem é prejudicada pelas conseqüências das falhas, é preciso aumentar a classificação E para o nível imediatamente superior ao estabelecido, ou seja, de E0 para E1, E2 para E3, etc.

Ao final da análise, deve-se selecionar sempre a maior classificação dentre as três obtidas. Algumas companhias ainda adotam classificações superiores às resultantes, para aumentar o grau de confiabilidade e segurança, desde que estejam dispostas a arcarem com os custos associados a tal decisão.

Para as classes de II a VI, deve-se instalar um pré-alarme, a menos que não seja possível qualquer ação corretiva por parte do operador.

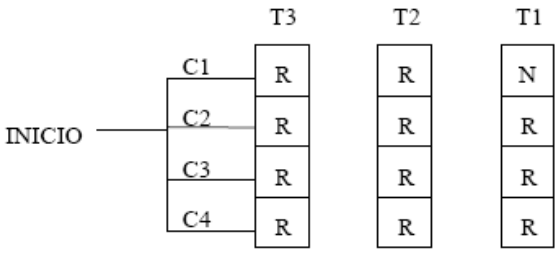
Pode ser necessário ainda, em alguns casos, que se aplique uma tolerância a falhas ocultas, utilizando um sistema de votação 1oo2, no qual, havendo falha em um dos componentes da malha, o segundo pode atuar.

B) Possibilidade de Ocorrência de Falhas Espúrias

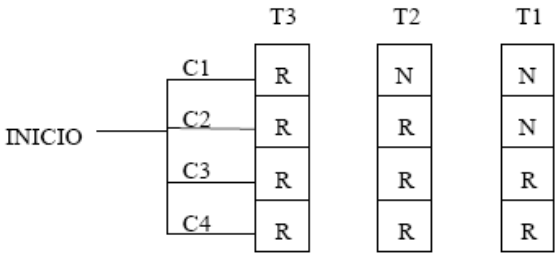
Falha espúria é aquela cuja ocorrência causa a atuação de pelo menos um atuador, sem que tenha ocorrido realmente um evento iniciador que o demandasse.

Para esta análise, primeiramente é estabelecida uma tolerância das malhas de segurança a falhas aparentes. Esta tolerância deve reduzir a ocorrência de falhas aparentes a níveis desprezíveis. O critério adotado é baseado nos próximos três diagramas apresentados a seguir, onde R significa que a implementação de tolerância a falha aparente é recomendada, e N que a mesma não é recomendada.

- CTFA < US$ 1.000,00



- US$ 1.000,00 < CTFA < US$ 10.000,00



- para US$ 10.000,00 < CTFA < US$ 100.000,00

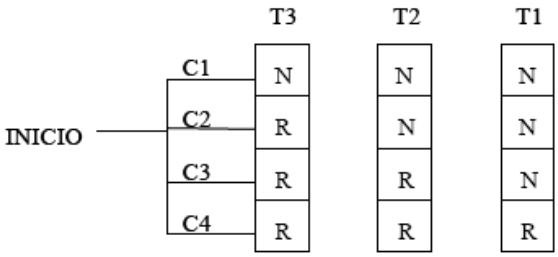


Figura 12 - Diagrama para Classificação de Malhas de Segurança - Análise de Falhas Aparentes.

Os critérios que aparecem no diagrama são:

(C) Potencial de perda de produção, e demais conseqüências associadas, em caso de falha aparente da malha de segurança (CFA):

C1 – custo < US$100.000,00;

C2 – US$100.000,00 < custo < US$1.000.000,00;

C3 - US$1.000.000,00 < custo < US$10.000.000,00;

C4 – custo > US$10.000.000,00.

(T) Frequência de falhas aparentes (TFA):

T1 – Muito baixa (uma em cada 10 ~ 100 anos);
T2 – Baixa (uma em casa 1 ~ 10 anos);
T3 – Relativamente alta (mais de uma por ano).

Quando for recomendada a implementação de tolerância a falha espúria, deve-se implementar a malha em questão com redundância 2oo2.

Para o caso de se exigir tolerâncias, tanto a falha espúria, como a falha sob demanda, deve-se implementar redundância 2oo3 para os iniciadores e para os relés que acionam os equipamentos.

Na **Erro! Fonte de referência não encontrada.** a seguir tem-se um diagrama esquemático de todo o processo realizado por esta metodologia para classificação das malhas.

2.4. NORMAS

Os controladores lógicos programáveis (CLP’s) ganharam a confiança do mercado graças a sua praticidade e confiabilidade. Então, passaram a ser amplamente empregados nas aplicações industriais e surgiram diversas normas para regulamentar os projetos e implementação destes controles programáveis.

2.4.1. Norma IEC 61131

A norma IEC 61131 foi publicada pela primeira vez em 1992 e atualizada no ano de 2003. Ela estabelece padrões para os controladores lógicos programáveis e é dividida em oito partes:

IEC 61131/1 - Informações gerais

IEC 61131/2 - Requisitos de hardware

IEC 61131/3 - Linguagens de programação

IEC 61131/4 - Guia de orientação ao usuário

IEC 61131/5 - Comunicação

IEC 61131/6 - Comunicação via fieldbus

IEC 61131/7 - Programação utilizando a lógica fuzzy

IEC 61131/8 - Guia para implementação das linguagens

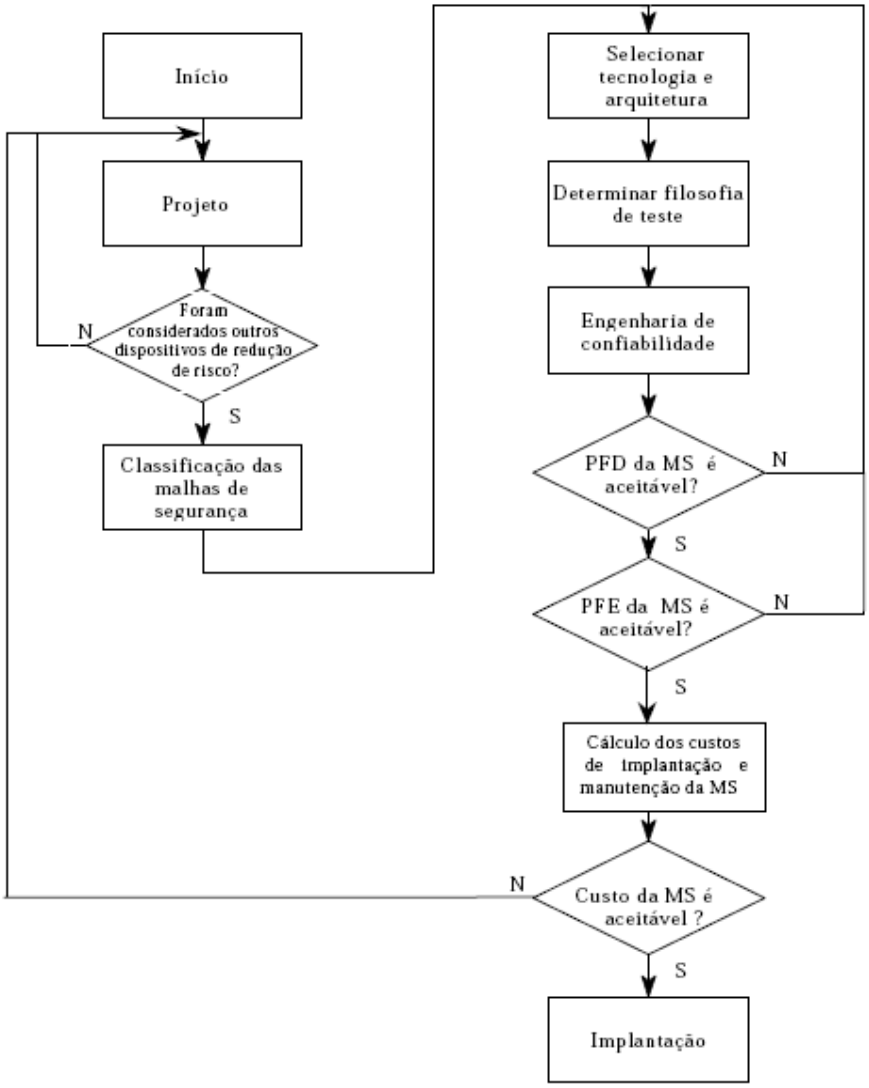


Figura 13 - Fluxograma das Etapas de Projeto do SIS.

Os algoritmos de controle a serem desenvolvidos neste projeto deverão seguir a norma IEC 61131-3, cujo escopo direciona-se às linguagens de programação. A edição atual desta norma estabelece padrões às seguintes linguagens direcionadas a PLCs (Controladores Lógicos Programáveis):

Ladder Diagram (LD): é uma linguagem de programação gráfica que representa um programa. A lógica ladder foi adotada pela facilidade encontrada pelos profissionais de trabalhar com esta lógica devido à similaridade com os circuitos elétricos a relés.

Function Block Diagram (FBD): é um diagrama que descreve uma função entre variáveis de entrada e saída. A função é descrita como um conjunto de blocos elementares. As variáveis de entrada e de saída são conectadas aos blocos por linhas com uma sequência definida e a saída de um bloco pode estar ligada à entrada de outro.

Structured Text (ST): é uma linguagem de alto nível estruturada em blocos e que, sintaticamente lembra linguagens procedurais como C, Pascal, etc.

Instruction List (IL): é uma linguagem de baixo nível, que lembra assembly. É o nível mais básico das linguagens de programação. Todas as outras linguagens podem ser facilmente convertidas para programas IL.

Sequential Function Chart (SFC): é definida por uma sequência de passos ativos e inativos, sendo que apenas os passos ativos podem ser executados. Uma etapa pode ser ativa por apenas dois motivos: ser um passo inicial, conforme determinado pelo programador, ou ser ativado em um ciclo e não desativado até então. Os componentes básicos de um grafo SFC são: passos com ações associadas, transições com condições lógicas associadas e arcos orientados entre passos e transições.

Todas estas linguagens possuem elementos comuns da IEC 61131-3. Suas variáveis e chamadas de função são definidas por estes elementos, de forma que diferentes linguagens podem ser usadas no mesmo programa.

2.4.2. Norma IEC 61508

A norma IEC 61508, intitulada "*Functional safety of electrical/electronic/programmable electronic safety-related systems*", está focada na segurança funcional, alcançada pelos SISs que são implementados utilizando tecnologia elétrica/eletrônica/eletrônica programável (E/E/EP).

Esta norma é composta por sete partes, conforme ilustra a Figura 14:

IEC 61508-1 – Requisitos gerais: define o modelo de ciclo de vida de segurança. A norma emprega técnicas quantitativas e qualitativas para identificar os riscos de processos.

IEC 61508-2 – Requisitos para sistemas de segurança E/E/EP: fornece um método para o desenvolvimento dos requisitos do sistema de segurança E/E/EP;

IEC 61508-3 – Requisitos de software: fornece diretrizes para o desenvolvimento dos requisitos dos softwares utilizados no sistema de segurança;

IEC 61508-4 – Definições e abreviações: contém definições, abreviações e terminologias utilizadas nos processos de segurança;

IEC 61508-5 – Exemplos de métodos na determinação do SIL: fornece uma abordagem formal para determinar o SIL do sistema de segurança;

IEC 61508-6 – Diretrizes para aplicar as partes 2 e 3;

IEC 61508-7 – Visão geral das técnicas e medidas: fornece detalhes das técnicas e medidas de segurança relevantes.

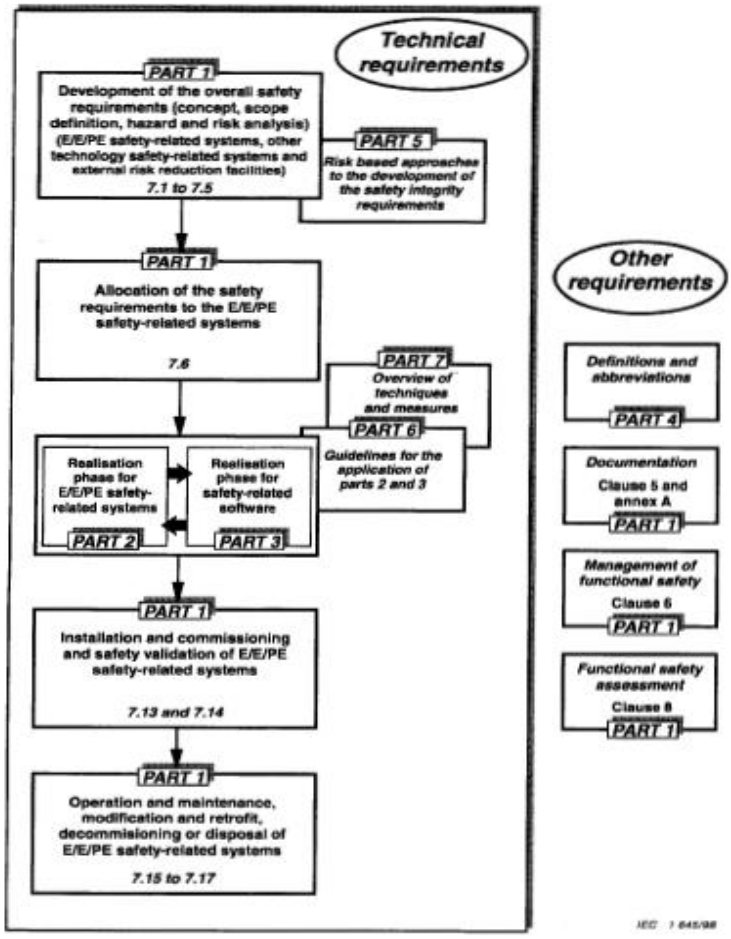


Figura 14 - Estrutura geral da IEC 61508. Fonte: IEC 61508.

