JEFERSON AFONSO LOPES DE SOUZA

# MITIGAÇÃO DE FALHAS CRÍTICAS EM SISTEMAS PRODUTIVOS

SÃO PAULO

2015

**JEFERSON AFONSO LOPES DE SOUZA**

# MITIGAÇÃO DE FALHAS CRÍTICAS EM SISTEMAS PRODUTIVOS

Dissertação apresentada à Escola Politécnica da Universidade de São Paulo para obtenção do título de Mestre em Ciências.

Programa: Engenharia Mecânica.

Área de Concentração: Engenharia de Controle e Automação Mecânica.

Orientador: Prof. Dr. Diolino José dos Santos Filho.

**SÃO PAULO**

**2015**

Este exemplar foi revisado e corrigido em relação à versão original, sob responsabilidade única do autor e com a anuência de seu orientador.

São Paulo, _____ de _____ de _____

Assinatura do autor: _____

Assinatura do orientador: _____

Catalogação-na-publicação

Jeferson Afonso Lopes, Souza
Mitigação de Falhas Críticas em Sistemas Produtivos / S. Jeferson Afonso Lopes -- versão corr. -- São Paulo, 2015.
144 p.

Dissertação (Mestrado) - Escola Politécnica da Universidade de São Paulo. Departamento de Engenharia Mecatrônica e de Sistemas Mecânicos.

1.Sistemas Produtivos 2.Falhas Críticas (Mitigação) I.Universidade de São Paulo. Escola Politécnica. Departamento de Engenharia Mecatrônica e de Sistemas Mecânicos II.t.

*À Carina, pela paciência...*

# AGRADECIMENTOS

Este trabalho não é, de forma alguma, o resultado do trabalho isolado de um pesquisador ao longo de três anos, mas sim a soma das contribuições de diversas pessoas que, de diferentes formas e amplitudes, me inspiraram, me motivaram e me deram forças para que este trabalho fosse edificado a cada dia de pesquisa.

Desta forma, não poderia deixar de agradecer aos meus pais Daltro e Adelfina, a meus irmãos Denise, Fábio e Rafael, além de meus sobrinhos, e sobretudo a meus avós, que sempre pediram por minha proteção ao meu Anjo da Guarda...

Agradeço também à minha companheira Carina, que sempre ficou ao meu lado, mesmo nas situações difíceis, e que sempre me incentivou a seguir com o trabalho como forma de contornar tais situações.

De forma particular, agradeço ao meu orientador, Prof. Dr. Diolino José dos Santos Filho, por me fazer entender a postura e o método de trabalho que um (bom) pesquisador deve ter quando se depara com um problema. Talvez este foi o maior aprendizado que tive neste período, cujo resultado é representado neste trabalho.

Agradeço também ao Prof. Dr. Paulo Eigi Miyagi pela onipresente atenção e ajuda, ao grupo de pesquisas do PMR-LSA, em especial aos alunos doutorandos Marcosiris Pessoa, Caio Fattori, Osvaldo Asato, Edinei Legaspe, ao MSc Eng. Rodrigo Ferrarezzi, e em particular ao MSc Eng. Reinaldo Squillante Jr, por sua disposição em ajudar às pessoas sempre de forma calorosa, e ao Dr Eng. Andre Cesar Cavalheiro por me incentivar e a me ajudar no início de minha profissão como Docente.

# RESUMO

O cenário competitivo e globalizado em que as empresas estão inseridas, sobretudo a partir do século XXI, associados a ciclos de vida cada vez menores dos produtos, rigorosos requisitos de qualidade, além de políticas de preservação do meio ambiente, com redução de consumo energético e de recursos hídricos, somadas às exigências legais de melhores condições de trabalho, resultaram em uma quebra de paradigma nos processos produtivos até então concebidos. Como solução a este novo cenário produtivo pode-se citar o extenso uso da automação industrial, fato que resultou em sistemas cada vez mais complexos, tanto do ponto de vista estrutural, em função do elevado número de componentes, quanto da complexidade dos sistemas de controle. A previsibilidade de todos os estados possíveis do sistema torna-se praticamente impossível. Dentre os estados possíveis pode-se citar os estados de falha que, dependendo da severidade do efeito associado à sua ocorrência, podem resultar em sérios danos para o homem, o meio ambiente e às próprias instalações, caso não sejam corretamente diagnosticados e tratados. Fatos recentes de catástrofes relacionadas à sistemas produtivos revelam a necessidade de se implementar medidas para prevenir e para mitigar os efeitos da ocorrência de falhas, com o objetivo de se evitar a ocorrência de catástrofes. De acordo com especialistas, os Sistemas Instrumentados de Segurança – SIS, referenciados em normas como a IEC 61508 e IEC 61511, são uma solução para este tipo de problema. Trabalhos publicados tratam de métodos para a implementação de camadas SIS de prevenção, porém com escassez de trabalhos para camadas SIS de mitigação. Em função do desconhecimento da dinâmica do sistema em estado de falha, técnicas tradicionais de modelagem tornam-se inviáveis. Neste caso, o uso de inteligência artificial, como por exemplo a lógica fuzzy, pode se tornar uma solução para o desenvolvimento do algoritmo de controle, associadas a ferramentas de edição, modelagem e geração dos códigos de controle. A proposta deste trabalho é apresentar uma sistemática para a implementação de um sistema de controle para a mitigação de falhas críticas em sistemas produtivos, com referência às normas IEC 61508/61511, com ação antecipativa à ocorrência de catástrofes.

**Palavras-chave**: sistemas produtivos, falhas críticas, sistema instrumentado de segurança, mitigação, lógica fuzzy, ação antecipativa, catástrofes.

# ABSTRACT

The competitive and globalized scenario in which the companies operate, especially from the twenty-first century, associated with shrinking life cycles of products, stringent quality requirements, and environmental preservation policies, reducing energy consumption and water resources, in addition of legal requirements for better working conditions, resulted in a paradigm shift in production processes previously designed. As a solution to this new production scenario may be mentioned the extensive use of industrial automation, which has resulted in ever more complex systems, both from a structural point of view, due to the high number of components, the complexity of control systems. The predictability of all possible states of the system becomes practically impossible. Among the possible states can mention the states of fault, depending on the severity of the effect associated with its occurrence, can result in serious damage to man, the environment and own facilities, if not properly diagnosed and treated. Recent events for disasters related to production systems show the need to implement measures to prevent and mitigate the effects of the occurrence of faults in order to prevent the occurrence of disasters. According to experts, the Safety Instrumented Systems - SIS, referenced in standards such as IEC 61508 and IEC 61511, are a solution to this problem. Published papers deal with methods for the implementation of SIS layers of prevention, but with shortage of jobs for mitigation SIS layers. Depending on the system dynamics of ignorance in a fault state, traditional modeling techniques become unviable. In this case, the use of artificial intelligence, such as fuzzy logic can become a solution to the development of the control algorithm, associated with editing tools, modeling and generation of control codes. The purpose of this paper is to present a systematic for implementing a control system for the mitigation of critical failures in production systems, with reference to IEC 61508/61511 standards, with preemptive action to the occurrence of disasters.



**Keywords**: production systems, critical faults, safety instrumented system, mitigation, fuzzy logic, preemptive action, disasters.

# LISTA DE FIGURAS

Figura 1.1 - Exemplos de automação industrial no cenário produtivo atual. .....2

Figura 1.2 - Exemplos de sistemas produtivos com uso intrínseco de automação. ....3

Figura 1.3 - Exemplo de instalação industrial moderna.....3

Figura 1.4 - Exemplos de acidentes em sistemas produtivos com sérias consequências ao homem, ao meio ambiente e aos equipamentos. .....5

Figura 1.5 – Arquitetura de controle de um Sistema Instrumentado de Segurança. Fonte: Squillante (2011). .....6

Figura 1.6 - Camadas de redução de riscos (adaptado da norma IEC 61511-1). .....7

Figura 2.1 - IEC 61508 como referência à SIS em SP. Extraído de (Bojorge, 2012) 12

Figura 2.2 - Ciclo de vida de segurança (Adaptado da IEC 61511). .....13

Figura 2.3 - Normas derivadas da IEC 61508 (Adaptado da (IEC, 2010)). .....13

Figura 2.4 - Aspectos associados à redução de risco em SIS .....17

Figura 2.5 - Disposição das camadas SIS em um SP. Extraído de Bojorge (2012) ..19

Figura 2.6 - Exemplo de aplicação da FTA Extraído de Takayama (2008). .....27

Figura 2.7 - Representação de uma árvore de eventos. Extraído de Takayama (2008).....28

Figura 2.8 - Comportamento de SVC x SED. . .....31

Figura 2.9 - Estrutura básica de um sistema de controle de SED (MIYAGI, 1996) (VILLANI, 2000).....31

Figura 2.10 - Representação em RdP de duas atividades em sequência. .....32

Figura 2.11 - Representação do paralelismo em RdP de duas atividades. .....33

Figura 2.12 - Representação em RdP da sincronização de duas atividades. .....34

Figura 2.13 - Representação em RdP de conflito entre duas atividades. .....35

Figura 2.14 - Representação clássica de dois conjuntos. .....35

Figura 2.15 – Representação de um conjunto nebuloso ou fuzzy. .....36

Figura 2.16 - Exemplos de função de pertinência. .....37

Figura 2.17 - Operador mínimo ou conector “AND” lógico. .....37

Figura 2.18 - Operador máximo ou conector “OR” lógico. .....37

Figura 2.19 - Operador negação ou conector “NOT” lógico .....38

Figura 2.20 – Áreas de Inteligência Computacional (ANDRADE, 2002). .....39
Figura 2.22 - Função de pertinência para altura.....39
Figura 2.22 - Inferência Mandani. Adaptado de (SIMÕES; SHAW, 2007). .....41
Figura 2.23 - Exemplo da saída com centro de gravidade (IEC, 2000).....43
Figura 2.24 - Exemplo de código FCL (IEC, 2000).....45
Figura 3.1 - Arquitetura SIS para implemetação da sistemática proposta.....46
Figura 3.2 - Dispositivo de realização de controle fuzzy (IEC, 2000). .....47
Figura 3.3 - Função de pertinência da variável “erro” (POPA, 2008). .....48
Figura 3.4 - Controlador fuzzy básico (Adaptado da (IEC, 2000).....49
Figura 3.5 – Relação da técnica *What-If* com a base de regras fuzzy. .....49
Figura 3.6 – Ciclo de vida do projeto e desenvolvimento da sistemática proposta. Adaptado de Miyagi (1996) .....50
Figura 3.7 – Lógica 2oo3 para sensores. Fonte: Ferrarezi (2014) .....53
Figura 3.8 – Toolbox fuzzy MatLab®.....58
Figura 3.9 – Exemplo de regiões de operação para uma variável de entrada. .....59
Figura 3.10 – Regiões de operação para a evolução temporal da variável.....59
Figura 3.11 – Conjunto de regras fuzzy, extraídas do conhecimento humano.....60
Figura 3.12 – Modelo do atuador no *toolbox.* .....61
Figura 4.1 – Vista da Estação de Compressão de Gás. Fonte: http://www.bonatti.it/Projects/Mellitah-Gas-Compression-Station. Acesso: 23/11/2014 .....63
Figura 4.2 – P&ID de uma das unidades compressoras. .....65
Figura 4.3 - FTA para “Alta temperatura do óleo lubrificante do mancal de eixo”. ....66
Figura 4.4 - P&ID cilindros de dióxido de carbono na *Ecomp*. .....68
Figura 4.5 – Modelo em RdP da SIF 1. .....71
Figura 4.6 – Ações de mitigação para a SIF 1. .....72
Figura 4.7 – Modelo em RdP para identificação do estado seguro dos sensores.....73
Figura 4.8 - Funções de pertinência fuzzy para a temperatura. .....74
Figura 4.9 - Funções de pertinência para a derivada da temperatura.....75
Figura 4.10 – Função de pertinência para a variável de saída.....76

Figura 4.11 – Módulo de inferência fuzzy no *toolbox* do MatLab®.....77
Figura 4.12 – Regras Fuzzy no *toolbox.*.....77
Figura 4.13 - Superfície gerada pelo algoritmo fuzzy. .....78
Figura 4.14 – Sinais de entrada para o controlador fuzzy. .....79
Figura 4.15 – Programa de controle implementado em FCL (IEC, 2000). .....80
Figura 4.16 – Modelo em RdP para a detecção e tratamento da SIF 1. .....92
Figura 4.17 – Modelo em RdP para as ações de mitigação associadas à SIF 1.....93
Figura 4.18 - Modelo em RdP para a detecção e tratamento da SIF 2. .....94
Figura 4.19 – Modelo em RdP para as ações de mitigação associadas à SIF 2.....95
Figura 4.20 - Modelo em RdP para a detecção e tratamento da SIF 3. .....96
Figura 4.21 - Modelo em RdP para as ações de mitigação associadas à SIF 3. .....97
Figura 4.22 - Modelo em RdP para a detecção e tratamento da SIF 4. .....98
Figura 4.23 – Atividades de mitigação para a SIF 4.....99
Figura 4.24 – Controlador para a SIF 1 de mitigação.....100
Figura 4.25 – Bases de Regras para a SIF 1 Mitigação.....101

Figura A 1 - Representação gráfica dos elementos da RdP .....114
Figura A 2 - Exemplo de RdP como modelo de processo.....115
Figura A 3 - Complemento de arco orientado inibidor. .....117
Figura A 4 - Representação gráfica da transição temporizada na RdP.....118
Figura A 5 - Exemplo de RdP para verificação da alcançabilidade. .....120
Figura A 6 - Exemplo de RdP para verificação de limitabilidade e segurança. .....120
Figura A 7 - Exemplo de RdP para verificação da propriedade de vivacidade.....122
Figura A 8 - Exemplo de RdP para a verificação da propriedade de persistência...123
Figura A 9 - Exemplo de RdP para a verificação da propriedade de equidade.....124