2.4.3. Norma IEC 61511

A norma IEC 61511, intitulada "*Functional safety: Safety instrumented systems for the process industry sector*" é equivalente à norma ANSI / ISA 84 e apresenta os requisitos para a especificação, projeto, instalação, operação e manutenção de um SIS para a indústria de processos, de forma a estabelecer e/ou manter o processo em um estado seguro.

De acordo com a Figura 15, esta norma consiste das seguintes partes:

IEC 61511-1 – estrutura, definições, sistema, requisitos de hardware e software;

IEC 61511-2 – diretrizes para a aplicação da IEC 61511;

IEC 61511-3 – diretrizes para a determinação dos níveis de integridade de segurança (SIL) requisitados.

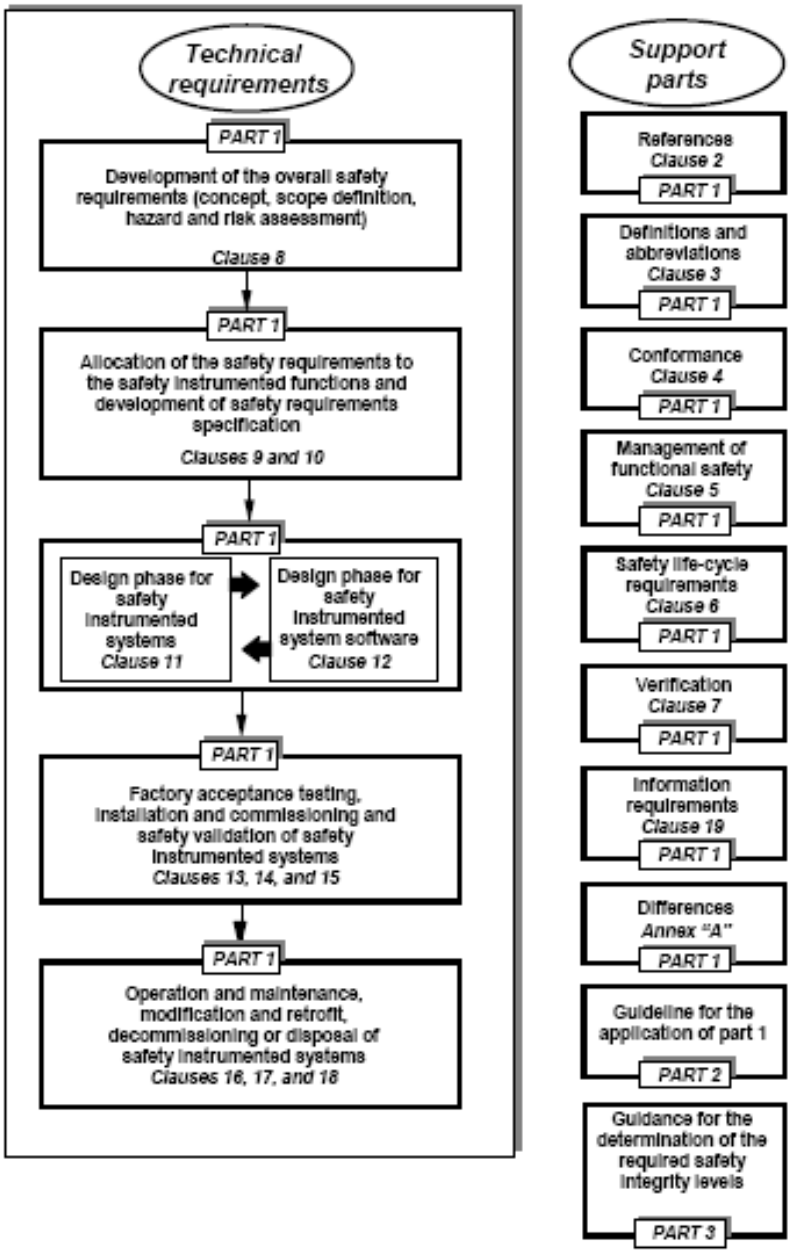


Figura 15 - Estrutura geral da IEC 61511. Fonte: IEC 61511.

2.4.4. ISO 14001

A ISO 14001 é uma das diversas normas da série ISO 14000, desenvolvida pela International Organization for Standardization (ISO) e tem como foco a proteção

ao meio ambiente e a prevenção da poluição de acordo com as necessidades sócio-econômicas do mundo atual.

2.4.5. OHSA 18001

A OSHA 18001 consiste em um sistema de gestão que tem o foco na saúde e na segurança ocupacional. Esta é uma ferramenta disponível para que as empresas possam melhorar e controlar os níveis de desempenho da saúde e de segurança do trabalho.

3. REDE DE PETRI

Uma Rede de Petri (RdP) é uma ferramenta para a modelagem e projeto de sistemas, utilizando uma representação matemática do mesmo, sendo uma extensão das máquinas de estados finitos. A análise da rede de Petri permite avaliar a estrutura e o comportamento dinâmico da modelagem. O resultado desta avaliação pode levar a melhorias ou mudanças no sistema.

Pode ser usada para modelar a ocorrência de diversos eventos e atividades em um sistema. Em particular, pode modelar o fluxo de informação ou outros recursos dentro de um sistema

Eventos são ações que acontecem num sistema. A ocorrência desses eventos é controlada pelo estado do sistema, descrito por um conjunto de condições. Uma **condição** é um predicado ou descrição lógica do estado do sistema. Dessa forma, uma condição pode ser verdadeira ou falsa. Uma vez que eventos são ações, eles podem ocorrer. Para que um evento ocorra, pode ser necessário que certas condições sejam verdadeiras. Estas são denominadas de **pré-condições** do evento. A ocorrência de um evento pode tornar as pré-condições falsas e pode tornar outras condições verdadeiras, chamadas **pós-condições**.

Condições são modeladas por lugares numa rede de Petri, e eventos são modelados por transições. As entradas de uma transição são as pré-condições do correspondente evento. As saídas são as pós-condições. A ocorrência de um evento

corresponde ao disparo da transição a ele relacionada (Adaptado de MORELLE). A seguir, uma definição formal da RdP.

Definição 5. uma Rede de Petri R é uma quíntupla R = (P, T, I, O, K), onde P = {p1, p2,...,pn} é um conjunto finito não-vazio de lugares, T = {t1, t2,..., tm} é um conjunto finito não-vazio de transições. I : T → P é um conjunto de *bags* que representa o mapeamento de transições para lugares de entrada. O : T → P é um conjunto de *bags* que representa o mapeamento de transições para lugares de saída. K : P → N é o conjunto da capacidades associadas a cada lugar, podendo assumir um valor infinito (FRANCÊS, 2003).

4. PROPOSTA

Usualmente, a programação dos CLP's de Segurança se dá de forma direta, através de iniciadores, lógica de controle e elementos finais, sem qualquer divisão entre a identificação das SIF's e seu tratamento.

Este trabalho, por sua vez, vem trazer uma nova proposta de desenvolvimento destes algoritmos, apresentando uma abordagem modular de estruturação dos mesmos de forma que haja uma separação das entradas e saídas físicas para com as lógicas de controle que, por sua vez, são aqui separadas em camadas de Diagnose e de Tratamento das SIF's de um SIS. Desta forma, é proposta aqui uma substituição à estrutura formal estabelecida, citada acima, por uma modelagem que divide a camada lógica, como citado. Isto vai ao encontro do que é recomendado pela norma IEC 61508, com a definição de métodos formais de desenvolvimento de especificações técnicas para a modelagem dos algoritmos de controle dos Sistemas Instrumentados de Segurança.

Não obstante, propõe-se ainda o desenvolvimento destes algoritmos baseados em RdP para, posteriormente, fazer sua transcrição nas linguagens citadas na IEC 61131-3, como o LD, por exemplo.

A grande vantagem da utilização da RdP para o desenvolvimento dos algoritmos é que, através desta linguagem, é possível que se faça a divisão das camadas físicas de entrada e saída dos sensores e atuadores, para com a camada

de controle, com a Diagnose e o Tratamento, de maneira que seja permitida a utilização das boas práticas envolvendo esta linguagem, para análise, não favorecida nos modelos formais de diagramas lógicos.

A RdP é uma linguagem amplamente difundida e de alta funcionalidade, sendo uma ferramenta formal, matemática, que permite uma análise profunda das lógicas de controle a ela relacionadas, bem como de suas boas propriedades, como vivacidade, segurança dos algoritmos, alcançabilidade de estados, entre outras. Desta forma, esta linguagem permite a verificação e análise dos estados alcançáveis, de maneira formal, permitindo ainda a detecção e correção de falhas nos algoritmos de maneira mais segura, evitando assim que haja erros de programação e, consequentemente, falhas na atuação do CLP de Segurança.

Além disso, a RdP permite ainda, a migração para as linguagens da IEC 61131-3 de uma maneira sistemática. A migração dos algoritmos desenvolvidos em RdP para as linguagens da IEC 61131-3 inclusive é hoje fruto de estudos e já existem propostas de metodologias e até mesmo modelos de software que permitem uma transcrição de maneira sistêmica.

Além das funcionalidades citadas a respeito da RdP, a abordagem incluindo diagnose e tratamento das SIF`s também contribui para a organização da programação, bem como para que se tenha maior confiabilidade e que se evite falhas de programação e interferência quando da atuação de diversas SIF`s simultaneamente. A estrutura proposta segue o esquema da Figura 16 a seguir. Em adição, é possível ainda ter uma melhor visualização desta proposta de substituição, através do exemplo, na Figura 24.

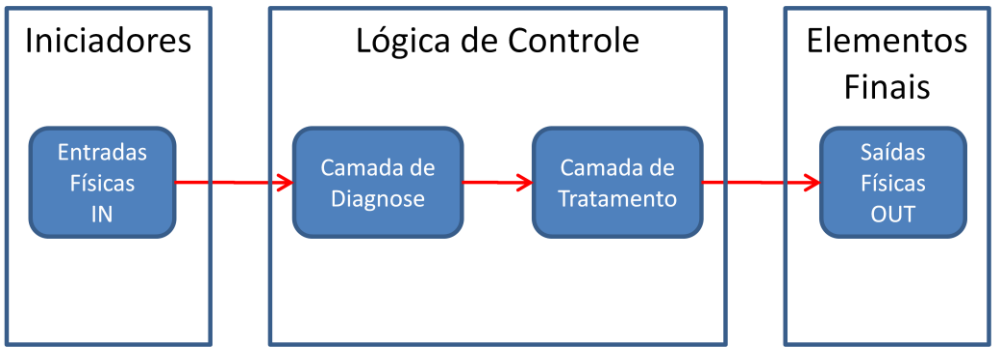


Figura 16 - Estruturação do programa de controle

Como se pode verificar, há uma clara separação em quatro diferentes módulos na estruturação da programação. O primeiro módulo é o de entradas físicas. Nele são inclusos cada um dos iniciadores das lógicas de controle. Desta forma, temos o registro da parte física que iniciará as ações das SIF's.

Em seguida observa-se a região de Diagnose, que consiste na comunicação entre as entradas físicas que, atendendo a certas condições identificam a necessidade de atuação de determinada SIF.

Após a camada de Diagnose de cada SIF está a de Tratamento que são as medidas que devem ser tomadas para estabelecer uma situação segura, ou seja, deve-se passar à lógica de controle. Desta forma, para cada SIF identificada na Diagnose, passa-se a indicar todas as ações que envolvem os atuadores que são representados numa camada de saídas físicas.

Com este tipo de modelagem, temos uma clara divisão entre as entradas físicas e as internas, inseridas na lógica de controle, o que permite uma melhor visualização de cada um dos iniciadores e dos atuadores de forma isolada, ou ainda em conjunto através das SIF's. Isto permite uma melhor representação de todos os dispositivos envolvidos no projeto como um todo, bem como a relação entre estes elementos existentes. Desta forma, a estrutura do programa apresenta melhor organização, divisão dos elementos relacionados, eliminação de eventuais conflitos e interferências que possam ocorrer sobre os estados a serem atingidos pelos

elementos finais que sofrem ações de controle de mais de uma SIF de forma simultânea.

4.1. PROCEDIMENTO DE ELABORAÇÃO DOS MODELOS

Para o desenvolvimento dos modelos das SIF's, devem ser realizadas as seguintes etapas, representadas graficamente na Figura 17:

a) **Estudo de Caso / Análise HAZOP (etapa preliminar):** Como já citado neste documento, caso seja necessário o projeto de um SIS, anteriormente ao desenvolvimento dos algoritmos de controle, deve-se passar pela etapa em que se estuda a planta e é feita uma análise de riscos, utilizando o método HAZOP, por exemplo, para o mapeamento de todas as Funções Instrumentadas de Segurança, cujo SIL deve ser determinado, indicando a necessidade ou não de desenvolvimento de um SIS. Esta é uma etapa preliminar à aplicação da proposta em questão, já que não envolve ainda a representação dos modelos nem a elaboração dos algoritmos.

b) **Análise das SIF's (etapa preliminar):** Após a definição das SIF's anterior, é necessário que estas sejam analisadas e que sejam extraídas delas todas as variáveis envolvidas, como entradas e saídas, bem como todas as lógicas de controle, para que seja aplicada a proposta, a partir do próximo item. Portanto, esta é mais uma etapa preliminar.

c) **Desenvolvimento do Modelo em RdP:** A partir dos dados gerados nas etapas anteriores, parte-se para a construção do modelo de cada SIF em RdP, incluindo camadas de Diagnose e Tratamento. Esta etapa deve ser feita separadamente, SIF a SIF, e por partes, como citado abaixo.

   - **Entradas:** Inclusão de todas as entradas da SIF no modelo, incluindo todas as lógicas e pré-requisitos a elas relacionadas

   - **Camada de Diagnose:** programação da primeira camada da lógica de controle. É essencial ter o conhecimento de todos os pré-requisitos para que a SIF seja diagnosticada. No desenvolvimento do modelo, é preciso cruzar todas estas condições, que são representadas pela atuação dos

iniciadores nas entradas, de forma que a SIF somente seja diagnosticada, para posterior tratamento, uma vez que todos os sensores, ou então que parte deles acusem falha no sistema. A lógica por trás disto está diretamente relacionada à condição de votação para atuação de cada SIF, já que cada uma especifica se é necessário que todos, ou apenas um certo número de sensores a ela ligados acusem falha para entrar em atuação.Quando da diagnose de uma SIF, deve-se transmitir um “sinal” para a próxima camada, que dará início ao tratamento em si da mesma.

- **Camada de Tratamento:** Após identificada e diagnosticada uma SIF para atuar, entra-se na camada de tratamento, que direcionará o modelo para gerar o funcionamento de cada um dos elementos finais responsáveis por manter a planta em um estado seguro, para a situação perigosa que a SIF representa. Desta forma, esta camada deve fazer com que todos os atuadores da SIF entrem em funcionamento, conforme especificado, ou seja, respeitando a lógica, a ordem/simultaneidade dos acontecimentos, bem como as lógicas *AND* ou *OR*, intrínsecas ao funcionamento de todos os elementos em conjunto. É importante frisar ainda que é necessário que seja verificada a possibilidade de interferências entre mais de uma SIF relacionada aos mesmos elementos finais, analisando se existe a possibilidade de atuação simultânea de condições concorrentes para um determinado atuador. Além disso, é importante que seja inclusa ainda um “ou inclusivo” para o acionamento, fazendo com que, mesmo que mais de uma SIF requisite uma mesma ação de um único elemento final, ele atue apenas uma única vez, evitando que uma mesma ação seja repetida desnecessariamente.

- **Saídas:** Por fim, incluem-se todas as saídas especificadas de acordo com as SIFs, sem repetição, provenientes da camada de Tratamento, como já dito, evitando interferências.

d) Análise do Modelo em RdP: Uma vez desenvolvido o modelo em RdP, é preciso que o mesmo seja analisado através de simulações, levando em consideração as boas propriedades da RdP (conservatividade, vivacidade,

limitação e reiniciabilidade). Com esta análise, deve-se buscar falhas de modelagem ou de atuação da SIF, bem como ter uma visão local e também global do modelo. Isto faz com que o mesmo tenha muito menos probabilidade de falhas, já que aumenta sua confiabilidade.

e) **Transcrição de RdP para LD (Desenvolvimento dos Algoritmos de Programação):** Após a modelagem em RdP e sua análise, passa-se à segunda etapa, correspondente à sua transcrição para outra linguagem compatível com a IEC 61131-3. Aqui faremos a transcrição para LD, mas este mesmo projeto tem ainda a possibilidade de se representar os programas de controle em FBD ou IL. O ambiente de programação é o CoDeSys, abordado neste documento. A transcrição se dá de forma sistemática, utilizando, neste caso, basicamente as funções de set e reset para as lógicas. O primeiro passo foi a transcrição de todas as transições, cujos requisitos são as marcações, na RdP, dos lugares cujos arcos (orientados, habilitadoras e inibidoras), são direcionados a estas transições. Posteriormente, passa-se às lógicas envolvendo o set e reset dos lugares, onde as marcações devem chegar e sair. As condições para estes acontecimentos envolvem, basicamente, as transições a eles relacionadas.

f) **Verificação e Validação:** Esta etapa consiste na análise e comparação do modelo em RdP e dos algoritmos gerados a partir deste, verificando se as condições de cada SIF são atingidas, simulando os resultados, e comparando-os com as simulações da RdP. Isso faz com que se possa verificar a paridade entre os dois modelos, a eficácia da transcrição, e então, a consistência do projeto.

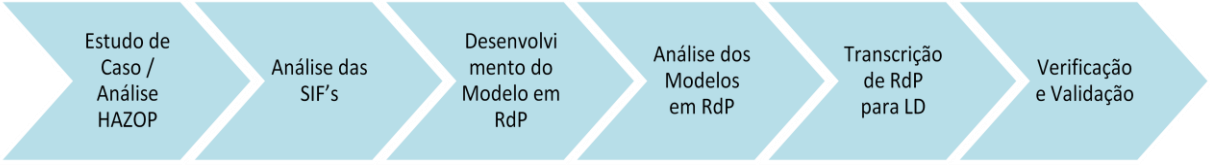


Figura 17 - Etapas para o Desenvolvimento dos Algoritmos de Controle.

A seguir é apresentado o Estudo de Caso sobre o qual foi baseado este trabalho, bem como o desenvolvimento dos algoritmos de controle a ele relacionados, seguindo as premissas desta proposta.

5. ESTUDO DE CASO

O estudo de caso deste trabalho é uma estação de compressão de gás natural. O gás natural é uma mistura de hidrocarbonetos leves. É um produto inflamável e sua manipulação envolve diversos riscos. O grupo escolheu realizar tal estudo devido ao alto grau de riscos da planta, de acordo com o contexto em que se insere o trabalho em questão.

Este estudo focará na descrição de Funções Instrumentadas de Segurança (SIF) para o sistema, bem como na análise, segundo a metodologia apresentada anteriormente, da classificação destas SIFs como malhas de segurança para determinação do SIL exigido para implementação do SIS.

5.1 DESCRIÇÃO DO PROCESSO

De forma geral, o gás natural é extraído de uma fonte local e, a partir da mesma, é distribuído aos diversos destinos nos quais será utilizado. O transporte deste gás entre a zona de produção até os consumidores é realizado por tubulações e, muitas vezes, as distâncias envolvidas são grandes e esta condução gera perdas de carga em seus intermédios. Por este motivo, as estações de compressão de gás são necessárias para viabilizar este transporte.

A estação de compressão estudada possui duas linhas de alimentação do gás que, basicamente, é captado da tubulação na zona de sucção e passa por filtros antes de ser comprimido pelos quatro turbocompressores (A, B, C, D) existentes. Os dois filtros trabalham em paralelo, em conjunto com as duas linhas de alimentação. Esta configuração permite uma flexibilidade para a planta, pois quando um filtro está em manutenção o outro pode ser colocado em marcha. O mesmo acontece com as linhas: se uma linha precisa ser isolada, a outra continua alinhada com o filtro em operação.

Uma parte do gás é desviada para o setor de utilidades. Este gás recebe um tratamento para ser usado como combustível e gerar energia elétrica para a planta. Esta operação é necessária, pois a estação se encontra numa região onde uma estrutura de fornecimento de energia elétrica não é disponível.

Após o gás ser comprimido pelos turbocompressores, ele é enviado de volta para o gasoduto na zona de descarga, voltando à linha de transmissão.

A Figura 18 apresenta uma imagem do Diagrama de Processo e Instrumentação (*P&ID – Process and Instrumentation Diagram*) que contém os filtros e as válvulas principais sobre as quais atuarão o SIS.

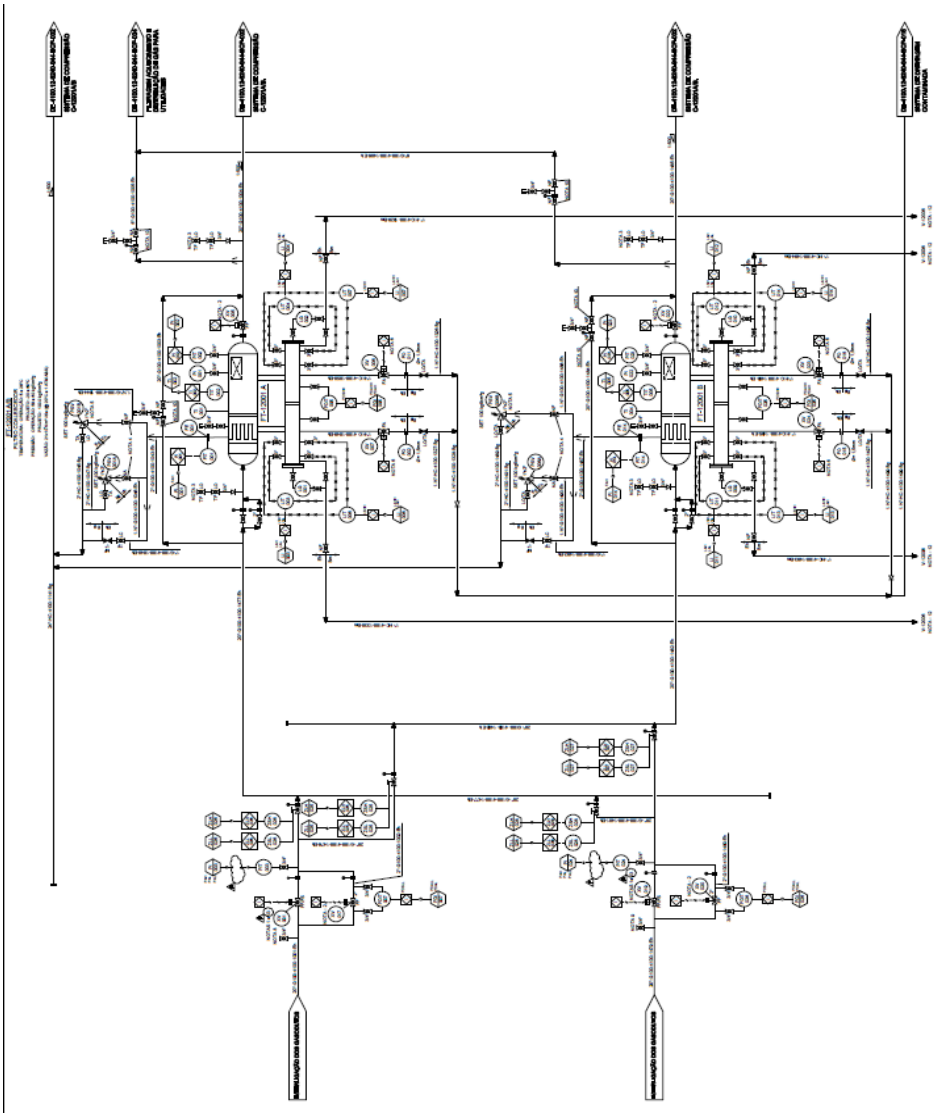


Figura 18 - P&ID da planta contendo os filtros e atuadores do SIS.

5.2 ARQUITETURA DO SISTEMA DE CONTROLE

O sistema conta com um CLP ESC (Estação de Supervisão de Controle) de controle da planta, além de um CLP independente para o SIS, e de outros quatro CLPs integrados a cada turbocompressor. De forma simplificada, a estrutura é ilustrada na Figura 19.

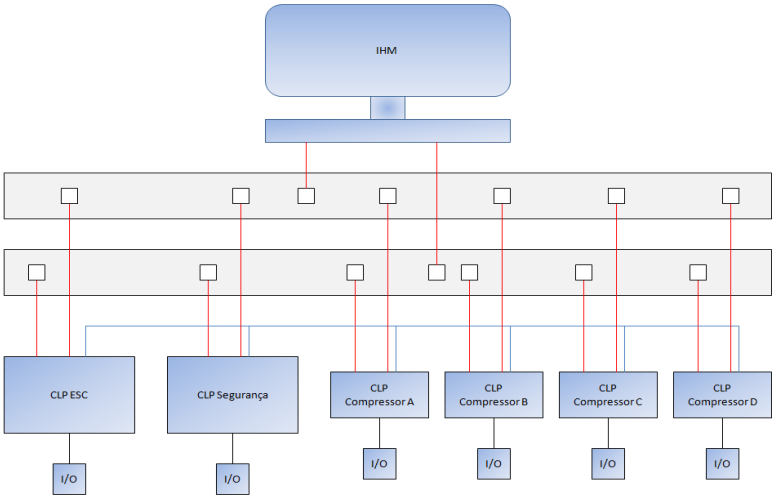


Figura 19 – Arquitetura do Sistema de Controle da Estação.

Como se nota na figura anterior, os CLPs se comunicam entre si, mas não são dependentes uns dos outros, e nem o poderiam ser, já que se trata de sistemas com funcionalidades específicas: controle básico e segurança.

O CLP ESC é responsável pelo controle do funcionamento dos equipamentos das plantas, bem como de sua monitoração, também exercendo algumas funções de segurança. Paralelamente a ele, o CLP SIS, é aquele que controla as SIFs. Os CLPs dos compressores fazem a monitoração destes e, inclusive, podem levar os mesmos ao estado de marcha lenta ou shutdown, de acordo com o estado da planta.