Figura B 1 – Modelo em RdP para detecção e tratamento da SIF Gás1. .....136
Figura B 2 - Modelo em RdP para detecção e tratamento da SIF Gás 2. .....137
Figura B 3 - Modelo em RdP para detecção e tratamento da SIF Gás 3. .....138
Figura B 4 - Modelo em RdP para detecção e tratamento da SIF Gás 4. .....139
Figura B 5 - Modelo em RdP para detecção e tratamento da SIF Fogo.....140
Figura B 6 – Controlador fuzzy para a SIF Gás 1.....141
Figura B 7 – Bases de regras para a SIF Gás 1.....142

# LISTA DE TABELAS

Tabela 2.1 - Níveis de integridade de segurança (SIL) – (IEC, 2010) ..... 15

Tabela 2.2 – Exemplo de tabela FMEA – adaptado de Helman (1995). ..... 25

Tabela 2.3 - Elementos estruturais de uma FTA. Adaptado de Helman e Andrey (1995) ..... 26

Tabela 2.4 – Exemplo de documentação de HAZOP–IEC 61882, (IEC, 2001)..... 29

Tabela 2.5 – *Fuzzificação* da variável altura ..... 40

Tabela 3.1 – Exemplo de matriz causa-efeito. ..... 54

Tabela 4.1 - FMEA- falha de lubrificação do eixo do mancal do compressor..... 65

Tabela 4.2 – Matriz causa-efeito ..... 69

Tabela 4.3 – SIF 1 – derivada da matriz causa-efeito na Tabela 4.2 ..... 70

Tabela 4.4 - Regras fuzzy para a camada de mitigação. ..... 75

Tabela 4.5 – Fuzzy Set ..... 76

Tabela 4.6 – Efeitos da ocorrência de falhas e correspondentes TAGs..... 81

Tabela 4.7 – Ações de mitigação propostas e TAGs dos atuadores. ..... 83

Tabela 4.8 – SIF 1 Mitigação..... 86

Tabela 4.9 – SIF 2 Mititgação..... 87

Tabela 4.10 – SIF 3 Mitigação..... 88

Tabela 4.11 – SIF 4 Mitigação..... 89

Tabela B 1 - Efeitos da ocorrência de falhas e correspondentes TAGs ..... 127

Tabela B 2 – Ações de Mitigação para a camada gás e fogo. ..... 128

Tabela B 3 – SIF 1 Gás ..... 131

Tabela B 4 – SIF 2 Gás ..... 132

Tabela B 5 – SIF 3 Gás ..... 133

Tabela B 6 – SIF 4 Gás ..... 134

Tabela B 7 – SIF 5 FOGO ..... 135

# LISTA DE EQUAÇÕES

Equação 1-1 - Estados totais alcançáveis dos componentes de um sistema. .....4

Equação 2-1 – Relação de risco inerente e risco aceitável. .....15

Equação 2-2 – Fator de redução de risco. .....15

Equação 2-3 – Funções de pertinência para a função altura. .....40

Equação 2-4 – Cálculo do centro de gravidade.....43

Equação 4-1 – Relação lógica dos sensores para a SIF1 – caso de uso 1. .....79

# LISTA DE ABREVIATURAS, ACRÔNIMOS E SIGLAS

| | |
|---|---|
| AAE | Análise de Árvore de Eventos |
| ANSI | *American National Standards Institute* |
| BPCS | Sistema de Controle Básico de Processo |
| C/E | Condição / evento |
| CP | Controlador Programável |
| ECOMP | Estação de Compressão de Gás |
| FMEA | *Failure Modes and Effect Analysis* |
| FMECA | *Failure Modes and Effects Consequences Analysis* |
| FRR | Fator de redução de risco |
| FTA | *Fault Tree Analysis* |
| HAZOP | *Hazard and Operability* |
| IEC | *International Electrotechnical Commission* |
| ISA | *The instrumentation, Systems and Automation Society* |
| ISO | *International Organization for Standardization* |
| LD | *Ladder Diagram* |
| PFD | Probabilidade de Falha em demanda |
| PHA | *Preliminar Hazard Analysis* |
| PN | *Petri net* |
| P&ID | *Process Identification* |
| RdP | Rede de Petri |
| SED | Sistemas a Eventos Discretos |
| SIF | *Safety Instrumented Function* |
| SIL | *Safety Integrated Level* |
| SIS | Sistemas Instrumentados de Segurança |
| SP | Sistemas Produtivos |
| SVC | Sistemas a variáveis contínuas |
| TIC | Técnica de Incidentes Críticos |
| WI | *What-If* |

# LISTA DE SÍMBOLOS

| | |
|---|---|
| *P* | conjunto finito de lugares |
| *T* | conjunto finito de transições |
| *Tn* | conjunto finito de transições normais da RdP |
| *Tor* | conjunto finito de transições “OU inclusivo” da RdP |
| *F* | conjunto finito de arcos orientados |
| *W* | conjunto de pesos dos arcos orientados |
| $M_0$ | conjunto de marcas iniciais nos lugares |
| *M* | conjunto de marcas nos lugares |
| *N* | estrutura da rede de Petri |
| *(N, M)* | rede de Petri com uma certa distribuição de marcas nos lugares |
| *R(N, M)* | conjunto de marcas alcançáveis em uma estrutura de rede de Petri N a partir da marcação M |

# SUMÁRIO

**1. INTRODUÇÃO ..... 1**

**1.1 Motivação ..... 7**

**1.2 Justificativa ..... 9**

**1.3 Objetivo ..... 9**

**1.4 Estrutura do trabalho ..... 10**

**2. REVISÃO BIBLIOGRÁFICA ..... 11**

**2.1 Sistemas Instrumentados de Segurança ..... 11**

2.1.1 Normas relacionadas a SIS ..... 11

2.1.2 Nível de Integridade de Segurança (SIL) ..... 14

2.1.3 Camadas individuais de proteção de riscos ..... 16

**2.2 TÉCNICAS DE ANÁLISE DE RISCOS ..... 19**

2.2.1 Modos de Falha de Componentes ..... 20

2.2.2 Série de Riscos - SR ..... 22

2.2.3 Análise Preliminar de Riscos – PHA ..... 22

2.2.4 What-If – WI ..... 22

2.2.5 Checklist ..... 23

2.2.6 What-If / Checklist – WIC ..... 23

2.2.7 Técnica de Incidentes Críticos – TIC ..... 24

*2.2.8* Análise de Modos de Falha e seus Efeitos – FMEA ..... 24

*2.2.9* Análise de Árvore de Falhas – FTA ..... 25

2.2.10 Análise de Árvore de Eventos – AAE ..... 27

2.2.10 Estudo de Operabilidade e Riscos – Hazop ..... 28

**2.3 SISTEMAS A EVENTOS DISCRETOS – SED ..... 29**

2.3.1 Características de SEDs ..... 31
2.3.1.1 Sequência ..... 32
2.3.1.2 Paralelismo ..... 33
2.3.1.3 Sincronização ..... 33
2.3.1.4 Conflito ..... 34

**2.4 CONTROLE FUZZY ..... 35**
2.4.1 Teoria de conjuntos fuzzy e números fuzzy ..... 35
2.4.2 Operações com conjuntos fuzzy ..... 36
2.4.3 Lógica Fuzzy ..... 38
2.4.3.1 Fuzzificação ..... 40
2.4.3.2 Módulo de Inferência ..... 41
2.4.3.3 Base de Regras ..... 42
2.4.3.4 Defuzzificação ..... 43
2.4.4 IEC 61131-7 ..... 44

**3. SISTEMÁTICA PROPOSTA ..... 46**

**3.1 Determinação dos elementos críticos ..... 51**

**3.2 Detecção dos efeitos da ocorrência de falhas dos elementos críticos ..... 52**

**3.3 Ações de mitigação propostas ..... 53**

**3.4 Elaboração da matriz causa-efeito ..... 54**

**3.5 Identificação das SIFs ..... 55**

**3.6 Modelagem do algoritmo de controle ..... 55**

**3.7 Geração dos algoritmos fuzzy para as SIFs ..... 57**

**3.8 Códigos de controle com referência à IEC 61131-7 ..... 62**

**4. EXEMPLO DE APLICAÇÃO ..... 63**

**4.1 Aplicação da Sistemática Proposta – Caso de Uso 1 ..... 64**

4.1.1 Determinação dos Elementos Críticos ..... 64

4.1.2 Detecção dos efeitos da ocorrência de falhas dos elementos críticos ..... 67

4.1.3 Ações de Mitigação propostas ..... 67

4.1.4 Elaboração da matriz causa-efeito ..... 68

4.1.5 Identificação das SIFs ..... 69

4.1.6 Modelagem do algoritmo de controle ..... 71

4.1.7 Geração dos algoritmos fuzzy para as SIFs ..... 73

4.1.8 Códigos de controle com referência à IEC 61131-7 ..... 79

**4.2 Aplicação da Sistemática Proposta – Caso de Uso 2 ..... 80**

4.2.1 Detecção dos efeitos da ocorrência de falhas dos elementos críticos ..... 81

4.2.2 Ações de mitigação propostas ..... 82

4.2.3 Elaboração da matriz causa-efeito ..... 84

4.2.4 Identificação das SIFs ..... 85

4.2.5 Modelagem do algoritmo de controle ..... 90

4.2.6 Geração dos algoritmos fuzzy para as SIFs. ..... 100

4.2.7 Códigos de controle com referência à IEC 61131-7. ..... 101

**5. OBSERVAÇÕES FINAIS ..... 102**

**5.1 Trabalhos futuros ..... 103**

**BIBLIOGRAFIA ..... 104**

**ANEXO A - REDE DE PETRI – RdP ..... 113**

A.1 Formalização ..... 114

A.2 Extensões da RdP ..... 117

A.2.1 Arco Inibidor ..... 117

A.2.2 Temporizações ..... 118

A.3 Propriedades ..... 119
A.3.1 Alcançabilidade ..... 119
A.3.2 Limitabilidade e Segurança ..... 120
A.3.4 Vivacidade ..... 120
A.3.5 Reversibilidade ..... 122
A.3.6 Cobertura ..... 122
A.3.7 Persistência ..... 123
A.3.8 Distância Síncrona ..... 123
A.3.9 Equidade ..... 124

**ANEXO B - MATRIZ CAUSA-EFEITO CASO DE USO 2 ..... 125**

**APÊNDICE B - CAMADA SIS DE GÁS E FOGO ..... 126**
B1 Detecção dos efeitos da ocorrência de falhas dos elementos críticos ..... 126
B2 Ações de mitigação propostas ..... 127
B3 Elaboração da matriz causa-efeito ..... 129
B4 Identificação das SIFs ..... 130
B5 Modelagem do algoritmo de controle ..... 136
B6 Geração dos algoritmos fuzzy para as SIFs ..... 141
B7 Códigos de controle com referência à IEC 61131-7 ..... 143
ANEXO C – Matriz Causa-Efeito Camada SIS Gás e Fogo ..... 144

# 1. INTRODUÇÃO

No cenário globalizado e competitivo no qual as organizações estão inseridas, sobretudo a partir do final do século XX, a exigência cada vez maior dos mercados consumidores, o aspecto da sustentabilidade e a necessidade da preservação do meio ambiente são fatores que tornam obrigatórias, para a própria sobrevivência destas organizações, a adoção de planejamentos estratégicos e práticas operacionais que assegurem a capacidade para uma rápida adaptação e consequente mudança dos sistemas produtivos até então concebidos. A expectativa é de que além de resultar num processo com redução efetiva de custos, alta qualidade do produto e flexibilidade das linhas de produção, e redução dos tempos de desenvolvimento de novos produtos e de entrega (SANTOS FILHO, 2000) (CHEN e DAI, 2004) (WU, XI e ZHUO, 2008), também provoque a redução de impactos ambientais do processo de fabricação, com consequente redução da energia utilizada e na utilização de matérias-primas de fontes renováveis, além do enquadramento aos rígidos controles de emissões (emissão de gases poluentes na atmosfera e de dejetos nos leitos de rios).

A exigência legal da qualidade do ambiente de trabalho, com foco na saúde e segurança do trabalhador, fez com que atividades humanas, até então comuns para o chão de fábrica, fossem substituídas por máquinas e processos automatizados (KAMTEKAR, 2009), como, por exemplo, os braços robóticos, que podem desempenhar tarefas repetitivas em ambientes hostis. Como exemplo têm-se os processos de soldagem e pintura nas linhas de montagem automotivas ou no controle contínuo de processos industriais.

Políticas governamentais, expressas em forma de Lei, estão também restringindo cada vez mais a operação de indústrias, obrigando a instalação de novas tecnologias e equipamentos tanto para a produção quanto para o gerenciamento e monitoração destes processos.

Uma das soluções, que comprovadamente atendem às exigências deste cenário, é o extenso uso da automação industrial, cujo avanço se dá de forma paralela ao progresso das tecnologias de informática, junto com o desenvolvimento de elementos de *hardware,* tanto na velocidade de processamento e capacidade de

armazenamento, com consequente desenvolvimento de softwares cada vez mais complexos e, sobretudo, o avanço da Internet.

Os resultados obtidos neste novo cenário são Sistemas Produtivos (SPs) que executam processos altamente complexos (SAMPAIO, 2011) (FERREIRA, *et al.*, 2014) que não poderiam ser exequíveis por meio de métodos convencionais de produção (MAZZOLINI, BRUSAFERRI e CARPANZANO, 2011), sobretudo os métodos de produção em larga escala das linhas de produção características do período entre guerras até meados dos anos 70. A Figura 1.1 ilustra o cenário atual de linhas de produção de SPs alinhadas com o cenário atual.

Figura 1.1 - Exemplos de automação industrial no cenário produtivo atual.