Os CLPs têm sistema de monitoração local e ainda se comunicam também através de rede Ethernet, levando informações a uma sala de controle isolada, com sua própria IHM e com atuação sobre os equipamentos, sendo possível fazer alteração de parâmetros e comandar ações remotamente.

5.3 ANÁLISE DE RISCO

Uma vez esclarecida de forma básica e sucinta o funcionamento e a estrutura da estação de compressão de gás, parte-se agora para a aplicação da metodologia HAZOP de análise, segundo a técnica apresentada anteriormente.

Para isto, serão apresentadas aqui onze SIFs da planta, incluindo o evento que desencadeia sua atuação, seus iniciadores e seus atuadores, ou elementos finais, bem como das conseqüências dos riscos. A análise apresentada englobará tanto a falha sob demanda, quanto a falha espúria. Esta abordagem se dará de forma concisa e objetiva, sendo que apenas para a primeira SIF será feita uma explanação mais a fundo, de forma que, para as SIFs subseqüentes, a análise deve ser semelhante.

Na

Tabela 7 está um modelo utilizado na planta em análise para a descrição das SIFs. O preenchimento desta tabela pode ser tomado como base para a aplicação do HAZOP de forma mais clara, incluindo todos os parâmetros necessários já citados. É neste formato que as SIFs serão aqui apresentadas.

Tabela 7 - Modelo de Preenchimento das SIFs.

Serviço:	
Identificação do(s) iniciadores:	
Identificação do(s) atuador(es) da malha de segurança:	
Consequências de falha na demanda:	
Demanda:	
Segurança pessoal:	Classe associada:
Perda de produção / equipamento:	Classe associada:
Meio ambiente:	Classe associada:
Classificação final para falha na demanda da malha de segurança:	
Consequência de falha espúria da malha de segurança:	
Frequencia de falha espúria:	
Perda financeira associada à ocorrência de falha espúria:	
CTFE:	
Implementar tolerância a falha espúria ? (S/N):	
Esquema de votação selecionado para o(s) iniciadores:	
Esquema de votação selecionado para o(s) atuadores:	

5.3.1 SIF 01

Esta SIF está relacionada ao evento em que a pressão dos filtros A e B das linhas torna-se muito baixa. Os iniciadores que indicam tal fato são os PIT-003 e PIT-024, que são sensores de tomada de pressão da planta.

Quando requisitada, esta SIF terá como atuação o fechamento das válvulas XV-001/017/019/020/003/018, além de dar o comando para o by-pass da estação e colocar os compressores em marcha lenta. Para colocar os compressores neste estado, fecha-se válvulas de alimentação dos mesmos. Com a queda de pressão, os controladores dos compressores automaticamente fecharão válvulas na entrada e na saída dos mesmos, e ainda farão o comando de parada rápida dos mesmos.

A) Falha sob Demanda:

Como visto na metodologia HAZOP, a falha sob demanda analisa questões como a demanda, a segurança pessoal, a perda de produção/equipamento, e o meio ambiente.

Para esta SIF, a demanda selecionada foi W2, considerando que sua freqüência é baixa, ou seja, o evento ocorre uma vez em um período entre 1 e 10 anos.

Feito isto, passa-se à análise da segurança pessoal. O evento em questão, por ter um potencial de risco ao ser humano de invalidez, ou morte de apenas uma pessoa, quando ocorrer, no pior caso, foi classificado como S2 neste critério. Como raramente há pessoas presentes na área de risco quando o evento ocorre, o grau de presença humana na área de risco é A1. Apesar disto, dificilmente pode ser evitada a exposição das pessoas ao risco e, portanto, deve ser ainda classificado o evento como G2. Desta forma, para a segurança pessoal, conforme o diagrama da Figura 20, identificou-se a classe da malha de segurança como sendo equivalente a III e, portanto, o SIL exigido, de acordo com a Tabela 6.

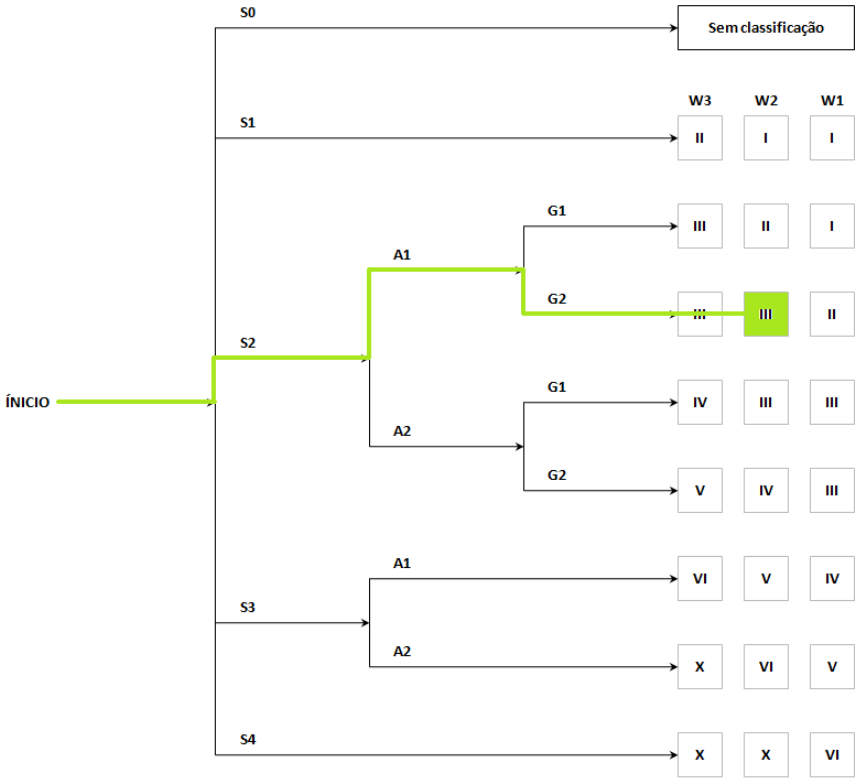


Figura 20 - Definição da Classe para a Segurança Pessoal.

Já com relação à perda de produção ou danos a equipamentos, foi considerado que podem ocorrer moderadas perturbações operacionais, ou danos moderados aos equipamentos, ou seja, L2. Com isso, a classe da malha identificada pela Figura 21 foi equivalente a II, ou seja, SIL 0, o que indica que este caso não exige a implementação de um SIS.

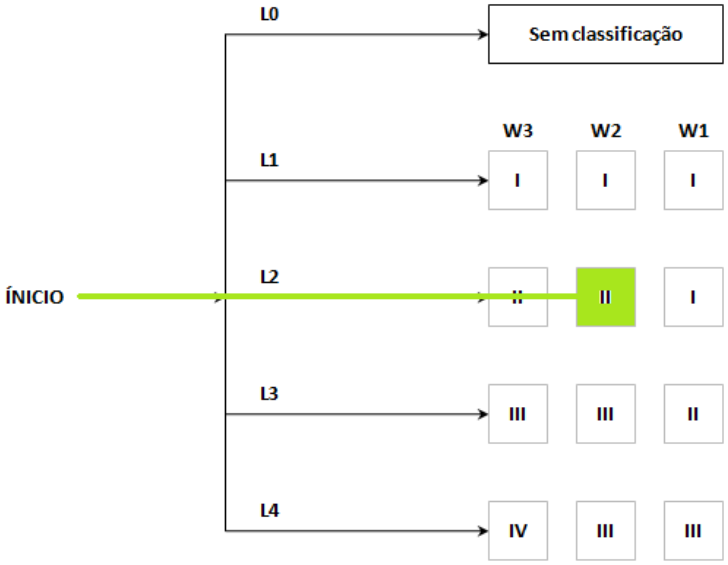


Figura 21 - Definição da Classe para a Perda de Produção/Equipamento.

Para a análise quanto às conseqüências ao meio ambiente, verificou-se que esta SIF pode causar liberação de gás para dentro dos limites geográficos da companhia, com conseqüências conhecidas, com grau E1, portanto. Pela Figura 22, juntamente com a freqüência W2, chega-se à classe III, equivalente ao SIL 1.

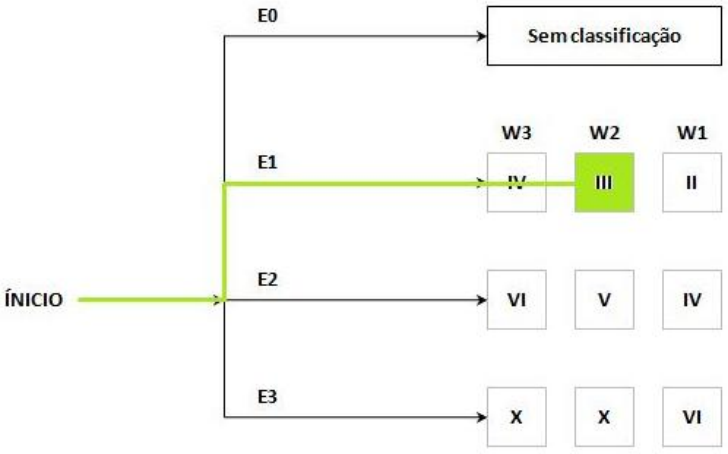


Figura 22 - Definição da Classe para o Meio Ambiente.

Feito isto, o maior SIL exigido pelo SIF, de acordo com a análise, foi SIL 1, e é este que deve ser implementado. Muitas companhias, devido ao alto risco envolvido, ainda assumem uma folga de segurança, aplicando sempre um SIL maior do que aquele definido na classificação. Neste caso, poderia ser definido, por exemplo, um SIL 3. Apesar disto, essa aplicação envolve custos e, para utilizar tal critério, é preciso arcar com os mesmos, ainda que não seja necessário, segundo a metodologia aplicada.

B) Falha Espúria:

Semelhantemente à análise anterior, para esta situação inicia-se também pela definição da freqüência com a qual a falha espúria pode ocorrer. Assim como a falha sob demanda, a freqüência foi verificada como T2, ou seja, baixa com ocorrência uma vez a cada 1 a 10 anos.

Além disso, é importante determinar a perda financeira associada à falha espúria. Para esta SIF, a potencial perda de produção foi C1, com custo menor que US$100.000,00. Outro custo importante é o custo para a implementação da tolerância a falha espúria. Este custo deve ser previsto e, para isso, deve-se ter uma clara noção de quais serão as ações e equipamentos necessários para esta implementação. No caso em questão, a CTFE ficou definida entre US$1.000,00 e US$10.000,00.

De acordo com a Figura 23, obtém-se da combinação de tais parâmetros um valor “N”, indicando que não é recomendada a implementação de tolerância a falha espúria e, portanto, os iniciadores e atuadores devem ter esquema de votação simples 1oo1.

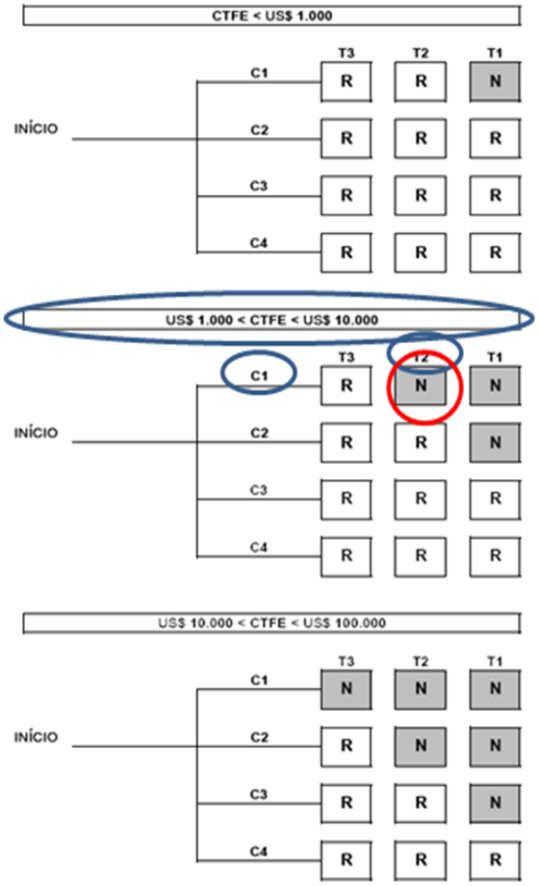


Figura 23 - Definição para Falha Espúria.

A seguir é apresentada a tabela modelo preenchida com os dados analisados e os resultados obtidos para a SIF 01, de forma objetiva

Tabela 8 - SIF 01.