Portanto, este trabalho está focado em SPs como sistemas que fazem uso intrínseco da automação industrial para o fornecimento de produtos, serviços e transporte, como se pode observar nos exemplos das Figuras 1.2 e 1.3.

Figura 1.2 - Exemplos de sistemas produtivos com uso intrínseco de automação.

Figura 1.3 - Exemplo de instalação industrial moderna.

Considerando a lógica de evolução dos estados destes SPs, pode-se considerá-los como uma classe de Sistemas a Eventos Discretos – SEDs, uma vez que estes sistemas evoluem dinamicamente em função da ocorrência de eventos vistos como instantâneos. Tais estados dependem do número de dispositivos independentes presentes no sistema e, o número de estados globais resulta da produtória dos estados locais dos vários dispositivos (MIYAGI, 2007), tendo-se como resultado uma explosão combinatória de estados alcançáveis do sistema, representado na Equação 1.1 (MIYAGI, 2007).

$$N_t = \prod_{i=1}^{m} N_i \qquad (1.1)$$

Na Equação 1.1, o número de estados totais $N_t$ é resultante da combinação dos estados indivuduais $N_i$ de cada componente $m$ de um sistema.

Em todo projeto de automação, que tem por meta a produção de um bem ou serviço, o algoritmo de processo baseia-se na sucessão de estados desejados para o cumprimento do objetivo proposto. O resultado dos estados alcançáveis, decorrente do elevado número de componentes presentes nos SPs, resulta em uma impossibilidade prática, ainda que na fase de projeto, associada ao determinismo da dinâmica associada à combinatória de todos os estados alcançáveis. Restringe-se, pois, o comportamento do sistema a determinadas transições de estados que se sucedem de acordo com um algoritmo pré-definido de controle da lógica que estabelece estas transições, para que o SP cumpra seu objetivo, que é a produção de um determinado bem ou serviço.

Entretanto, apesar das restrições consideradas, em determinadas situações anormais ou imprevistas, o sistema pode atingir estados indesejados, que podem colocar o sistema em risco. Tais estados comprometem o resultado do sistema produtivo, fazendo com que o objetivo proposto não seja contemplado.

Aos estados alcançáveis e indesejados, pode-se citar os estados de falha de componentes, os erros operacionais propositais (intencionais) ou não, ou ainda as falhas de projeto. Tais ocorrências podem resultar, dependendo da complexidade do SP, em sérios riscos à integridade física das pessoas, ao meio ambiente e a perdas econômicas decorrentes de danos ao próprio equipamento (SALLAK, SIMON e AUBRY, 2008).

Embora muitos trabalhos tenham sido apresentados, tanto para o diagnóstico quanto para o tratamento de uma determinada classe de falhas (MORALES, GARCIA MELO e MIYAGI, 2007) (RU e HADJICOSTS, 2008) (WANG, *et al.*, 2008), os acidentes continuam ocorrendo. Registros de catástrofes recentes podem ser observados na Figura 1.4.

Figura 1.4 - Exemplos de acidentes em sistemas produtivos com sérias consequências ao homem, ao meio ambiente e aos equipamentos.

Partindo da hipótese de que não existe risco zero em SPs, uma vez que: (i) dispositivos físicos não possuem risco de falha nulo, (ii) operadores humanos não são isentos de erros operacionais e (iii) não há projetos de programas computacionais desenvolvidos que possam prever todas as possibilidades operacionais (SQUILLANTE JR, *et al.*, 2011) (SQUILLANTE JR, 2011), a ocorrência de falhas em SPs é possível, ainda que em uma probabilidade pequena, porém não nula.

A ocorrência de falhas pode estar associada a falhas de projeto, falhas de equipamentos, erros operacionais humanos e a falhas nos softwares de controle de processo (YOE, 2012).

Neste contexto, falhas cujos efeitos não proporcionem riscos ao homem, ao meio ambiente e às instalações, denominadas como falhas não críticas (IEC-61508, parte IV (IEC, 2010)), podem ser tratadas pelo Sistema de Controle Básico do Processo – BPCS (IEC 61508 (IEC, 2010)), em que o sistema de controle opera para regenerar o sistema a partir da ocorrência destas falhas, de acordo com a arquitetura de controle proposta por Dei-Svaldi e Vautrin (1989), representada na Figura 1.5.

Por sua vez, para uma determinada classe de falhas, sua ocorrência pode resultar em efeitos que podem levar a um cenário catastrófico, sendo classificadas como falhas críticas (NBR 5462 (ABNT, 1994))(IEC-61508, parte IV (IEC, 2010).

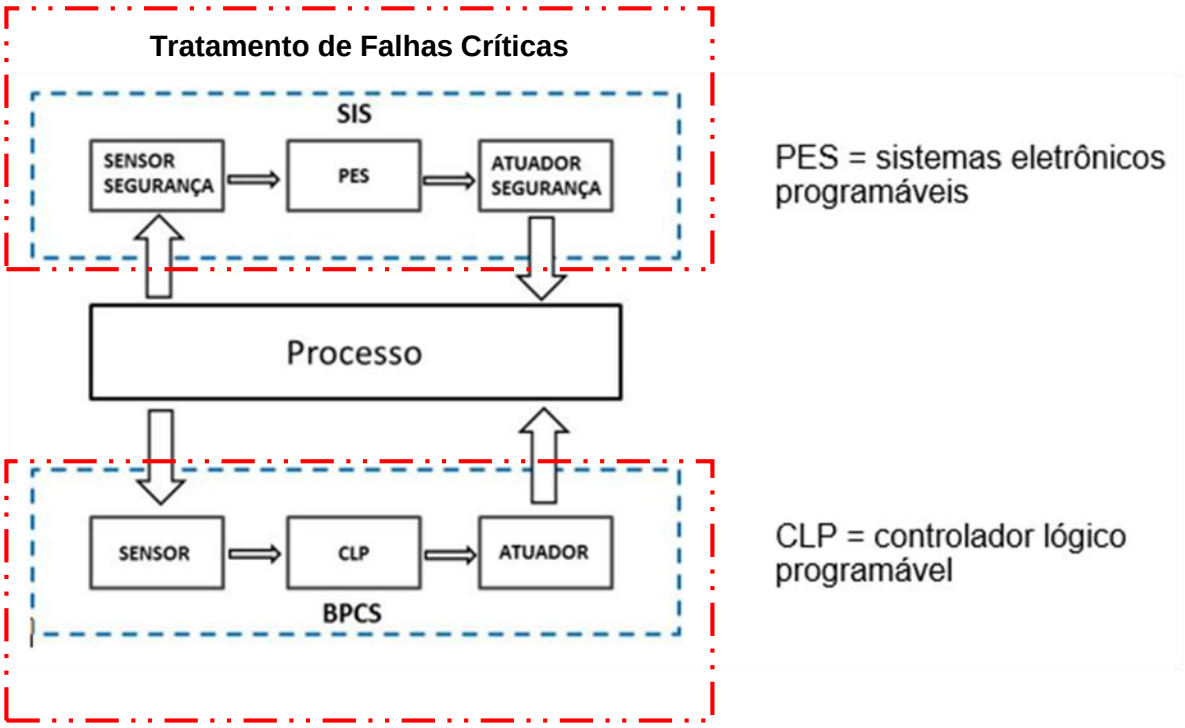



Figura 1.5 – Arquitetura de controle de um Sistema Instrumentado de Segurança. Fonte: Squillante (2011).

Para tais classes de falhas, a utilização de Sistemas Instrumentados de Segurança – SIS, são uma solução para implementação de níveis ou camadas de redução de riscos, conforme se observa na Figura 1.6, inerente a todo SP, para um nível aceitável, propondo camadas sucessivas de prevenção / mitigação aos efeitos da ocorrência de falhas críticas.

Normas, como a IEC 61508 referenciam os parâmetros de desempenho de um SIS, além de requisitos para a implementação e a determinação do ciclo de vida do projeto de um SIS.

Outras normas, derivadas da IEC 61508, aplicam-se a determinados seguimentos: a norma IEC 6151, por exemplo, é voltada para a indústria de processos.

O propósito de um SIS é monitorar eventos potencialmente críticos, com consequências catastróficas, e alarmar ou executar ações pré-programadas para a prevenção de acidentes ou mitigação das consequências geradas pela ocorrência de um evento crítico num sistema de produção (GOBLE, 1998).

Figura 1.6 - Camadas de redução de riscos (adaptado da norma IEC 61511-1).

## 1.1 Motivação

Baseado numa pesquisa em bases de dados como o *Web of Science* e o *Scopus,* observou-se que inúmeros trabalhos tratam de (*i*) práticas para evitar a ocorrência de uma falha, tais como os programas de manutenção preventiva e preditiva (ARATO JR, 2003); (*ii*) sistemas de monitoração de falha, tais como o RCM – *Reliability centered maintenance* - ou manutenção centrada na confiabilidade (MOUBRAY, 2001); (*iii)* sistemas de detecção e controle que monitoram o comportamento da falha em função do tempo, ou ciclos, seguindo curvas de probabilidade ou taxas de falha e, de acordo com determinados critérios gerenciais, providenciam a parada do equipamento ou instalação para a devida manutenção (KELLY, 2006) (LEVITT e NYMAN, 2010).

Outros trabalhos (MORALES, GARCIA MELO e MIYAGI, 2007) (RU e HADJICOSTS, 2008) (WANG, *et al.*, 2008) (ZHANG e JIANG, 2008) (SUMMERS e RANEY, 1999) (SALLAK, SIMON e AUBRY, 2008), tratam de falhas em SPs, com foco na classificação das falhas e de modelos para diagnóstico. Riascos (2002) trata de estratégias para a detecção e tratamento de falhas relacionadas ao processo produtivo em si, de modo que se entende que ele é tratado na camada BPCS da arquitetura proposta (IEC 61508 (IEC, 2010)) para um SIS. O contexto para a detecção e tratamento de falhas cujos efeitos possam comprometer o homem, o meio ambiente e ao próprio equipamento não são abordados.

Normas relacionadas ao tema, tai como a IEC 61508 (IEC, 2010) e IEC 61511 (IEC, 2003) tratam dos requisitos, e não de procedimentos ou métodos para a implementação das camadas de proteção.

Em Squillante (2011) e Squillante *et al* (2011) a abordagem para diagnóstico, tratamento e coordenação de falhas críticas utilizando-se o conceito de SIS é feita, porém limitada à camada SIS de prevenção (Figura 1.6) em que o sistema, composto por um controlador programável de segurança, e de sensores e atuadores independentes da camada BPCS, degenera o sistema a um estado seguro quando ocorre o diagnóstico de ocorrência de uma determinada falha crítica.

Em Marseglia *et al* (2014), há uma abordagem híbrida (estocástica e determinística) para o diagnóstico de falhas, porém não se fala de ações de mitigação. Já Lopez Estrada *et al* (2014) aborda uma sistemática para o diagnóstico de falhas de sensores e a proposta de seu isolamento no sistema.

Há uma lacuna, portanto, em uma camada de proteção ativa que possa inferir ações de mitigação aos efeitos da ocorrência deste tipo de falha, de forma a se evitar a ocorrência de catástrofes. A velocidade de atuação destas ações deve contribuir para a eficácia. Se a ação de mitigação se mostrar lenta, a catástrofe já pode ter ocorrida.

Por outro lado, para a determinação de algoritmos de controle é necessário o conhecimento da dinâmica do objeto de controle, que pode ser obtido, convencionalmente, por meio de modelos matemáticos ou equações diferenciais, dentro de uma determinada faixa de operação.

Ocorre que o comportamento dinâmico de uma planta em estado de falha obviamente não está sob uma condição normal de operação. Logo, o comportamento

dinâmico do SP neste estado em geral não é conhecido, não se tendo, portanto, o determinismo de seu comportamento.

Bancos de dados para responder a tais questões são praticamente inexistentes, pois a estados de falha são associados, de forma geral, apenas às ações de *shutdown* e ao gerenciamento de alarmes quando da detecção da variação ou valor anormal de uma variável de monitoramento ou processo.

## 1.2 Justificativa

Diante do exposto, caracteriza-se a necessidade em se propor uma sistemática para a implementação de uma camada de proteção ativa para a mitigação dos efeitos da ocorrência de falhas críticas em SPs, de modo a reduzir o risco inerente do processo a um patamar aceitável, com o objetivo de se evitar a ocorrência de catástrofes, preservando a vida, o meio ambiente e as instalações.

Esta sistemática deve ser baseada no conceito de Sistemas Instrumentados de Segurança, por ser uma referência em termos de normas internacionais como IEC 61508 e IEC 61511. Tais normas apresentam os requisitos de projeto, a definição dos conceitos, os parâmetros de desempenho e o ciclo de vida do projeto e implementação de Sistemas Instrumentados de Segurança.

## 1.3 Objetivo

Este trabalho tem como objetivo desenvolver uma sistemática para o desenvolvimento de um sistema de controle para a mitigação de falhas críticas em SPs, utilizando-se o conceito de Sistemas Instrumentados de Segurança – SIS, com referência às normas IEC 61508 / IEC 61511. Neste contexto, têm-se como metas:

(a) A identificação dos elementos críticos de um SP, ou seja, aqueles que, sob estado de falha, podem levar a um cenário catastrófico, colocando em risco a integridade física dos trabalhadores, causar a poluição do meio ambiente e ocasionar danos às instalações.

(b) A identificação dos efeitos gerados pelas falhas destes elementos críticos, e a especificação de dispositivos que possam detectar a ocorrência de tais efeitos.

(c) A proposta de ações para a mitigar dos efeitos da ocorrência das falhas, de forma antecipativa à ocorrência de catástrofe.

(d) O desenvolvimento de um sistema de controle capaz de detectar a ocorrência da falha e, através de uma lógica antecipativa, mitigar os possíveis efeitos, de forma a potencializar as ações controladas para eliminar as consequências das falhas, levando o sistema a um estado seguro desejado.

É fundamental destacar que o presente trabalho utiliza como referência normas pertinentes ao tema, como as já citadas IEC 61508/61511, e também as normas IEC 61131-3, IEC 61131-7, ABNT NBR 5462, ANSI/ISA S5.1, IEC 60812, IEC 61025 e IEC 61882.

## 1.4 Estrutura do trabalho

Inicialmente tem-se a contextualização do uso da automação industrial nos sistemas produtivos modernos e a identificação de problemas decorrentes, que podem gerar riscos à população, ao meio ambiente e às próprias instalações. A verificação de lacunas quanto à propostas de soluções para a mitigação dos efeitos de falhas críticas em SP serviu de base para a motivação do desenvolvimento deste trabalho.

O segundo capítulo é dedicado à revisão bibliográfica sobre os conceitos teóricos, as técnicas e as ferramentas pertinentes, além de normas relacionadas.

O terceiro capítulo trata da proposta do trabalho, que objetiva uma sistemática para a implementação de um sistema de controle para a mitigação de falhas críticas em sistemas produtivos, com referência às normas vigentes.

Já o capítulo quatro apresenta dois exemplos de aplicação em um sistema produtivo real, com o detalhamento de cada passo da sistemática, e a análise dos resultados obtidos para cada exemplo.

No capítulo cinco são apresentadas as principais conclusões do trabalho, além do encaminhamento para a continuidade desta pesquisa.

O trabalho encerra-se com a bibliografia utilizada e documentos adicionais, composto pelo Anexo A – Redes de Petri, o Anexo B, com a matriz causa-efeito do caso de uso 2, o Apêndice B, composto pela camada SIS de gás e fogo, e o Anexo C, composto pela matriz causa-efeito da camada SIS de gás e fogo.

# 2. REVISÃO BIBLIOGRÁFICA

## 2.1 Sistemas Instrumentados de Segurança

De acordo com especialistas, a utilização de Sistemas Instrumentados de Segurança SIS, são uma solução para implementação de níveis ou camadas de proteção com objetivo de redução do risco inerente de um sistema produtivo.

De acordo com Lundteigen e Rausand (2009), um SIS é instalado para detectar eventos perigosos (ex.: vazamentos de gases inflamáveis, explosivos ou venenosos, pressões e temperaturas em níveis muito elevados em relação aos seus níveis operacionais) para evitar e/ou mitigar suas conseqüências aos seres humanos, meio-ambiente e equipamentos a partir do uso de tecnologias modernas como equipamentos elétricos, eletrônicos e eletrônicos programáveis (E/E/EP). Em geral os SIS são usados para trazer o processo a um estado seguro (ex.: *shutdown*) quando pré-condições de variáveis de controle são violadas (ROUVROYE e VAN DEN BLIEK, 2002). Geralmente é constituído por um ou mais sensores, um ou mais controladores programáveis (freqüentemente chamados de *logic solvers*) e um ou mais atuadores (LUNDTEIGEN e RAUSAND, 2009).

Há mais de uma década, Goble (1989) já ressaltava que segurança e confiabilidade são parâmetros essenciais em projetos de sistemas de controle. Entre os benefícios gerados com a implantação de um SIS estão:

- ✓ sistemas seguros e confiáveis,
- ✓ redução da perda de produção,
- ✓ redução de riscos.

### 2.1.1 Normas relacionadas a SIS

Dentre as normas que tratam da implementação de SIS em SP, pode-se destacar a IEC 61508 (IEC, 2010), e suas derivações para as demais indústrias de processos, (Figura 2.1).

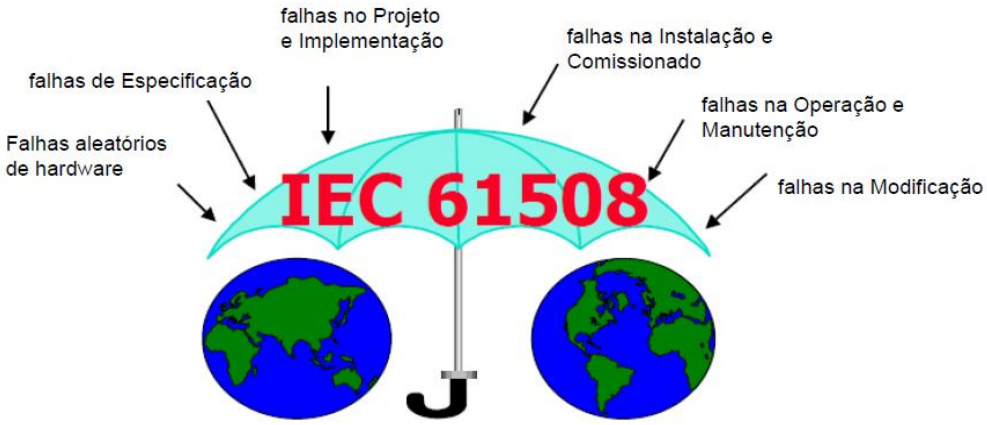



Figura 2.1 - IEC 61508 como referência à SIS em SP. Extraído de (Bojorge, 2012)

A norma IEC 61508 baseia-se em dois conceitos fundamentais:

- ✓ Ciclo de vida de segurança.
- ✓ Níveis de integridade de segurança.

O ciclo de vida de segurança é definido como um processo de engenharia que inclui todos os passos necessários para se atingir a segurança funcional exigida (EXIDA, 2007). Segundo a IEC 61508, o ciclo de vida de segurança é definido como um conjunto de atividades necessárias envolvidas na implementação de Funções Instrumentadas de Segurança (SIFs), ocorrendo durante o período de tempo que começa na fase de concepção do projeto e finaliza quando todas as funções instrumentadas de segurança não serão mais utilizadas. As etapas para a implementação de um SIS, bem como os estágios e a definição do ciclo de vida são representados na Figura 2.2

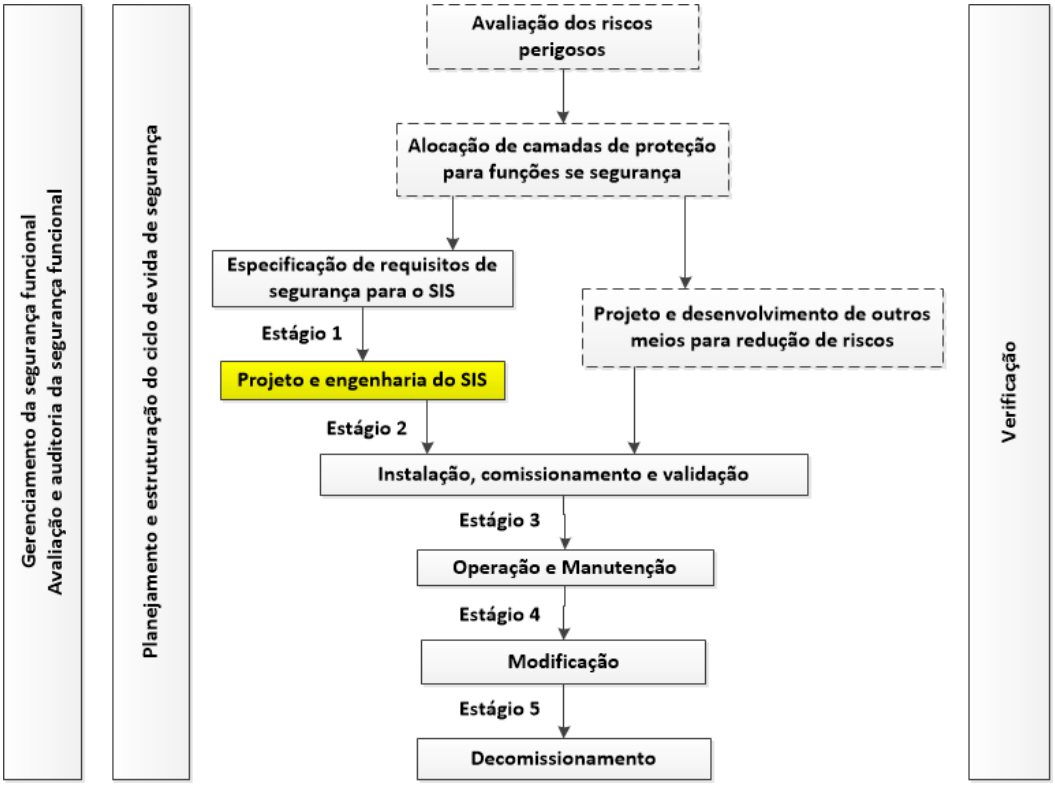



Figura 2.2 - Ciclo de vida de segurança (Adaptado da IEC 61511).

Outras normas, derivadas da IEC 61508, referenciam os requisitos para a implementação de SIS para cada tipo de sistema produtivo, conforme representado na Figura 2.3

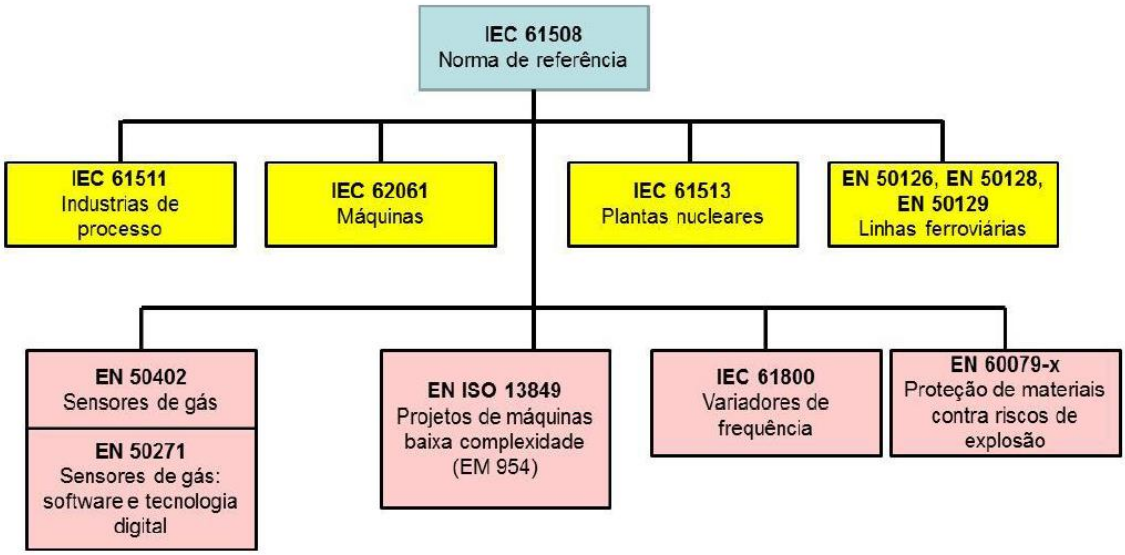



Figura 2.3 - Normas derivadas da IEC 61508 (Adaptado da (IEC, 2010)).

De acordo com a norma IEC 61508, as falhas críticas são definidas a partir da identificação das Funções Instrumentadas de Segurança (SIF). Ainda de acordo com a IEC 61508 parte IV (IEC, 2010), o conceito de **falha** pode ser definido como "condição anormal que pode provocar uma diminuição ou perda da capacidade funcional de uma unidade, para executar uma necessária função".

Baseado neste conceito, a norma define duas classes de falhas, as falhas não críticas e as falhas críticas. Falhas não críticas são aquelas cujos efeitos não representem riscos, e, portanto, devem ser tratadas pelo Sistema Básico de Controle de Processo, ou BPCS. Já as falhas críticas são aquelas cujos efeitos podem resultar em sérios riscos ao homem, ao meio ambiente e às próprias instalações.

Um SIS implementa suas SIFs por meio de: (a) um ou mais sensores; (b) um ou mais dispositivos de realização de controle (ex.: equipamentos elétricos, eletrônicos ou eletrônicos programáveis onde o mais comum são os controladores lógicos programáveis de segurança) e; (c) um ou mais atuadores. Para cada SIF é definido um parâmetro denominado Nível de Integridade de Segurança (SIL), conforme é descrito a seguir.

### 2.1.2 Nível de Integridade de Segurança (SIL)

O nível de integridade de segurança (*Safety Integrated Level* ou SIL) é a medida da confidência que se espera do sistema na realização de sua função de segurança quando solicitado (DUTUIT, *et al.*, 2008), ou seja, o SIL reflete aquilo que os usuários finais podem esperar de um dispositivo ou sistema na sua função de segurança e, em caso de falha, que a falha seja de maneira segura (LIU, *et al.*, 2008). Ainda de acordo com a norma IEC 61508, SILs são medidas de segurança de componentes/sistemas.

Existem quatro níveis SIL definidos na IEC 61508. O SIL 1 tem o menor nível de redução de risco. O SIL 4 tem o maior nível de redução de risco. A Tabela 2.1 mostra os níveis de integridade de segurança de acordo com a norma IEC 61508.

Tabela 2.1 - Níveis de integridade de segurança (SIL) – (IEC, 2010)

| Nível de Integridade de Segurança SIL | Fator de Redução de Risco RRF | Probabilidade média de falha na demanda $PFD_{avg}$ |
|---|---|---|
| SIL 4 | 100000 a 10000 | $>=10^{-5}$ a $<10^{-4}$ |
| SIL 3 | 10000 a 1000 | $>=10^{-4}$ a $<10^{-3}$ |
| SIL 2 | 1000 a 100 | $>=10^{-3}$ a $<10^{-2}$ |
| SIL 1 | 100 a 10 | $>=10^{-2}$ a $<10^{-1}$ |

De acordo com Goble (1989), a probabilidade de falha sob demanda (PFD) é um parâmetro importante para medir a capacidade de redução de risco de um SIS. O fator de redução de risco (FRR) pode ser definido como sendo a relação entre o risco inerente e o risco aceitável, de acordo com a Equação 2.1.

$$FRR = \frac{(risco\ inerente)}{(risco\ aceitável)} \qquad (2.1)$$

Ainda segundo Goble (1989), o fator de redução de risco é o inverso da PFD, de acordo com a Equação 2.2.