Serviço: pressão muito baixa na entrada dos FT-12001 A/B por vazão alta	
Identificação do(s) iniciadores: PIT-003 / 024	
Identificação do(s) atuador(es) da malha de segurança: fecha XV-001 / 017 / 019 / 020 / 003 / 018, comando para o by-pass da estação e para os compressores serem colocados em marcha lenta.	
Consequências de falha na demanda: queda de pressão do sistema; danos aos elementos internos; vazamento descontrolado; ruido alto; vibração excessiva	
Demanda: W2	
Segurança pessoal: S2 A1 G2	Classe associada: III (SIL 1)
Perda de produção / equipamento: L2	Classe associada: II (SIL 0)
Meio ambiente: E1	Classe associada: III (SIL 1)
Classificação final para falha na demanda da malha de segurança: SIL 1	
Consequência de falha espúria da malha de segurança: fechamento das XV-001/ 017 E XV-019/ 020 com perda de produção	
Frequencia de falha espúria: T2	
Perda financeira associada à ocorrência de falha espúria: C1	
CTFE: U$ 1000 < CTFE < U$ 10.000	
Implementar tolerância a falha espúria ? (S/N): N	
Esquema de votação selecionado para o(s) iniciadores: 1oo1	
Esquema de votação selecionado para o(s) atuadores: 1oo1	

Para as próximas SIFs serão apresentadas apenas as tabelas contendo suas descrições, bem como os parâmetros analisados do HAZOP e os resultados atingidos.

5.3.2 SIF 02

Tabela 9 - SIF 02.

Serviço: nivel muito alto nos FT-12001 A/B	
Identificação do(s) iniciadores: LIT-006/7 E LIT-013/014	
Identificação do(s) atuador(es) da malha de segurança: fecha XV-001 / 017 E XV-019 / 020; Shut-down dos compressores; fecha XV-005 / 022 E XV-003 / 018	
Consequencias de falha na demanda: arraste de condensado para os compressores	
Demanda: W2	
Segurança pessoal: S0	Classe associada: -
Perda de produçào / equipamento: L4	Classe associada: III (SIL 1)
Meio ambiente: E1	Classe associada: III (SIL 1)
Classificação final para falha na demanda da malha de segurança: SIL 1	
Consequencia de falha espúria da malha de segurança: parada indevida dos compressores com perda de produção	
Frequencia de falha espúria: T2	
Perda financeira associada a ocorrencia de falha espúria: C1	
CTFE: U$ 1000 < CTFE < U$ 10.000	
Implementar tolerancia a falha espúria ? (S/N): N	
Esquema de votaçào selecionado para o(s) iniciadores: 1oo1	
Esquema de votaçào selecionado para o(s) atuadores: 1oo1	

5.3.3 SIF 03

Tabela 10 - SIF 03.

Serviço: diferencial de pressão muito alto nos FT-12001 A/B	
Identificação do(s) iniciador(es): PDIT-005 / 025	
Identificação do(s) atuador(es) da malha de segurança: fecha XV-001 / 017 / 019 / 020 / 003 / 018 / 005 / 022, comando para o by-pass da estação e para os compressores serem colocados em Marcha lenta.	
Consequencias de falha na demanda: vazão baixa nos compressores; possiveis danos aos elementos filtrantes	
Demanda: W2	
Segurança pessoal: S0	Classe associada: -
Perda de produçào / equipamento: L2	Classe associada: II (SIL 0)
Meio ambiente: E0	Classe associada: -
Classificação final para falha na demanda da malha de segurança: SIL 0	
Consequencia de falha espúria da malha de segurança: fechamento das XV-001 / 017 E XV-019 / 020 com perda de produção	
Frequencia de falha espúria: T2	
Perda financeira associada a ocorrencia de falha espúria: c1	
CTFE: U$ 1000 < CTFE < U$ 10.000	
Implementar tolerancia a falha espúria ? (S/N): N	
Esquema de votaçào selecionado para o(s) iniciadores: 1oo1	
Esquema de votaçào selecionado para o(s) atuadores: 1oo1	

5.3.4 SIF 04

Tabela 11 - SIF 04.

Serviço: pressão muito alta na descarga dos compressores	
Identificação do(s) iniciador(es): PIT- 206 A/B/C/D	
Identificação do(s) atuador(es) da malha de segurança: shut-down do compressor correspondente	
Consequencias de falha na demanda: possiveis danos aos compressores; possivel fluxo reverso	
Demanda: W2	
Segurança pessoal: S2 A1 G2	Classe associada: III (SIL 1)
Perda de produçào / equipamento: L2	Classe associada: II (SIL 0)
Meio ambiente: E1	Classe associada: III (SIL 1)
Classificação final para falha na demanda da malha de segurança: SIL 1	
Consequencia de falha espúria da malha de segurança: parada indevida do compressor correspondente com perda de produção	
Frequencia de falha espúria: T2	
Perda financeira associada a ocorrencia de falha espúria: C1	
CTFE: U$ 1000 < CTFE < U$ 10.000	
Implementar tolerancia a falha espúria ? (S/N): N	
Esquema de votaçào selecionado para o(s) iniciadores: 1oo1	
Esquema de votaçào selecionado para o(s) atuadores: 1oo1	

5.3.5 SIF 05

Tabela 12 - SIF 05.

Serviço: pressão muito alta no header de descarga	
Identificação do(s) iniciador(es): PIT-006 A/B/C	
Identificação do(s) atuador(es) da malha de segurança: fecha XV-001 / 017 / 019 / 020 / 003 / 018, comando para o by-pass da estação e para os compressores serem colocados em marcha lenta.	
Consequencias de falha na demanda: possiveis danos no header de descarga	
Demanda: W2	
Segurança pessoal: S2 A1 G2	Classe associada: III (SIL 1)
Perda de produçào / equipamento: L4	Classe associada: III (SIL 1)
Meio ambiente: E1	Classe associada: III (SIL 1)
Classificação final para falha na demanda da malha de segurança: SIL 1	
Consequencia de falha espúria da malha de segurança: parada indevida dos compressores com perda de produção	
Frequencia de falha espúria: T2	
Perda financeira associada a ocorrencia de falha espúria: C1	
CTFE: U$ 1000 < CTFE < U$ 10.000	
Implementar tolerancia a falha espúria ? (S/N): N	
Esquema de votaçào selecionado para o(s) iniciadores: 1oo1	
Esquema de votaçào selecionado para o(s) atuadores: 1oo1	

5.3.6 SIF 06

Tabela 13 - SIF 06.

Serviço: temperatura muito alta na descarga dos compressores	
Identificação do(s) iniciador(es): TIT-206 A/B/C/D	
Identificação do(s) atuador(es) da malha de segurança: shut down do compressor correspondente	
Consequencias de falha na demanda: possiveis danos no header de descarga	
Demanda: W2	
Segurança pessoal: S1	Classe associada: I (SIL 0)
Perda de produçào / equipamento: L1	Classe associada: I (SIL 0)
Meio ambiente: E1	Classe associada: III (SIL 1)
Classificação final para falha na demanda da malha de segurança: SIL 1	
Consequencia de falha espúria da malha de segurança: parada indevida do compressor com correspondente perda de produção	
Frequencia de falha espúria: T2	
Perda financeira associada a ocorrencia de falha espúria: C1	
CTFE: U$ 1000 < CTFE < U$ 10.000	
Implementar tolerancia a falha espúria ? (S/N): N	
Esquema de votaçào selecionado para o(s) iniciadores: 1oo1	
Esquema de votaçào selecionado para o(s) atuadores: 1oo1	

5.3.7 SIF 07

Tabela 14 - SIF 07.

Serviço: pressão muito baixa no gas de utilidades para as turbinas, por vazão alta	
Identificação do(s) iniciador(es): PIT-105	
Identificação do(s) atuador(es) da malha de segurança: fecha XV-125	
Consequencias de falha na demanda: falha na contenção de possiveis vazamentos	
Demanda: W2	
Segurança pessoal: S2 A1 G2	Classe associada: III (SIL 1)
Perda de produçào / equipamento: L2	Classe associada: II (SIL 0)
Meio ambiente: E1	Classe associada: III (SIL 1)
Classificação final para falha na demanda da malha de segurança: SIL 1	
Consequencia de falha espúria da malha de segurança: perda de produção por parada das turbinas	
Frequencia de falha espúria: T2	
Perda financeira associada a ocorrencia de falha espúria: C1	
CTFE: U$ 1000 < CTFE < U$ 10.000	
Implementar tolerancia a falha espúria ? (S/N): N	
Esquema de votaçào selecionado para o(s) iniciadores: 1oo1	
Esquema de votaçào selecionado para o(s) atuadores: 1oo1	

5.3.8 SIF 08

Tabela 15 - SIF 08.

Serviço: pressão muito alta de gás de utilidades para geração	
Identificação do(s) iniciador(es): PIT-106 A/B	
Identificação do(s) atuador(es) da malha de segurança: fecha XV-102 A/B	
Consequencias de falha na demanda: danos a linhas e acessorios, desarme dos geradores.	
Demanda: W2	
Segurança pessoal: S0	Classe associada: -
Perda de produçào / equipamento: l4	Classe associada: III (SIL 1)
Meio ambiente: E1	Classe associada: III (SIL 1)
Classificação final para falha na demanda da malha de segurança: SIL 1	
Consequencia de falha espúria da malha de segurança: parada indevida da estação	
Frequencia de falha espúria: T1	
Perda financeira associada a ocorrência de falha espúria: C2	
CTFE: U$ 1000 < CTFE < U$ 10.000	
Implementar tolerância a falha espúria ? (S/N): N	
Esquema de votação selecionado para o(s) iniciadores: 1oo1	
Esquema de votação selecionado para o(s) atuadores: 1oo1	

5.3.9 SIF 09

Tabela 16 - SIF 09.

Serviço: pressão muito alta de gas de utilidades para partida das turbinas	
Identificação do(s) iniciador(es): PIT-103	
Identificação do(s) atuador(es) da malha de segurança: fecha XV-130	
Consequencias de falha na demanda: danos a linhas e acessorios, sem partida das turbinas.	
Demanda: W1	
Segurança pessoal: S1	Classe associada: I (SIL 0)
Perda de produçào / equipamento: L1	Classe associada: I (SIL 0)
Meio ambiente: E0	Classe associada: -
Classificação final para falha na demanda da malha de segurança: SIL 0	
Consequencia de falha espúria da malha de segurança: impedimento para partida da estação	
Frequencia de falha espúria: T1	
Perda financeira associada a ocorrencia de falha espúria: c1	
CTFE: U$ 1000 < CTFE < U$ 10.000	
Implementar tolerancia a falha espúria ? (S/N): N	
Esquema de votaçào selecionado para o(s) iniciadores: 1oo1	
Esquema de votaçào selecionado para o(s) atuadores: 1oo1	

5.3.10 SIF 10

Tabela 17 - SIF 10.

Serviço: temperatura alta / baixa na saida dos vent stack's (CM-12001 A/B)	
Identificação do(s) iniciador(es): TIT-302 A/B	
Identificação do(s) atuador(es) da malha de segurança: abre / fecha TV-302 A/B	
Consequencias de falha na demanda: possíveis danos aos vent stack's no caso de não abertura da respectiva TV.	
Demanda: W2	
Segurança pessoal: S0	classe associada: -
Perda de produçào / equipamento: L1	classe associada: (SIL 0)
Meio ambiente: E0	classe associada: -
Classificação final para falha na demanda da malha de segurança: SIL 0	
Consequencia de falha espúria da malha de segurança: perda de produção	
Frequencia de falha espúria: T2	
Perda financeira associada a ocorrencia de falha espúria: C1	
CTFE: U$ 1000 < CTFE < U$ 10.000	
Implementar tolerancia a falha espúria ? (S/N): N	
Esquema de votaçào selecionado para o(s) iniciadores: 1oo1	
Esquema de votaçào selecionado para o(s) atuadores: 1oo1	

5.3.11 SIF 11

Tabela 18 - SIF 11.

Serviço: pressão muito alta / muito baixa do ar no vaso pulmão V-12003	
Identificação do(s) iniciador(es): PIT-506	
Identificação do(s) atuador(es) da malha de segurança: pressão muito alta do ar desliga os compressores de ar. Pressão muito baixa do ar desliga os compressores de gás C-12001 A/B/C/D.	
Consequencias de falha na demanda: perda de produção	
Demanda: W2	
Segurança pessoal: S0	Classe associada: -
Perda de produçào / equipamento: L3	Classe associada: III (SIL I)
Meio ambiente: E0	Classe associada: -
Classificação final para falha na demanda da malha de segurança: SIL 1	
Consequencia de falha espúria da malha de segurança: perda de produção	
Frequencia de falha espúria: T2	
Perda financeira associada a ocorrencia de falha espúria: C1	
CTFE: U$ 1000 < CTFE < U$ 10.000	
Implementar tolerancia a falha espúria ? (S/N): N	
Esquema de votaçào selecionado para o(s) iniciadores: 1oo1	
Esquema de votaçào selecionado para o(s) atuadores: 1oo1	

5.4 PROGRAMAÇÃO DAS SIF'S

5.4.1 HPSim

A ferramenta utilizada para a modelagem dos algoritmos de controle do Sistema Instrumentado de Segurança da Estação de Compressão de Gás em Rede de Petri foi o HPSim.

O HPSim é um software para simulação de RdP que apresenta uma interface intuitiva de fácil utilização. Entre suas vantagens está a possibilidade do acompanhamento da evolução do estado da rede de uma forma gráfica, o que

auxilia no desenvolvimento do modelo e na detecção de erros e este software também é disponibilizado gratuitamente. O software foi utilizado para o desenvolvimento dos modelos em RdP.

5.4.2 Programação em Rede de Petri

A Figura 24 apresenta a visão geral da programação das SIF`s 01 e 02 em RdP. A malha superior representa a SIF 01 enquanto a inferior, a SIF 02. Então, os dois primeiros lugares da região IN representam os iniciadores da SIF 01 (PIT 003 e PIT 024). E os dois últimos nesta região, representam os iniciadores da SIF 02 (LIT 006 e LIT 007).

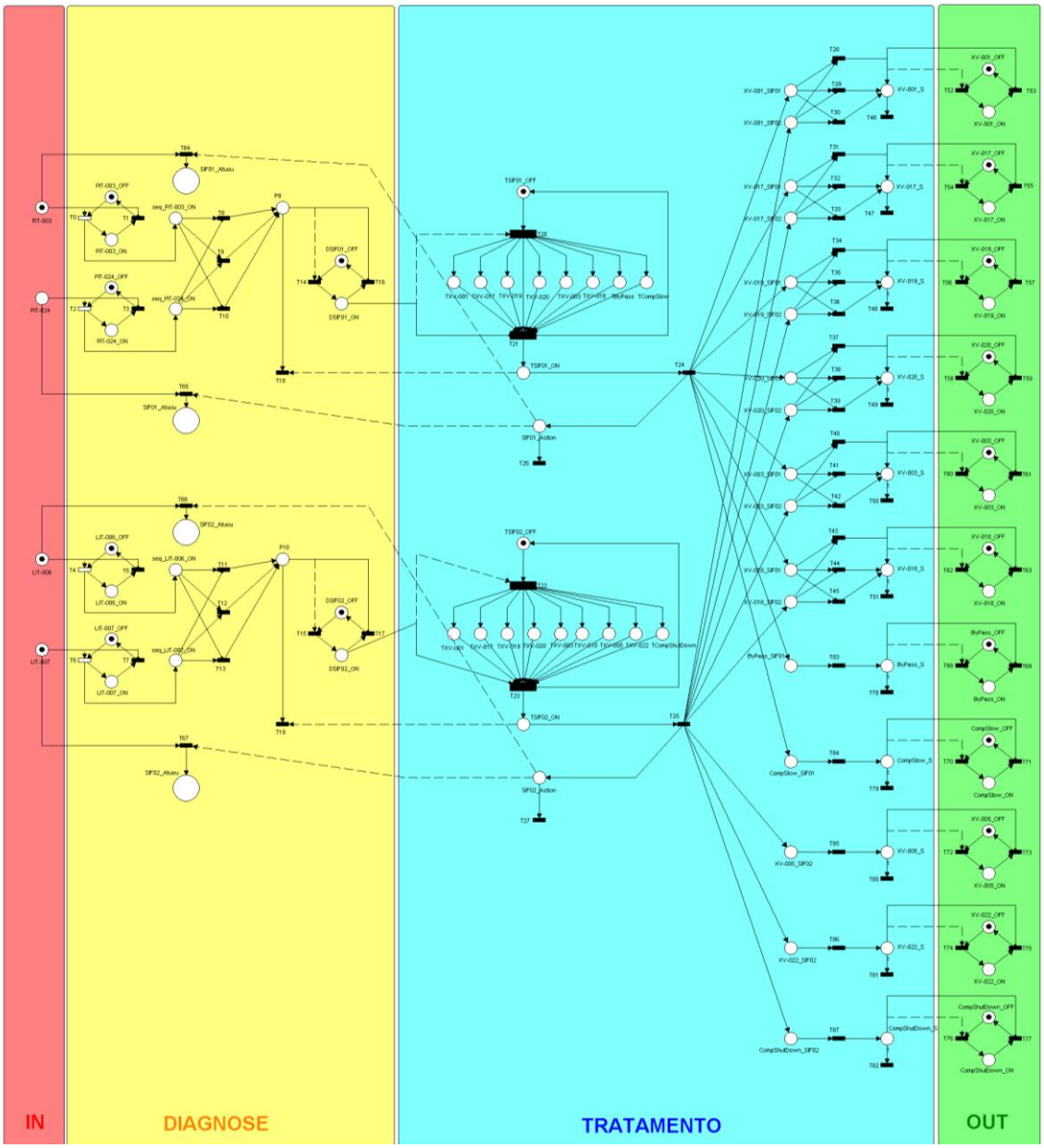


Figura 24 - Visão geral da programação das SIF's em RdP.

Neste item será descrito a SIF 01 com mais detalhes. A SIF 02 funciona de maneira análoga.

A Figura 25 mostra em detalhes os iniciadores da SIF 01 e a região de **Diagnose**. Se um dos iniciadores ou ambos indicarem situação de falha (votação 1oo2), ocorre a diagnose da SIF 01 que é representada pelo lugar DSIF01_ON. No caso abaixo, o iniciador PIT-003 indicou a situação de falha.

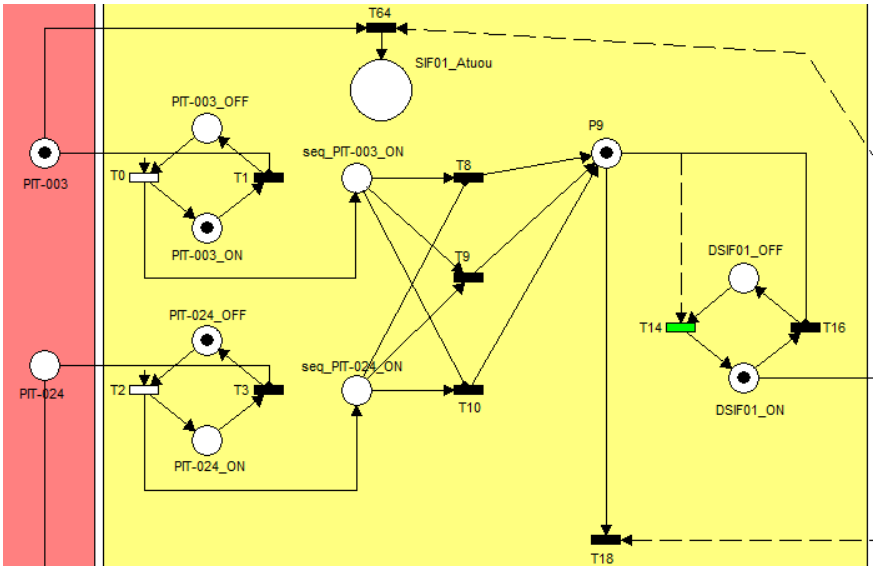


Figura 25 - Detalhe da região de entradas físicas (IN) e de Diagnose da SIF 01.

Uma vez diagnosticada a necessidade de atuação da SIF 01 (DSIF01_ON) a região de tratamento executa a lógica de atuação da SIF para manter a operação em estado seguro. O lugar TSIF01_ON indica que a lógica de **Tratamento** foi executada. A Figura 26 ilustra esta situação.

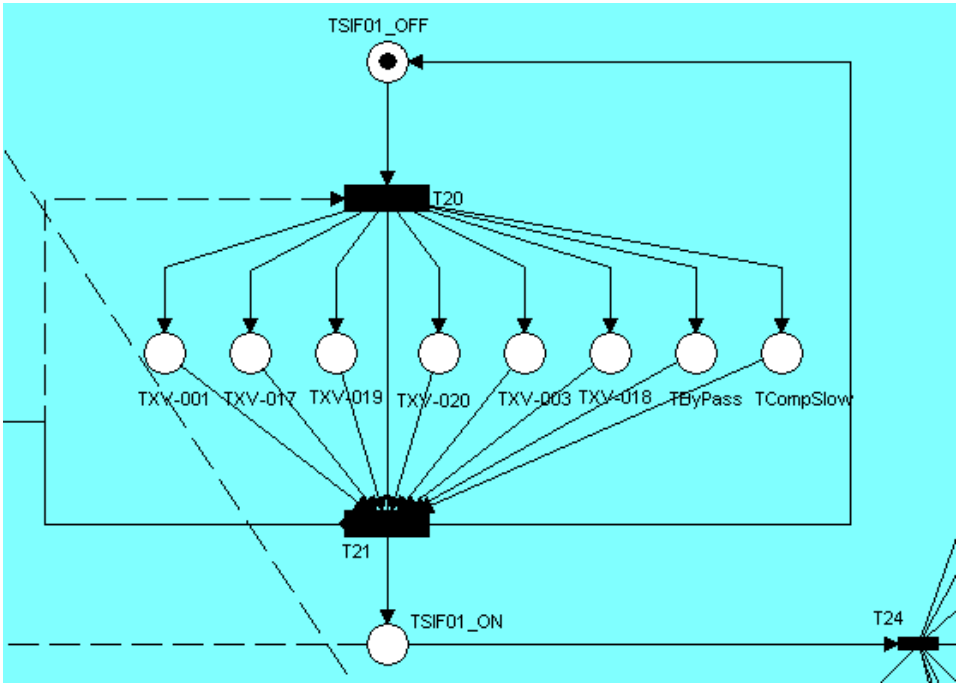


Figura 26 – Região de Tratamento da SIF 01 do tanque.

No entanto, esta lógica foi apenas executada acionando os modelos que representam os dispositivos finais. Portanto, os sinais de controle ainda serão transmitidos aos atuadores físicos. A transição T24 habilita a preparação de todos os atuadores da SIF 01. A Figura 27 representa a interface entre a parte final do tratamento e a saída física da válvula XV 001. Na figura em questão, tanto a SIF 01 como a SIF 02 requisitam o fechamento dessa válvula. Então, caso uma das SIF's ou ambas devam atuar, o lugar XV-001_S indica o resultado do tratamento com relação a esta válvula e dá o set para acionamento da válvula. Finalmente, a transição T52 habilita a saída de comando de fechamento da válvula XV-001 e o lugar XV-001_ON indica que a o sinal foi enviado para a válvula. Esta mesma seqüência ocorre para os outros atuadores.

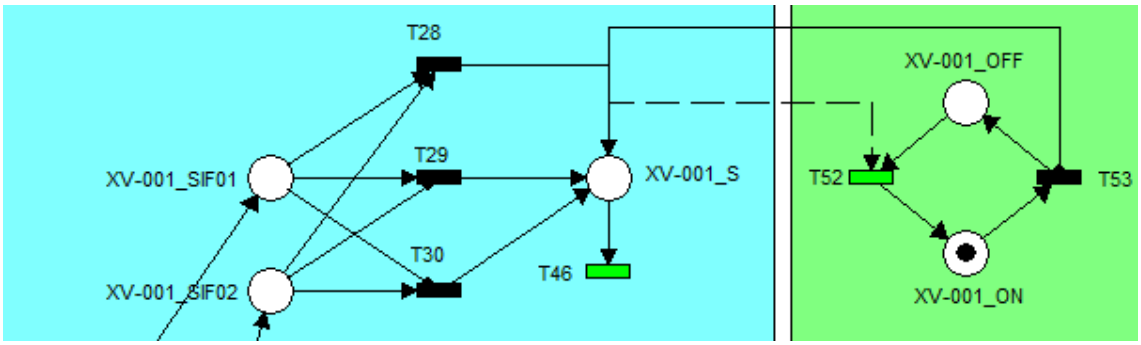


Figura 27 - Detalhe da região de entradas físicas (IN) e de Diagnose da SIF 01 do tanque.

5.4.3 Simulação do Modelo

Após a programação dos algoritmos do SIS relacionados ao exemplo simplificado do tanque, deu-se início à simulação dos mesmos para a validação do modelo e, posteriormente, para a verificação da efetividade da proposta do trabalho.

Devido à forma como se deu a estrutura da rede criada, foi possível simular diversas situações:

- como quando apenas um alarme de uma SIF indica falha;
- quando dois alarmes de uma mesma SIF indica falha;

- quando um alarme de cada SIF indica falha;
- quando um alarme de uma SIF e dois de outra indicam falha;
- quando todos os alarmes das duas SIF’s indicam falha.

Em todas as situações, independentemente de quais fossem os responsáveis pela atuação das SIF’s, o resultado esperado era que se indicasse o diagnóstico das SIF’s correspondentes, de acordo com a realidade desejada. Por exemplo, se mais de um sensor acusar erro para uma SIF, ela deve ser diagnosticada uma única vez, e seu tratamento, da mesma forma, deve atuar uma só vez, já que isto já é um ponto de ação corretivo para ambas as falhas. Em contrapartida, como é o caso do exemplo, se mais de uma SIF vai atuar em um mesmo atuador, mesmo que ambas estejam em atividade, o atuador deve ser acionado uma única vez, não havendo duplicidade de ações, ou seja, atuações desnecessárias, e seguindo o que foi previsto no trabalho.

Durante as simulações, o algoritmo desenvolvido, dentro da estrutura proposta, se mostrou muito satisfatório. Este impediu que houvesse interferência entre as SIF’s, bem como entre os iniciadores e elementos finais, comprovando o ganho em confiabilidade do modelo. Além disso, a estrutura desenvolvida permitiu uma análise mais profunda dos acontecimentos e da funcionalidade de cada SIF, o que não era favorecido pelo modelo diretamente desenvolvido em FBD ou LD, por exemplo.

Para uma simulação de eventos aleatórios, foi adaptado o modelo para que as situações a serem verificadas, relacionadas aos estados dos sensores, ocorressem ao acaso, ou seja, ora fosse um ou outro sensor indicando falha, ou ambos, ou nenhum, indicando a normalidade do sistema. Para esta situação de normalidade foi dada maior freqüência, já que espera-se que as SIF’s tenham que atuar em casos isolados, poucas vezes, já que os eventos perigosos que representam ocorrem com baixa freqüência. Abaixo, na Figura 28 é possível verificar a estrutura projetada para os testes aleatórios.