.

$$FRR = \frac{1}{PFD} \qquad (2.2)$$

Segundo Rouvroye e Van Den Bliek (2002) a PFD é a probabilidade média de que uma função de segurança não estará apta para executar sua função sob demanda do processo.

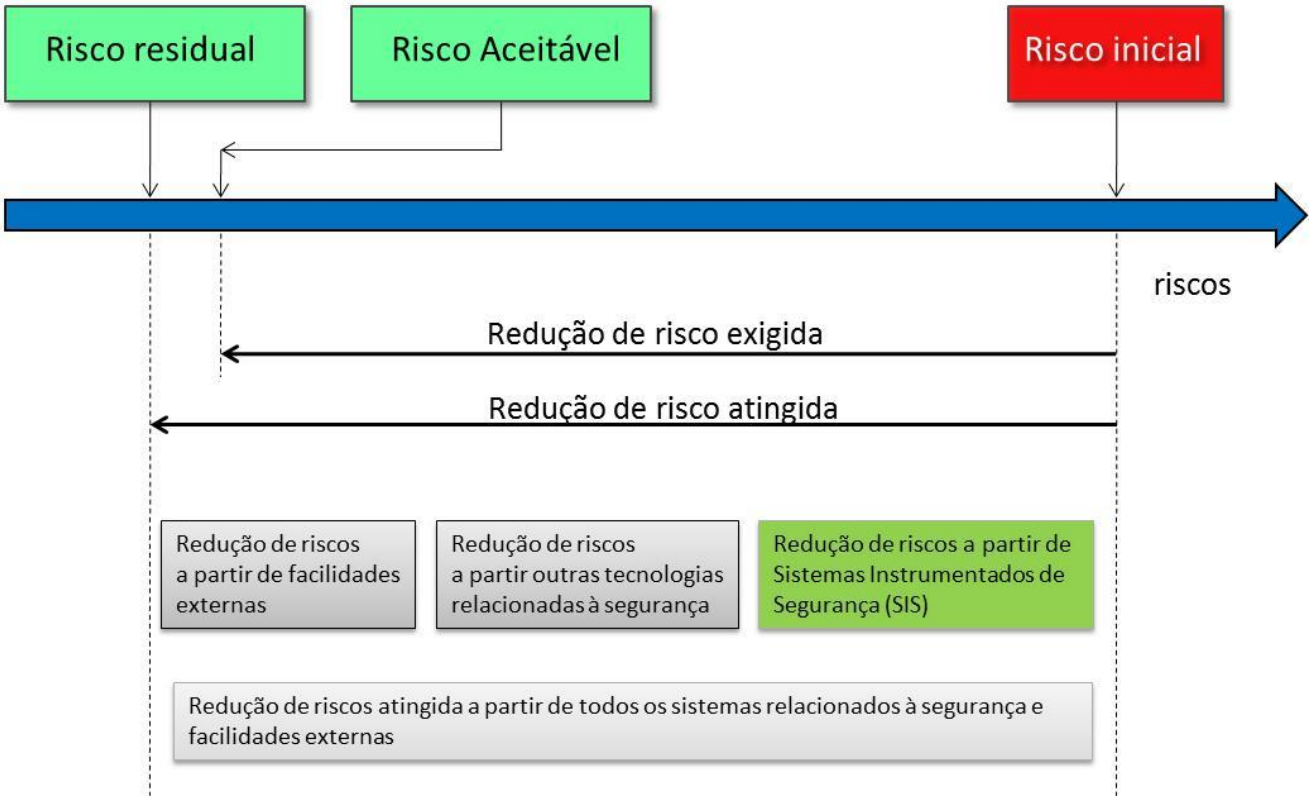
Importante ressaltar que os valores de PFD, que determinam o respectivo SIL devem ser aplicados para o conjunto da instalação, e não somente a um equipamento isolado. O fato de um atuador possuir certificação SIL 3 não implica que a instalação tenha este nível. Este conceito deve ser aplicado globalmente envolvendo todos os dispositivos contidos no SIS e o menor nível SIL identificado em um determinado dispositivo é que determinará o SIL do sistema (EXIDA, 2007).

### 2.1.3 Camadas individuais de proteção de riscos

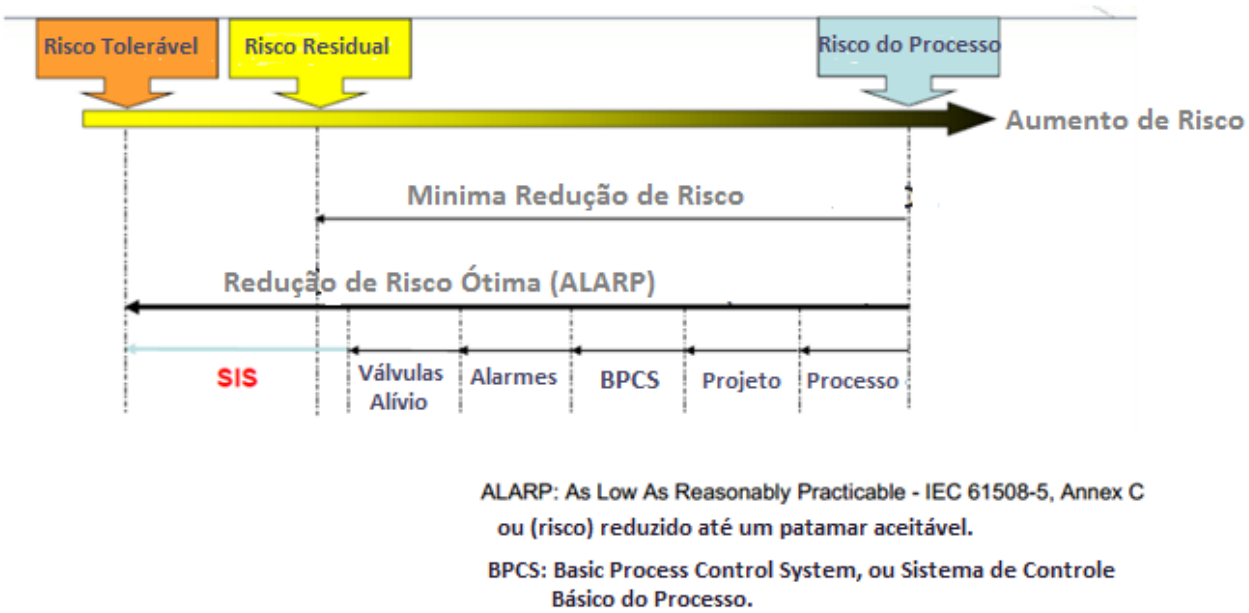
Conforme a IEC 61508, parte IV (IEC, 2010), o termo **risco** é definido como a combinação entre a probabilidade de ocorrência de um dano, associada à sua severidade. Já Bell (2005), define o termo “risco” como uma métrica para quantificar as lesões corporais, danos ambientais ou perdas econômicas em referência tanto à probabilidade do incidente acontecer como à magnitude da lesão, dano ou perda.

O risco de um sistema produtivo, portanto, pode ser classificado de acordo com a severidade de sua magnitude, podendo ser aceitável, ou de magnitude de severidade pequena, ou inaceitável. Quando o risco inerente de um sistema produtivo é maior que o risco aceitável, deve-se, necessariamente, tomar medidas para a redução deste risco a um patamar aceitável (GOBLE, 1998).

A Figura 2.4 ilustra a relação de redução do risco “inicial” de um SP a um nível de risco “aceitável”. Camadas individuais de proteção de riscos podem ser empregadas, sendo o SIS uma destas camadas. Outras camadas de proteção podem ser empregadas para a redução do risco, como por exemplo, por meio do uso de outras tecnologias relacionadas à segurança (exemplo: válvulas de alívio, etc) ou por meio de facilidades externas (ex: barreiras ou diques de contenção, invólucros ou compartimentos à prova de explosão, etc).




(a) Redução de riscos – conceitos gerais (baseada na Figura A.1 – IEC 61508-5;1998)




(b) Redução de riscos – conceitos gerais (baseada na figura A.1 – IEC 61508-5:1998).

Extraído de Invensys (2012)

Figura 2.4 - Aspectos associados à redução de risco em SIS

Por sua vez, salienta-se que as ações de prevenção e de mitigação são os dois contextos de ações complementares que devem ser previstas para a constituição das camadas de proteção de riscos de um SIS previstas na norma IEC 61508 para manter a operação de um SP em um nível aceitável de risco, de acordo com a Figura 2.4. Neste contexto têm-se:

**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;

**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;
- ✓ SIS.

O foco do presente trabalho está na camada SIS de Proteção Ativa de Mitigação, conforme representado na Figura 2.5.

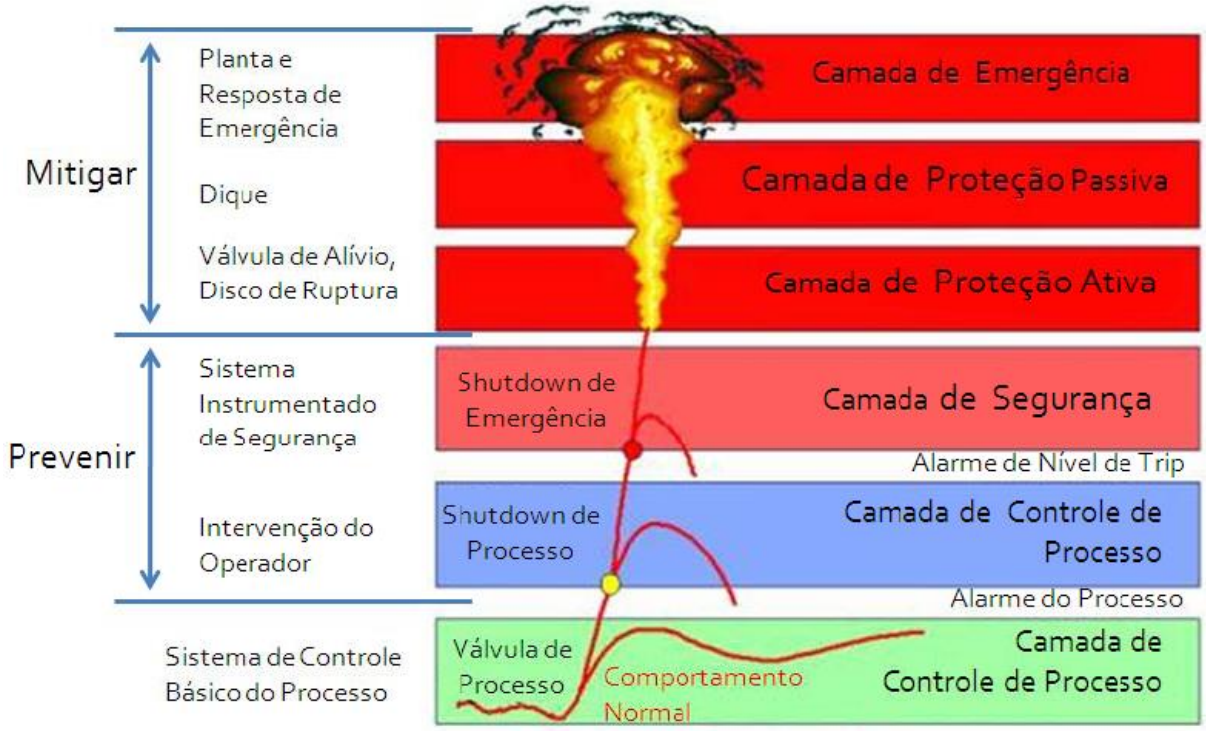



Figura 2.5 - Disposição das camadas SIS em um SP. Extraído de Bojorge (2012)

## 2.2 TÉCNICAS DE ANÁLISE DE RISCOS

A análise de riscos em plantas industriais é executada visando a prevenção de falhas e acidentes, a ação de mitigação dos efeitos causados por sua ocorrência e elaboração de planos de emergência. No entanto, para isso é necessária uma metodologia sistemática e estruturada de identificação e avaliação de riscos. De acordo com Roush (2000), as técnicas de análise de riscos permitem abranger todas as possíveis causas de acidentes com danos ao trabalhador, ao meio-ambiente e ao equipamento.

Observa-se, portanto, que um dos resultados de sua aplicação está na determinação dos componentes críticos do sistema, isto é, aqueles componentes que, sob falha, podem levar a um cenário catastrófico, ou ainda, os componentes que apresentam o maior produto entre frequência de ocorrência de falhas *versus* custos de manutenção (SCHUYLER, 2001). Em outras palavras, são os componentes que devem ter uma ação de mitigação dos efeitos causados quando em estado de falha, com o objetivo de degenerar o sistema a um estado seguro.

As técnicas de análise de risco podem ser concebidas com base no conhecimento técnico de um especialista no processo, por meio de manuais e documentos técnicos dos fabricantes e/ou fornecedores dos equipamentos e sistemas, através de dados de registros históricos de falhas e suas consequências, elaborados geralmente pelas equipes de manutenção, ou ainda com base em informações de plantas de outros sistemas similares (*benchmarking)* (MODARRES, KAMINSKIY e KRIVTSOV, 2009) (RAUSAND, 2011). Neste caso, devem ser observadas as características próprias de cada instalação, o padrão de desempenho adotado, bem como o contexto operacional ou ainda carregamentos a que são submetidos.

Para uma melhor compreensão das técnicas de análise de risco, faz-se necessária uma apresentação dos principais modos de falha de componentes.