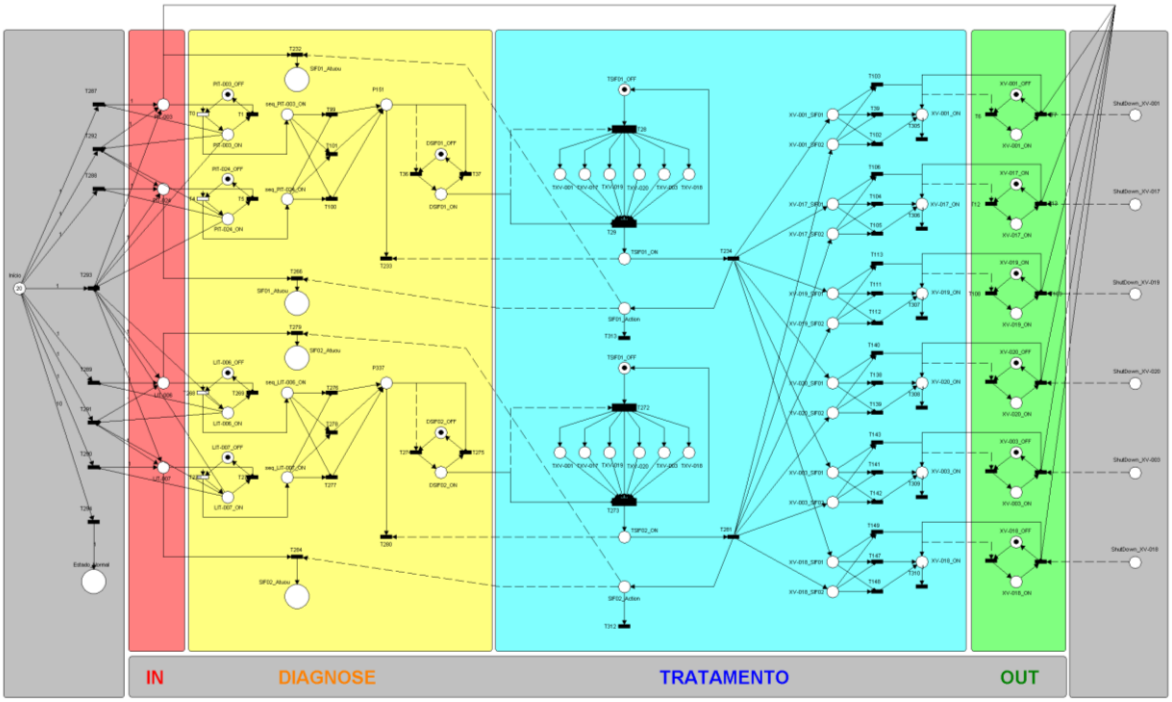


Figura 28 – Visão geral do modelo para testes aleatórios.

Através da figura anterior, pode-se verificar à esquerda uma “camada” anterior às entradas físicas. Esta região engloba os componentes dos testes aleatórios. Existe um lugar inicial, com capacidade e número inicial de marcas igual a 20. Daí projeta-se uma lógica “OU” que faz com que estas marcas sejam direcionados ora para uma, ora para outra transição dentre as que se seguem, conectadas por arcos. Estas transições são modeladas de forma a gerar diferentes combinações possíveis para as situações de falha, ou ainda para se manter em estado normal, indicado pelo lugar posicionado na parte inferior da região.

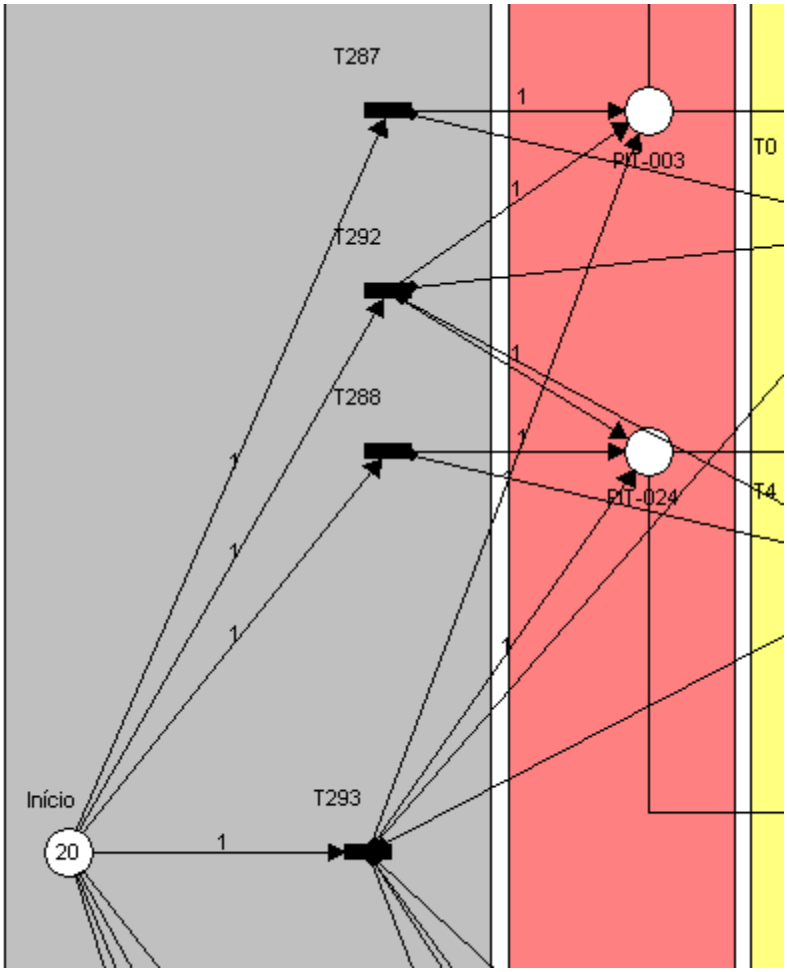


Figura 29 - Parte superior da estrutura da simulação aleatória.

Já na região ao final (direita), foram inseridos os *shutdown*'s dos atuadores, que podem ser feitos por um operador, apesar de esta situação já ser atingida automaticamente, quando os sensores são "desligados". Este *shutdown* só pode ser acionado uma vez que os sensores estejam em nível baixo (zero) e pode ser inserido como uma lógica adicional, caso este desligamento seja acionado de forma manual, por um supervisor do sistema, não somente pelos sensores em nível normal. No caso em questão, apresenta-se apenas a dependência com relação ao sensor PIT-003, para não poluir a imagem. Apesar disto, para a dependência dos outros iniciadores, o desenvolvimento é análogo.

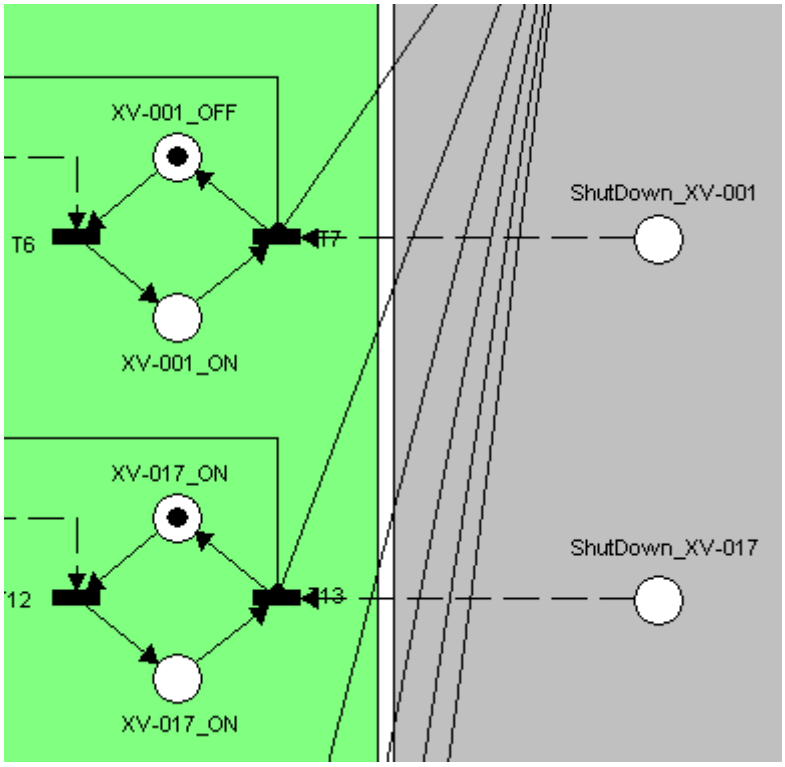


Figura 30 - Exemplo de *shutdown* dos atuadores.

Durante a simulação, ficou comprovada a eficiência trazida pela Rede de Petri para a análise dos modelos, especialmente no que tange à alcançabilidade dos estados, o que é essencial para a validação. Em se havendo um sistema de alta complexidade modelado, é possível adotar uma estrutura baseada em blocos funcionais para estruturar a programação, de forma a facilitar a compreensão, o desenvolvimento e a análise dos mesmos, além de possibilitar a localização de eventuais erros de sintaxe ou de lógica na codificação. Se isto fosse feito em outro tipo de linguagem, como o Ladder, certamente haveria problemas na análise da transição de estados e da situação em que se encontra programa a cada passo de processamento, uma vez que o modelo seria combinatório e não sequencial. Desta forma, mais uma vez podemos comprovar o ganho em se utilizar as Redes de Petri para tal desenvolvimento.

5.4.4 Transcrição de RdP para LD

O CoDeSys foi o software utilizado para a programação e algoritmos das SIF's do Estudo de Caso, em LD. Este é um software que permite a programação das lógicas de controle de acordo com a norma IEC-61131, em quaisquer das cinco linguagens citadas na mesma. Esta ferramenta é disponibilizada gratuitamente pela 3S-Smart Software Solution.

A seguir, nas Figuras 31 a 36 há uma representação da transcrição da parte de **Diagnose** do exemplo citado anteriormente, de acordo com a Figura 27. Todas as variáveis declaradas encontram-se anexadas ao final deste relatório.

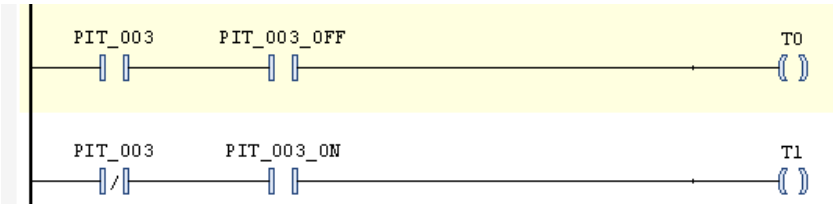


Figura 31 - Transições T0 e T1 em LD.

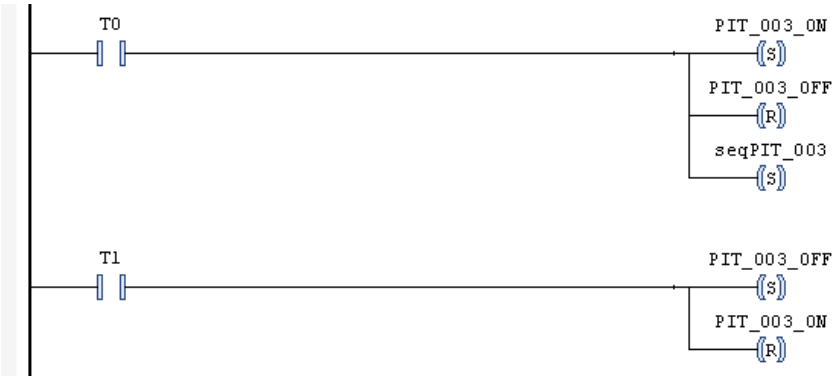


Figura 32 - Identificação dos sinais dos sensores em LD.

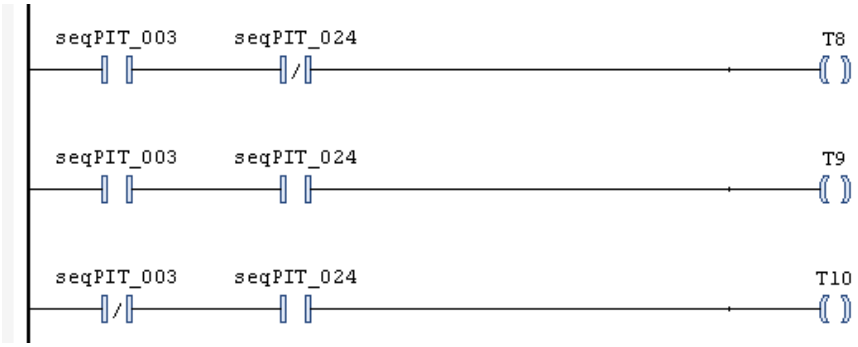


Figura 33 - Transições T8, T9 e T10 em LD.

Figura 34 - Sequenciamento dos sensores para a diagnose em LD.