### 2.2.1 Modos de Falha de Componentes

De acordo com a norma ABNT NBR 5462 (ABNT, 1994), tem-se as definições a seguir:

- **Componente, ou dispositivo**: pode ser definido como qualquer item físico de uma instalação, equipamento ou sistema, e que tenha papel atuante em seu desempenho.
- **Sistema**: pode ser definido como o conjunto ordenado de elementos ou dispositivos que se interligam e interagem entre si com o objetivo de gerar um produto específico. Este produto pode ser uma tarefa, um produto ou ainda um serviço.
- **Modo de falha**: é uma não conformidade no funcionamento de uma peça, componente ou sistema, em relação ao previsto em projeto. É relacionada a características físicas ou a parâmetros de desempenho do produto ou processo.
- **Defeito**: pode ser associado a um parâmetro de desempenho abaixo do esperado em projeto, mas ainda não em um patamar mínimo que esteja considerado como em estado de falha.

A um dispositivo pode ser associada uma ou mais funções (KECECIOGLU, 1995), tendo-se, via de regra, uma função primária que constitui a razão da existência deste dispositivo no equipamento sendo, portanto, imediatamente identificável. Entretanto, pode-se associar uma função secundária, nem sempre de fácil identificação, porém também importante para a operação do sistema a que pertence. Para efeito de exemplificação, a suspensão de um automóvel possui a função primária de absorver imperfeições do solo e conferir estabilidade ao veículo, mas também a função secundária associada à integridade estrutural do mesmo.

Considerando o contexto do presente trabalho, falha de um dispositivo, portanto, fica caracterizada quando o mesmo não mais é capaz de desempenhar uma ou mais das suas funções (primárias ou secundárias) ainda que não esteja completamente incapacitado. Ainda de acordo com a norma ABNT NBR 5462 (ABNT, 1994) as falhas podem ser classificadas como *aleatórias, por deterioração* ou *catastrófica.*

- **Falha aleatória**: qualquer falha cuja causa ou mecanismo faça com que seu instante de ocorrência se torne imprevisível, a não ser no sentido probabilístico.
- **Falha por deterioração**: falha que resulta de mecanismos de deterioração inerentes ao item, os quais determinam uma taxa de falha crescente com o tempo, devido ao seu envelhecimento.
- **Falha catastrófica**: falha repentina, a qual não pode ser prevista por monitoração, que resulta na incapacidade completa de um item desempenhar todas as funções requeridas.

Um componente pode falhar por diversas causas, associadas a inúmeros estados ou combinações de estados, porém geralmente estão associadas a um modo de falha ou, em determinados casos, a dois ou mais modos de falha que ocorreram de forma simultânea. O modo de falha não indica a causa da falha, pois pode-se ter várias causas para o mesmo modo de falha, como também vários modos para a mesma causa.

Temos a seguir os principais modos de falha de componentes (ABNT, 1994):

- ✓ Deterioração;
- ✓ Lubrificação;
- ✓ Contaminação;
- ✓ Desmontagem;

- ✓ Ação humana;
- ✓ Sobrecarregamento deliberado;
- ✓ Sobrecarregamento não deliberado ou não intencional;
- ✓ Sobrecarregamento repentino;
- ✓ Variação súbita de especificação.

### 2.2.2 Série de Riscos - SR

Técnica que permite a determinação da sequência de riscos associados ao evento catastrófico, que é considerado o risco principal (MODARRES, 2006). A partir dos riscos iniciais ou básicos, são sequenciados todos os riscos subsequentes capazes de contribuir na série, resultando no risco principal.

### 2.2.3 Análise Preliminar de Riscos – PHA

Técnica aplicada geralmente nas fases de concepção e/ou projeto de sistemas, principalmente quando do uso de novas tecnologias que carecem de maiores informações sobre seus riscos. Por meio desta técnica, uma análise é realizada na fase de projeto, de modo com que as mudanças necessárias, em função dos riscos potenciais, não impliquem em custos excessivos, sendo portanto mais fácil de ser executada (RAUSAND, 2011).

### 2.2.4 What-If – WI

Esta técnica examina ordenadamente as respostas do sistema frente às falhas de equipamentos, erros humanos e condições anormais do processo. Para o desenvolvimento desta técnica, se faz necessário a constituição de uma equipe com conhecimentos básicos sobre o processo a ser analisado e sua operação. Esta equipe procura responder a questões do tipo: “O que...se... ?” (MODARRES, 2006).

Exemplo: “O que ocorreria se a válvula de alívio não abrisse na pressão especificada?”.

Estas questões são elaboradas na tentativa de identificar os riscos potenciais presentes no processo. Como depende da experiência e do conhecimento do grupo de análise, esta técnica normalmente é utilizada como complemento ou parte auxiliar de outras técnicas.

### 2.2.5 Checklist

Esta técnica é utilizada para se assegurar a concordância entre as atividades desenvolvidas e os procedimentos operacionais padronizados (RAUSAND, 2011). Desta forma, as partes constituintes de um sistema ou sequências de operação / manutenção são analisados por comparação com uma lista pré-estabelecida, que pode ser elaborada com o auxílio dos manuais técnicos dos fabricantes / fornecedores, na tentativa de descobrir e documentar as possíveis deficiências do sistema. Geralmente o *checklist* é utilizado para embasar ou fortalecer os resultados de outras técnicas de análise de riscos. Fazem parte dos *checklists* partes de equipamentos ou processos operacionais de unidades industriais, ou ainda procedimentos e equipamentos de segurança padronizados.

### 2.2.6 What-If / Checklist – WIC

Como o próprio nome sugere, esta técnica une as características técnicas do *checklist* com o conhecimento da equipe ou *brainstorming* do *what-if*, resultando em uma análise mais detalhada e completa do sistema (MODARRES, KAMINSKIY e KRIVTSOV, 2009).

### 2.2.7 Técnica de Incidentes Críticos – TIC

Relativamente recente entre as técnicas de análise de riscos, é resultado de estudos realizados no Programa de Psicologia de Aviação da Força Aérea dos Estados Unidos. Esta técnica busca identificar os riscos de um sistema com base na análise do histórico de incidentes críticos ocorridos, os quais são levantados por entrevistas com as pessoas que possuem elevado conhecimento técnico a respeito do processo em análise (MODARRES, 2006).

### *2.2.8* Análise de Modos de Falha e seus Efeitos – FMEA

O FMEA, definido na IEC 60812 (IEC, 2006) e ABNT NBR 5462 (ABNT, 1994) como Análise dos Modos de Falha e seus Efeitos *(**F**ailure **M**odes and **E**ffects **A**nalysis)*, envolve um estudo detalhado e sistemático das possíveis falhas de componentes ou de sistemas mecânicos. Os modos de falha de cada componente são identificados e os efeitos destas falhas no sistema são avaliados, sendo propostas medidas de eliminação, mitigação e controle das causas e consequências destas falhas (MODARRES, KAMINSKIY e KRIVTSOV, 2009) (RAUSAND, 2011) (ROUSH, 2000).

Desta forma pode-se elencar quais os componentes críticos do sistema, ou seja, quais elementos que, sob falha, podem causar as consequências mais sérias ao sistema.

Deve-se refletir sobre cinco questões a respeito do sistema como base para uma correta elaboração do FMEA:

- ✓ Como cada componente do sistema pode falhar?
- ✓ Qual ou quais são seus modo(s) de falha?
- ✓ Quais os efeitos desta(s) falhas(s) sobre o sistema?
- ✓ Quão críticos são estes efeitos?
- ✓ Como detectar a falha?
- ✓ Quais as medidas contra estas falhas (evitar, prevenir a ocorrência, minimizar seus efeitos)?

Um exemplo de tabela usada na aplicação do FMEA é apresentado na Tabela 3.

Tabela 2.2 – Exemplo de tabela FMEA – adaptado de Helman (1995).

| FORMULÁRIO FMEA | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Produto/ Processo: | | | | | | Área envolvida: | | | | | | | Data Elaboração: | | | | |
| Fornecedor: | | | | | | Aplicação: | | | | | | | Data Revisão: | | | | |
| ITEM | NOME DO COMPONENTE OU PROCESSO | FUNÇÃO DO COMPONENTE OU PROCESSO | FALHAS POSSÍVEIS | | | ATUAL | | | | | AÇÃO CORRETIVA | | RESULTADO | | | | |
| | | | MODO | EFEITO(S) | CAUSA(S) | CONTROLES ATUAIS | ÍNDICES | | | | RECOMENDAÇÕES | TOMADA | ÍNDICES REVISTOS | | | | RESPONSÁVEL |
| | | | | | | | O | G | D | R | | | O | G | D | R | |
| | | | | | | | | | | | | | | | | | |

| Probabilidade de Ocorrência | Gravidade | Probabilidade de Detecção | Risco |
|---|---|---|---|
| muito remota.....1 | | muito alta.....1 | |
| muito pequena.....2 | apenas perceptível.....1 | alta.....2 | baixo.....2 |
| pequena.....3 | pouco importante.....2 e 3 | moderada.....3 | moderado.....3 |
| moderada.....4,5,6 | moderadamente grave.....4 a 6 | pequena.....4,5,6 | alto.....4,5,6 |
| alta.....7,8 | grave.....7 e 8 | muito pequena.....7,8 | |
| muito alta.....9,10 | extremamente grave.....9 e 10 | remota.....9,10 | |

Uma limitação do FMEA é que este estudo é centrado no componente, por isso possui limitações quando vários modos de falha ocorrem de forma simultânea.

Esta técnica pode incluir o nível de gravidade das consequências e as probabilidades de ocorrência, sendo denominada, neste caso, de FMECA (IEC 60812 (IEC, 2006)) ou Análise Crítica de Modos de Falhas e Efeitos.

## *2.2.9* Análise de Árvore de Falhas – FTA

Metodologia de raciocínio dedutivo que parte de um evento - uma falha específica do sistema, denominada evento topo, e busca determinar relações lógicas de falhas de componentes e erros humanos que podem ser associados à ocorrência do evento topo (MODARRES, KAMINSKIY e KRIVTSOV, 2009) (ROUSH, 2000) (VILLEMEUR, 1992).

Descrita na IEC 61025 (IEC, 2008), a análise é realizada por meio da construção de árvore lógica, partindo do evento topo para as falhas básicas. Utilizada para quantificar a frequência ou a probabilidade de falha do sistema, através da quantificação da probabilidade de falha de cada um dos componentes do sistema. Relações lógicas geram a probabilidade de falha do sistema, a partir de seus componentes, utilizando álgebra booleana.

De posse dos valores de probabilidades de falha, podem ser feitas inserções no sistema, como a utilização de paralelismos para o aumento da confiabilidade do sistema para níveis desejados, principalmente para os elementos críticos do sistema, que por sua vez podem ser identificados por meio do estudo do FMEA.

Um estudo qualitativo também pode ser realizado, não envolvendo os valores de probabilidades de ocorrência, somente o relacionamento lógico.

A vantagem da FTA sobre o FMEA é que o FTA é um processo centrado nos sintomas da falha, por isto leva em consideração a combinação dos modos de falhas dos diversos componentes na ocorrência da falha. A Tabela 2.3 ilustra os elementos estruturais de uma FTA:

Tabela 2.3 - Elementos estruturais de uma FTA. Adaptado de Helman e Andrey (1995)

| SÍMBOLO | SIGNIFICADO |
|---|---|
| Retângulo | Eventos que são saídas de portas lógicas |
| Círculo | Eventos associados a falhas básicas |
| | Porta lógica de relação causal (e/ou) |

A Figura 2.6 ilustra um exemplo de aplicação de uma estrutura de FTA:

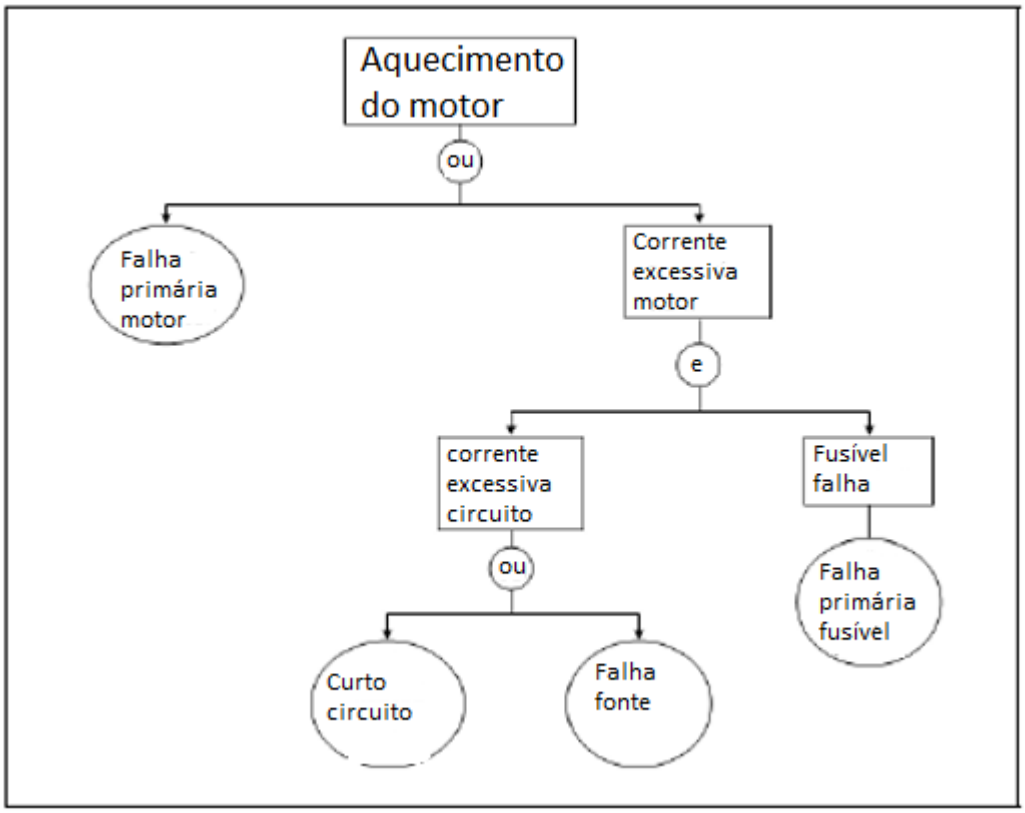



Figura 2.6 - Exemplo de aplicação da FTA Extraído de Takayama (2008).