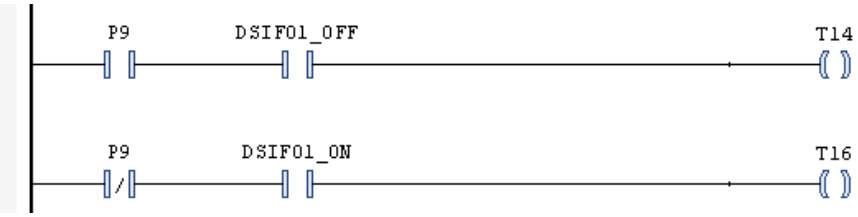


Figura 35 - Transições T14 e T16 em LD.

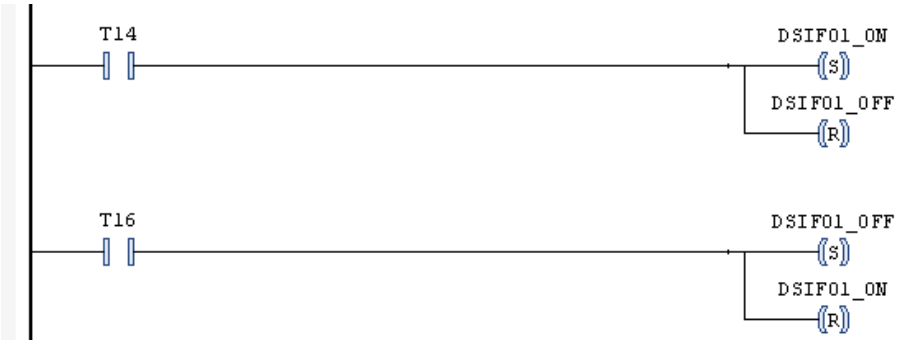


Figura 36 - Diagnose da SIF01 em LD.

6. ANÁLISE DOS RESULTADOS

Os modelos gerados podem ser analisados, primeiramente, por meio da verificação dos mesmos, que checa se determinada condições e/ou parâmetros e requisitos estabelecidos para o projeto foram atendidos durante seu desenvolvimento, para que se conclua um processo de validação efetiva, que comprove a funcionalidade e eficácia dos modelos gerados, através de análise por simulação.

6.1 VERIFICAÇÃO

Através dos modelos, foi possível fazer a verificação das estruturas geradas, analisando todas as exigências pré-estabelecidas para o desenvolvimento de um algoritmo para um SIS, bem como dos requisitos resultantes da proposta deste trabalho. Dentre as verificações, podemos citar:

- Existência de todos os iniciadores e elementos finais em todas as SIF's programadas;
- Separação das camadas de entrada e saída, para com a lógica de controle;
- Divisão da lógica de controle em Diagnose e Tratamento;
- Eliminação de possíveis interferências entre SIF's que utilizam mesmos sensores e/ou atuadores;

Desta forma, pode-se dizer que, ao final do trabalho, os pré-requisitos propostos foram obedecidos e que a metodologia sugerida é compatível com o contexto inserido.

6.2 VALIDAÇÃO

Com a realização de simulações, como citado anteriormente, foi possível analisar os estados alcançáveis pelo modelo, bem como a efetividade e confiabilidade do mesmo, que apresentou estrutura favorável a uma programação segura, ou seja, com menor possibilidade de falhas geradas pela interferência entre

os componentes, bem como por facilitar a análise e a manutenção do código, já que se mostra visual.

Além disso, a transcrição dos algoritmos em Rede de Petri para Ladder se mostrou compatível com o esperado, já que apresentou isomorfismo em relação ao modelo original. Esta fidelidade foi constatada através da comparação entre os resultados das simulações, passo a passo, apresentando correlação entre as condições e estados gerados.

Desta forma, através dos resultados das simulações desenvolvidas para cada modelo, foi possível uma análise dos mesmos, de forma a determinar sua validação. Como foi comprovada a funcionalidade da proposta e os resultados tiveram um comportamento compatível com o que se esperava dos modelos, o trabalho pode ser efetivamente validado, garantindo a contribuição positiva do projeto.

7. OBSERVAÇÕES FINAIS

O desenvolvimento deste trabalho permitiu aos alunos uma melhor compreensão de como sistemas de controle são implementados e a importância da preocupação com a segurança quando se trata de processos que envolvem riscos ao homem, às plantas industriais e ao meio ambiente. O tema tratado possibilitou aos alunos o aprendizado e a experiência sobre um aspecto não abordado durante a graduação, alheio ao que se tinha conhecimento até então. Isto trouxe a complementação da formação dos autores, com um tema de extrema importância em qualquer atuação na indústria, que é a segurança, sendo portanto, muito positivo o resultado ao final do trabalho.

O sucesso no desenvolvimento de sistemas de controle de segurança, como o SIS, depende de uma série de fatores. Uma metodologia adequada para se realizar o projeto juntamente com uma gestão de segurança eficiente diminui as chances de um evento perigoso ocorrer. Desta forma, normas como a IEC 61508 apresentam metodologias para guiar os profissionais que lidam com processos perigosos para tomarem as devidas providências.

Partindo-se destes dados, o trabalho obteve foco no estudo dos processos envolvidos numa estação de compressão de gás e na análise de risco do mesmo. Um aspecto importante foi o contato com todo o processo de análise de risco realizado por uma equipe especializada em diversas áreas da planta em questão, de acordo com a metodologia HAZOP. Com isso, os alunos tiveram a possibilidade de analisar todas as funções de segurança e a importância de cada consideração foi estudada em detalhes para compreender o trabalho desenvolvido, de acordo com a metodologia HAZOP. Este trabalho possibilitou ao grupo ter uma boa visão de como este processo se dá de fato na indústria, e construir conhecimentos novos sobre o assunto.

Normas como a IEC 61508 também estabelecem diretrizes para a elaboração das legislações, que são cada vez mais rígidas com relação à integridade do trabalhador e ao meio ambiente. As empresas já conscientes da sua responsabilidade adquirem certificados como a ISO 14001 e a OHSA 18001 que revelam a preocupação com o meio ambiente e com a integridade dos trabalhadores.

Por meio da modelagem em RdP, incluindo as camadas de Diagnose e Tratamento, permite-se uma análise global e de maior confiabilidade dos processos, através dos algoritmos, tratando individualmente cada um dos iniciadores e dos atuadores das SIF`s, possibilitando ainda a prevenção de falhas e interferências entre os componentes do processo, intrínsecos à programação, além da fácil migração para as linguagens usuais dos CLP`s, como o LD, por exemplo. Além disso, o simples desenvolvimento dos algoritmos propostos baseados nas camadas introduzidas de Diagnose e Tratamento, por si só já geram uma maior confiabilidade dos modelos, de forma que reduzem a possibilidade de falhas nos mesmos e, consequentemente, na atuação das SIF’s.

Através do Estudo de Caso da Estação de Compressão de Gás foi verificada a lógica de controle proposta, bem como a transcrição entre as linguagens citadas. Fazendo uso de simulações utilizando os softwares HPSim e CoDeSys, foi possível ainda a verificação dos estados alcançáveis e do funcionamento do modelo, de

acordo com o esperado, bem como a validação do trabalho proposto, por sua funcionalidade.

Desta forma, a abordagem utilizando Rede de Petri para o desenvolvimento dos algoritmos de controle se mostra bastante eficiente e abre uma gama de possibilidades de melhorias do que hoje se tem como prática comum para a programação de CLP's de segurança.

Além disso, uma outra abordagem possível pode ser feita através da utilização de Redes Bayesianas, considerando a disponibilidade de histórico de falhas para a dedução de uma lógica de diagnose para compor as SIF's.

Em síntese, ao final deste trabalho, os resultados gerais obtidos foram:

- Embasamento teórico sobre os conceitos relacionados a SIS;
- Estudo de Caso de uma Estação de Compressão de Gás;
- Desenvolvimento de algoritmos de controle das SIF's da Estação de Compressão de Gás, em Rede de Petri, incluindo camadas de Diagnose e de Tratamento separadamente na lógica de controle;
- Análise dos modelos gerados, em RdP, através de simulações;
- Maior confiabilidade, possibilidade de análises formais de estrutura do SIS e de seus estados alcançáveis com a RdP;
- Controle do SIS, através da programação das SIF's, a partir da migração dos modelos em RdP, para Ladder (linguagem da IEC 61131-3), indicados ao uso de CLP's SIS de segurança;
- Verificação e Validação dos modelos gerados.

8. REFERÊNCIAS BIBLIOGRÁFICAS

AGUIAR, L. A. **Metodologias de Análise de Riscos APP & HAZOP,** Rio de Janeiro, RJ.

CRUZ-CAMPA, H. J. & CRUZ-GÓMEZ, M. J. **Determine SIS and SIL Using HAZOPS**, AIChE, Cidade do México, México, 2009.

FRANCÊS, C. R. L. **Introdução às Redes de Petri**, UFPA, Pará, 2003

GOBLE, W.M. **Control Systems Safety Evaluation & Reliability**, ISA, 1998.

IEC 61508, **Functional safety of electrical / electronic / programmable electronic safety-related systems**, International Electrotechnical Commision, Geneva, Switzerland, 1998.

IEC 61511, **Functional safety - Safety Instrumented Systems for the process industry sector**, International Electrotechnical Commision, Geneva, Switzerland, 2003.

LUNDTEIGEN, M. A. & RAUSAND, M. **Architectural constraints in IEC 61508: Do they have the intended effect?,** Reliability Engineering and System Safety, pages 520 – 525, Elsevier Science Publisher Ltd., 2009.

MOURELLE, L. **Controle de Processos por Computador.** UERJ.

ANEXO – LISTA DE VARIÁVEIS DA PROGRAMAÇÃO EM LD

```
PROGRAM PLC_PRG
VAR
	//SIF 01
	//Transições
	T0, T1, T2, T3: BOOL;
	T8, T9, T10: BOOL;
	T14, T16: BOOL;
	T20, T21: BOOL;
	T24, T18, T26: BOOL;
	T64, T65: BOOL;
	//Sensores
	PIT_003, PIT_003_OFF, PIT_003_ON: BOOL;
	PIT_024, PIT_024_OFF, PIT_024_ON: BOOL;
	//Intermediários
	seqPIT_003, seqPIT_024: BOOL;
	P9: BOOL;
	SIF01_Atuou: BOOL;//DELETAR
	SIF01_Action: BOOL;
	//Diagnose
	DSIF01_OFF, DSIF01_ON: BOOL;
	//Tratamento
	TSIF01_OFF, TSIF01_ON: BOOL;
	TXV001, TXV017, TXV019, TXV020, TXV003, TXV018: BOOL;
	TByPass, TCompSlow: BOOL; //SIF01

	//SIF 02
	//Transições
	T4, T5, T6, T7: BOOL;
	T11, T12, T13: BOOL;
```

```
        T15, T17: BOOL;
        T22, T23: BOOL;
        T25, T19, T27: BOOL;
        T66, T67: BOOL;
        //Sensores
        LIT_006, LIT_006_OFF, LIT_006_ON: BOOL;
        LIT_007, LIT_007_OFF, LIT_007_ON: BOOL;
        //Intermediários
        seqLIT_006, seqLIT_007: BOOL;
        P10: BOOL;
        SIF02_Atuou: BOOL;//DELETAR
        SIF02_Action: BOOL;
        //Diagnose
        DSIF02_OFF, DSIF02_ON: BOOL;
        //Tratamento
        TSIF02_OFF, TSIF02_ON: BOOL;
        //TXV001, TXV017, TXV019, TXV020, TXV003, TXV018: BOOL;
        TXV005, TXV022, TCompShutDown: BOOL; //SIF02

        //Atuadores
        XV001_SIF01, XV001_SIF02, XV001_S, XV001_OFF, XV001_ON: BOOL;
        XV017_SIF01, XV017_SIF02, XV017_S, XV017_OFF, XV017_ON: BOOL;
        XV019_SIF01, XV019_SIF02, XV019_S, XV019_OFF, XV019_ON: BOOL;
        XV020_SIF01, XV020_SIF02, XV020_S, XV020_OFF, XV020_ON: BOOL;
        XV003_SIF01, XV003_SIF02, XV003_S, XV003_OFF, XV003_ON: BOOL;
        XV018_SIF01, XV018_SIF02, XV018_S, XV018_OFF, XV018_ON: BOOL;
        ByPass_SIF01, ByPass_S, ByPass_OFF, ByPass_ON: BOOL; //SIF01
        CompSlow_SIF01, CompSlow_S, CompSlow_OFF, CompSlow_ON: BOOL;
//SIF01
        XV005_SIF02, XV005_S, XV005_OFF, XV005_ON: BOOL; //SIF02
        XV022_SIF02, XV022_S, XV022_OFF, XV022_ON: BOOL; //SIF02
```

```
        CompShutDown_SIF02, CompShutDown_S, CompShutDown_OFF,
CompShutDown_ON: BOOL; //SIF02

        //Transições Comunsàs SIF`s
        T28, T29, T30, T31, T32, T33, T34, T35, T36: BOOL;
        T37, T38, T39, T40, T41, T42, T43, T44, T45: BOOL;
        T46, T47, T48, T49, T50, T51: BOOL;
        T52, T53, T54, T55, T56, T57, T58, T59, T60, T61, T62, T63: BOOL;
        T68, T69, T70, T71, T72, T73, T74, T75, T76, T77: BOOL; //ATUADORES
OUT
        T78, T79, T80, T81, T82, T83, T84, T85, T86, T87: BOOL;
//ATUADORES_SIF
END_VAR
```