## 2.2.10 Análise de Árvore de Eventos – AAE

Nesta análise, parte-se de um evento básico, resultante de uma falha específica de um equipamento ou erro humano, denominado evento iniciador, para determinar um ou mais estados subsequentes de falhas possíveis (MODARRES, KAMINSKIY e KRIVTSOV, 2009) (RAUSAND, 2011) (VILLEMEUR, 1992). Desta forma, a AAE considera a ação a ser tomada pelo operador ou a resposta do processo para o evento inicial. Assim como na FTA, o estudo é realizado por meio de uma árvore, partindo-se do evento iniciador, de sorte a quantificar as probabilidades de falha no sistema. Um diagrama esquemático de uma árvore de eventos é representado na Figura 2.7.

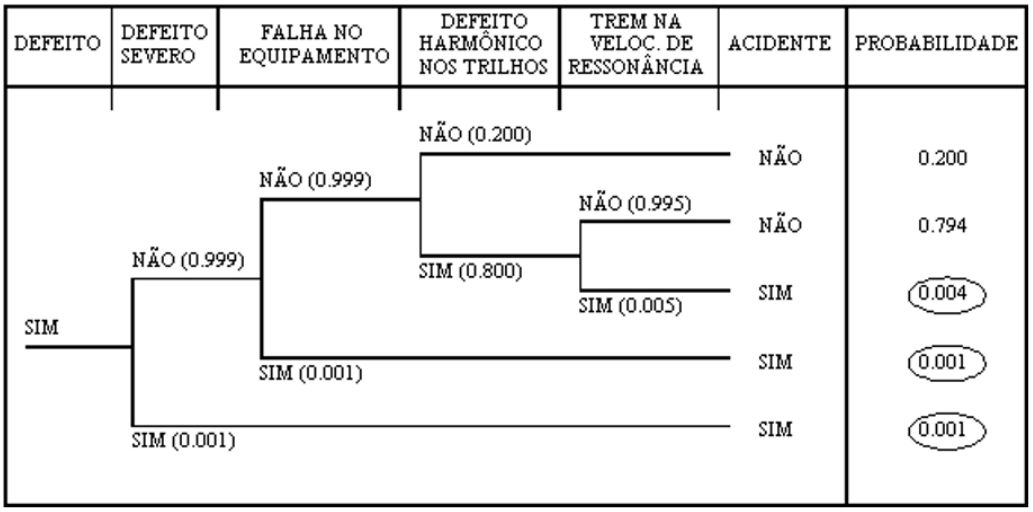



Figura 2.7 - Representação de uma árvore de eventos. Extraído de Takayama (2008)

## 2.2.10 Estudo de Operabilidade e Riscos – Hazop

O estudo de operabilidade e riscos, ou *HAZOP (**HA**zard and **OP**erability studies)* definido na IEC 61882 (IEC, 2001) foi desenvolvido para o exame eficiente e detalhado das variáveis de um processo, possuindo uma forte semelhança com o FMEA. Por meio do Hazop identificam-se os caminhos nos quais os equipamentos de processos podem falhar ou ser inadequadamente operados. É desenvolvida por uma equipe multidisciplinar, sendo guiada pela aplicação de palavras específicas – palavras guia – a cada variável do processo. Desta forma, geram-se os desvios dos padrões operacionais, os quais são analisados em relação às suas causas e consequências.

Dependendo do grau de severidade da consequência, possíveis tratamentos podem ser sugeridos. Para a aplicação da análise é importante utilizar diagramas de fluxo do processo (de acordo com a norma ISA S5.1 (ISA, 1984 (R1992)) baseado nos seguintes passos:

- ✓ Dividir o sistema em partes, e descrever o comportamento esperado de cada parte;
- ✓ Selecionar um parâmetro do processo;

- ✓ Aplicar as palavras guias ao parâmetro e identificar eventuais desvios;
- ✓ Determinar possíveis causas e consequências do desvio;
- ✓ Identificar sensores e atuadores para a identificação e tratamento do desvio.

A Tabela 2.4 ilustra um exemplo de tabela usado na aplicação do Hazop.

Tabela 2.4 – Exemplo de documentação de HAZOP–IEC 61882, (IEC, 2001).

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Título | | | | | | | Número da Folha: 2 de 4 | | |
| Número do documento | | | Número da Revisão | | | | Data: 17 de dezembro de 1998 | | |
| Responsáveis pelo estudo | | | LB, DH, EK, NE, MG, JK | | | | Data da Reunião: 15 de dezembro de 1998 | | |
| Elementos considerados | | | Linha de Transferência da alimentação do tanque A para o Reator | | | | | | |
| Objetivo do projeto | | | Material: A<br>Fonte: Tanque A | | Atividade:<br>Destino: | | Transferir continuamente com uma taxa maior que B<br>Reator | | |
| **n°** | **Palavra Guia** | **Elemento** | **Desvio** | **Possíveis Causas** | **Consequências** | **Medidas de Segurança** | **Comentários** | **Ações necessárias** | **Ação alocada para:** |
| 4 | Muito | Transferencia de A | Muita transferência<br><br>Aumento da taxa de fluxo de A | Diametro errado da tubulação<br><br>Especificação errada da bomba | Possível redução do Rendimento<br><br>O produto irá conter grande quantidade de A | Nenhuma | | Conferir o fluxo da Bomba e as suas características durante o comissionamento<br>Revisar os procedimentos do comissionamento | JK |
| 5 | Pouco | Material A | Pouca quantidade do material A | Nível Baixo no tanque | Sucção inadequada do produto<br><br>Possibilidade de vortex podendo causar uma explosão<br>fluxo inadequado | Nenhuma | Situação inaceitável | Alarme de nível baixo no tanque | MG |
| 6 | Pouco | Transferência de A (com taxa >B) | Redução da taxa de fluxo de A | Linha parcialmente bloqueada, vazamento, bomba com baixa performance, etc. | Explosão | Nenhuma | Situação inaceitável | Medição de fluxo de A, mais um alarme de baixa vazão e um sinal de fluxo baixo que desligue o bombeamento para B | JK |

## 2.3 SISTEMAS A EVENTOS DISCRETOS – SED

Ao longo da evolução tecnológica iniciada no final do século XIX, muitas soluções para os problemas de produção foram implementadas explorando a capacidade humana de abstrair situações e fazer com que sistemas se comportem de forma automática segundo uma lógica predefinida. Foram criados assim os sistemas concebidos e feitos pelo homem e para o homem (ITO, 1991) tentando abordar sistemas como linhas de produção e montagem, redes computacionais e de comunicação, sistemas de

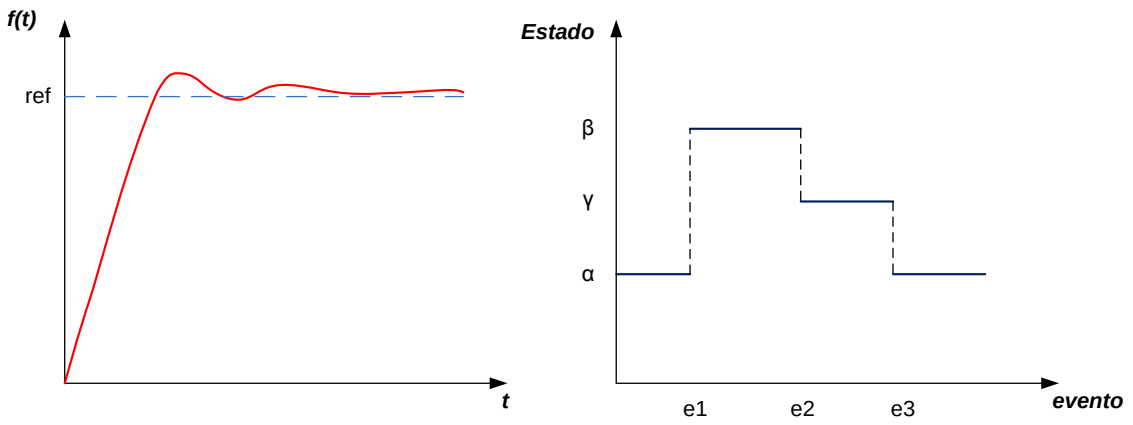
edifícios inteligentes, sistemas de transito, sistemas de comando, comunicação e controle inteligente, etc. (HO, 1987).

De acordo com a classificação de sistemas proposta por Cassandras (1993), SED é um sistema dinâmico, invariante no tempo, não linear, de estado discreto e dirigido por eventos instantâneos.

A ocorrência de eventos no SED é em geral em intervalos de tempo irregulares e desconhecidos (RAMADGE e WONHAM, 1988) o que caracteriza no sistema um primeiro nível de indeterminismo com relação ao tempo (SANTOS FILHO, 2000). Estes eventos (como a chegada de material, ‘inicio’ ou ‘término’ de uma tarefa ou processo, etc.) determinam a mudança de um estado para outro, que por sua vez é mantido constante até a ocorrência de um novo evento (CURY, 2001). Em contraposição, existem os sistemas de variáveis contínuas (SVC), cuja mudança de estado ocorre de forma continua ao longo do tempo, e cuja dinâmica é descrita por variáveis contínuas.

O estudo de SED é relativamente recente em relação ao conhecimento alcançado nos SVC (MIYAGI, 2007). Nota-se que a modelagem matemática dos SED ainda está longe de sua consolidação (HO, 1992), (CASSANDRAS e LAFORTUNE, 1999). A Figura 2.8 apresenta o comportamento de SED comparado com o comportamento de SVC. Esta comparação evidencia as diferenças que existem entre tais sistemas, sendo que nos SVC as variáveis pertencem a um conjunto infinito de valores, enquanto que nos SED as variáveis podem tomar valores de um conjunto discreto e finito, e cuja mudança só é realizada na ocorrência de um evento considerado instantâneo.

O problema de controle em SED consiste em estabelecer um conjunto de regras e restrições que permitam ao sistema comportar-se segundo uma lógica pré-estabelecida, atuando conforme uma seqüência de procedimentos que atendam o objetivo da produção, no caso de sistemas produtivos industriais. A Figura 2.8 representa uma comparação da evolução dinâmica de um SVC com um SED.




(a) SVC (b) SED

Figura 2.8 - Comportamento de SVC x SED. .

A Figura 2.9 representa a estrutura típica de um dispositivo de controle, que compõe um sistema de controle SED.

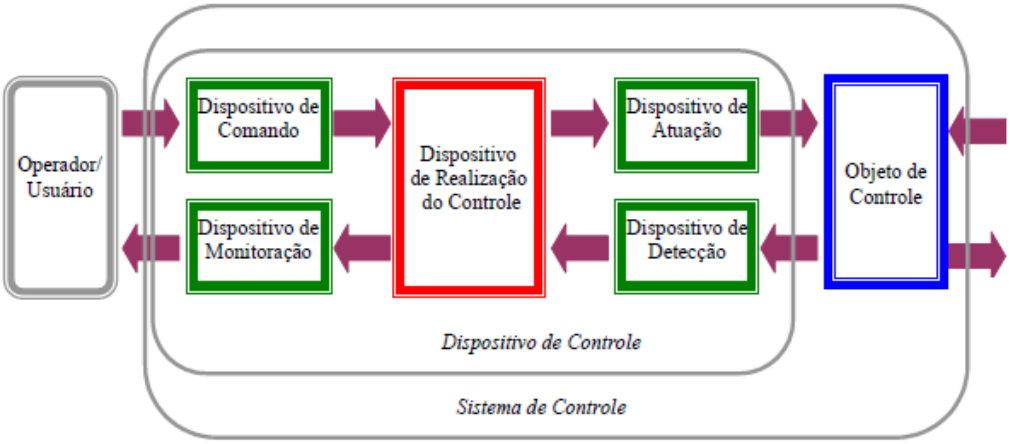



Figura 2.9 - Estrutura básica de um sistema de controle de SED (MIYAGI, 1996) (VILLANI, 2000)

## 2.3.1 Características de SEDs

O comportamento dinâmico de SEDs pode ser entendido a partir da evolução de seus estados, descritos por um conjunto de atividades, que possuem características

específicas e são realizadas a partir da ocorrência de eventos instantâneos. Neste contexto, pode-se identificar um SIS como uma classe de SEDs em que os processos são representados por funções instrumentadas de segurança que devem ser executadas para prevenção e mitigação de falhas.

A rede de Petri – RdP (BRAUER e REISIG, 2006), descrita no anexo A, como uma ferramenta gráfica e matemática, provê um ambiente uniforme para modelagem, análise formal e projeto de SEDs (ZURAWSKI e ZHOU, 1994) (ADAM; AT (ADAM, ATLURI e HUANG, 1998) (NASSAR, *et al.*, 2008) e é muito efetiva como técnica de descrição e especificação de processos (MORALES, GARCIA MELO e MIYAGI, 2007) (YOO, JEONG e CHO, 2010) (HAMADI e BENATALLAH, 2003).

Algumas das características mais importantes dos processos em SEDs e que estão presentes em um SIS são: sequência, paralelismo, sincronização e conflito de ações de prevenção e mitigação. Para modelar estes comportamentos, são utilizados modelos em rede de Petri nas próximas seções.

#### 2.3.1.1 Sequência

A sequência é a característica que indica uma ordem de realização das atividades envolvidas, isto é, qual conjunto de atividades deve ser concluído para que outro seja iniciado.

Em RdP, atividades são representadas por TRANSIÇÕES. Assim, a relação de sequência de duas atividades $t_1$ e $t_2$, pode ser representada adicionando-se um LUGAR $p_1$ e ARCOS ORIENTADOS de modo que $p_1 \in \cdot\, t_2$ e $p_1 \in t_1 \cdot$. Assim, para que a TRANSIÇÃO $t_2$ seja HABILITADA, é necessário que a TRANSIÇÃO $t_1$ tenha sido anteriormente disparada. A Figura 2.10 mostra duas atividades numa relação de sequência.

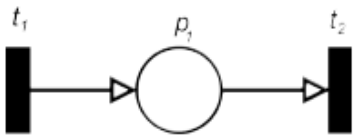



Figura 2.10 - Representação em RdP de duas atividades em sequência.

### 2.3.1.2 Paralelismo

O paralelismo é uma característica das atividades que podem ser executados concomitantemente sem que haja interferência da execução de um em outro, mas ambos com a mesma origem, isto é, uma única condição (estado) inicial.

Em RdP, o paralelismo de duas atividades pode ser modelado por duas TRANSIÇÕES $t_2$ e $t_3$ e dois LUGARES $p_1$ e $p_2$ e ARCOS ORIENTADOS de modo que $p_1 \in \cdot\, t_2$ , $p_2 \in \cdot\, t_3$ . Para representar a mesma condição inicial, adiciona-se mais uma TRANSIÇÃO $t_1$ e ARCOS ORIENTADOS para que, $p_1 \in t_1 \cdot$ e $p_2 \in t_1 \cdot$. Assim, quando ocorre o DISPARO da TRANSIÇÃO $t_1$, tanto a TRANSIÇÃO $t_2$ quanto a TRANSIÇÃO $t_3$ ficam posteriormente habilitadas, mas o disparo de um independe da outra. A Figura 2.11 ilustra um paralelismo de duas atividades.

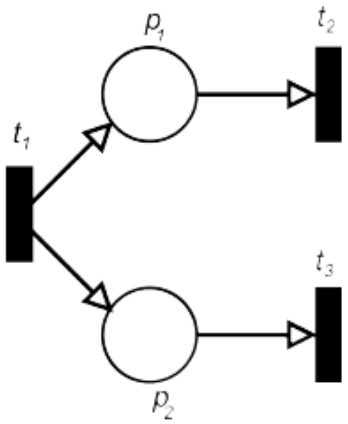



Figura 2.11 - Representação do paralelismo em RdP de duas atividades.

### 2.3.1.3 Sincronização

A sincronização é uma característica de sistemas em que uma atividade depende da execução de outras atividades. Em geral, a sincronização é feita entre atividades em paralelo, mas também pode ocorrer entre duas atividades com origens (processos) totalmente independentes.

Em RdP, a sincronização de duas atividades pode ser modelada por três TRANSIÇÕES $t_1$, $t_2$ e $t_3$ e dois LUGARES $p_1$ e $p_2$ e ARCOS ORIENTADOS de modo que $p_1 \in \cdot\, t_3$, $p_2 \in \cdot\, t_3$, $p_1 \in t_1 \cdot$ e $p_2 \in t_2 \cdot$. Assim, é necessário que tanto a TRANSIÇÃO $t_1$ como a TRANSIÇÃO $t_2$ sejam anteriormente disparadas para que a TRANSIÇÃO $t_3$ seja habilitada. A Figura 2.12 mostra uma sincronização de duas atividades.

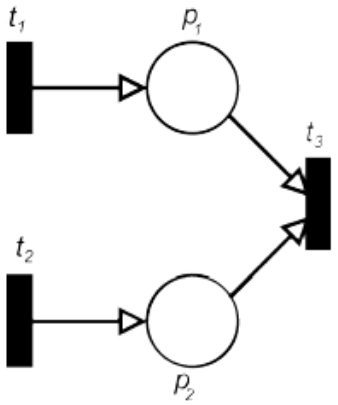



Figura 2.12 - Representação em RdP da sincronização de duas atividades.

### 2.3.1.4 Conflito

O conflito é uma característica de sistemas associada a escolha. Quando atividades estão em conflito, significa que apenas uma delas pode ser executada e a execução de uma dessas atividades inibe a execução das outras atividades que estavam em conflito.

Em RdP, o conflito de duas atividades pode ser modelado por três TRANSIÇÕES $t_1$, $t_2$ e $t_3$ e um LUGAR $p_1$ em que $p_1 \in \cdot\, t_2$, $p_1 \in \cdot\, t_3$ e $p_1 \in t_1 \cdot$. Assim, após o DISPARO da TRANSIÇÃO $t_1$, tanto TRANSIÇÃO $t_2$ quanto a TRANSIÇÃO $t_3$ ficam habilitadas, mas apenas uma delas pode ser DISPARADA. A Figura 2.13 ilustra este caso.

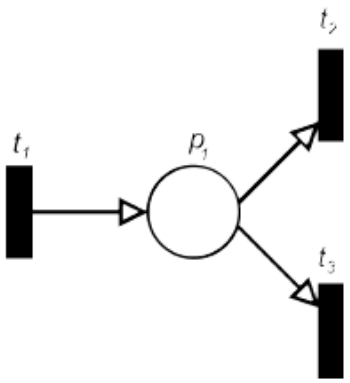



Figura 2.13 - Representação em RdP de conflito entre duas atividades.

## 2.4 CONTROLE FUZZY

### 2.4.1 Teoria de conjuntos fuzzy e números fuzzy

A Figura 2.14 ilustra a representação clássica de dois conjuntos A e B, com limites bem definidos de cada conjunto, representado pela linha que define sua extensão, e, portanto, definindo claramente duas regiões, uma região interna, em que um elemento pertence a este conjunto, e uma região externa ao limite, em que um elemento não pertence ao conjunto. Na teoria clássica de conjuntos, os valores 0 (Zero) ou 1 (Um) indicam “não contido” ou “contido” para um determinado elemento em relação a um dado conjunto.

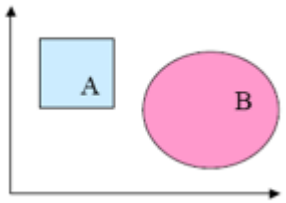



Figura 2.14 - Representação clássica de dois conjuntos.

Em contrapartida, na Figura 2.15 tem-se a representação de um conjunto nebuloso ou *fuzzy*, no qual a superfície que determina os limites de sua extensão não

é caracterizado por uma linha, e sim por uma região. Nota-se, portanto, uma região em seu interior, em que um elemento contido nesta região está contido neste conjunto, sendo atribuído um valor 1 – “contido”, uma região externa, não pertencente a este conjunto, e portanto um elemento nesta região não está contido neste conjunto – valor 0 ou “não contido”, e uma terceira região, caracterizada pela névoa.

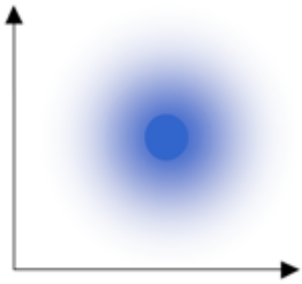


Figura 2.15 – Representação de um conjunto nebuloso ou fuzzy.

Neste caso, um elemento desta região pode ser caracterizado por um valor intermediário entre 0 e 1 em função de sua pertinência ao conjunto. Os números fuzzy são números que estão em um intervalo fechado entre o número 0 (zero) e o número 1(um), podendo assumir qualquer valor dentro desse intervalo. Como exemplo, o número 0.78 da relação de pertinência ao citado conjunto é um número *fuzzy* válido (ZADEH, 1996) (IEC, 2000) (SIMÕES e SHAW, 2007).

## 2.4.2 Operações com conjuntos fuzzy

As operações sobre conjuntos fuzzy são as mesmas utilizadas na teoria de conjunto clássico.

Para simplificação considere dois conjuntos fuzzy A e B, representados por funções de pertinência gráfica, conforme mostrado na Figura 2.16.

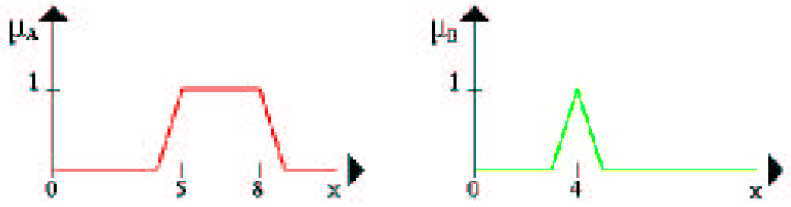



Figura 2.16 - Exemplos de função de pertinência.

Na Figura 2.17 é demonstrada a operação de intersecção dos conjuntos A e B, também conhecidos como operador mínimo ou conector lógico “AND” ou conector lógico “E”. Em azul têm-se o operador mínimo ou a intersecção dos conjuntos.

$$\mu_{A \cap B}(x) = \min(A,B) = A \wedge B$$

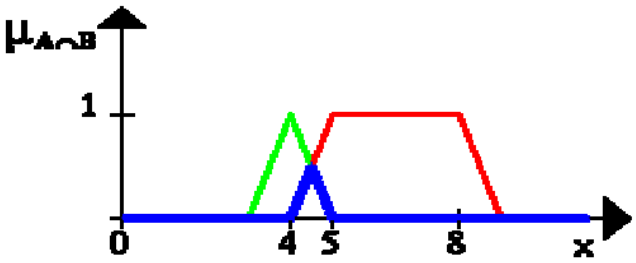



Figura 2.17 - Operador mínimo ou conector “AND” lógico.

Na Figura 2.18 é demonstrada a operação união dos conjuntos A e B, também conhecidos como operador máximo ou conector lógico “OR” ou conector lógico “OU”. Em azul têm-se o máximo operador ou a união dos conjuntos.

$$\mu_{A \cup B}(x) = \max(A,B) = A \vee B$$

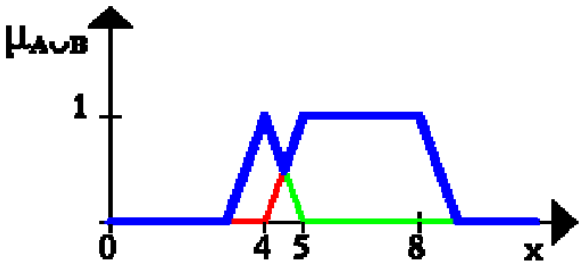



Figura 2.18 - Operador máximo ou conector “OR” lógico.

As operações mínimas e máximas são binárias, ou seja, são necessários dois resultados de conjuntos para se fazer essas operações. Na Figura 2.19 é demonstrado o “operador negação”, também conhecido como complemento ou simplesmente conector lógico “NOT” ou ainda conector lógico “não”. Em azul está a negação do valor em vermelho.

$$\mu \neg A\ (xi) = 1 - \mu A\ (xi)$$

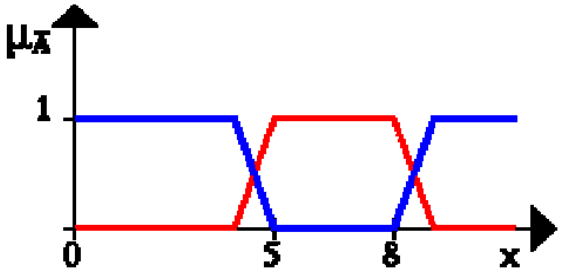



Figura 2.19 - Operador negação ou conector “NOT” lógico

## 2.4.3 Lógica Fuzzy

Nas últimas décadas se destacou da área de Inteligência Artificial - IA, um subcampo denominado Inteligência Computacional - IC. (ZADEH, 1996) (FOGEL, FUKUDA e GUAN, 1999). Segundo Andrade (2002) a IC trata de um conjunto de técnicas que exploram o potencial para se criar "máquinas inteligentes" por meio de modelagem dos comportamentos, e mecanismos que são subjacentes aos organismos biologicamente inteligentes.

A IC difere das demais técnicas de computação tradicionais, por tratar características como: abstração, imprecisão, aprendizado e busca por meio da evolução do conhecimento. As três áreas principais da IC são: computação fuzzy ou nebulosa, computação neural e computação evolutiva (ANDRADE, 2002). Uma representação das áreas de inteligência computacional – IC, é representada na Figura 2.20:

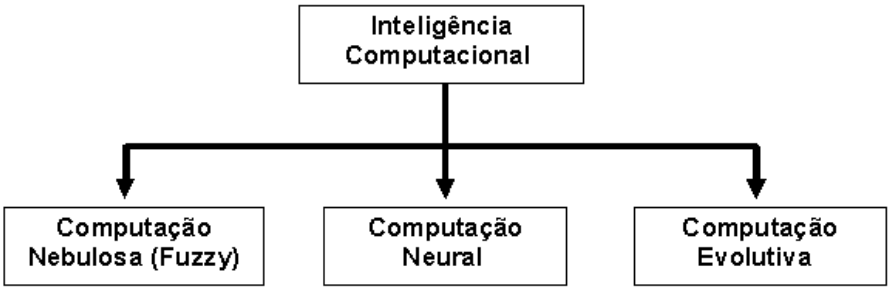



Figura 2.20 – Áreas de Inteligência Computacional (ANDRADE, 2002).

Uma representação do conhecimento em lógica fuzzy é feita através números fuzzy e de conjuntos fuzzy (ZADEH, 1965), representados por *funções de pertinência*.

As funções de pertinência podem ser representadas graficamente por segmentos de reta (IEC, 2000) (ARROFIQ e SAAD, 2010) (SIMÕES e SHAW, 2007).

Um exemplo de função de pertinência pode ser observado no exemplo abaixo, pela representação da altura de um indivíduo. Na Figura 2.21, pode-se observar a função de pertinência altura, composta por dois termos: baixo e alto. No eixo X está o valor real da altura de um individuo. Em Y está à conversão para o número fuzzy (que está no intervalo fechado de 0 a 1).

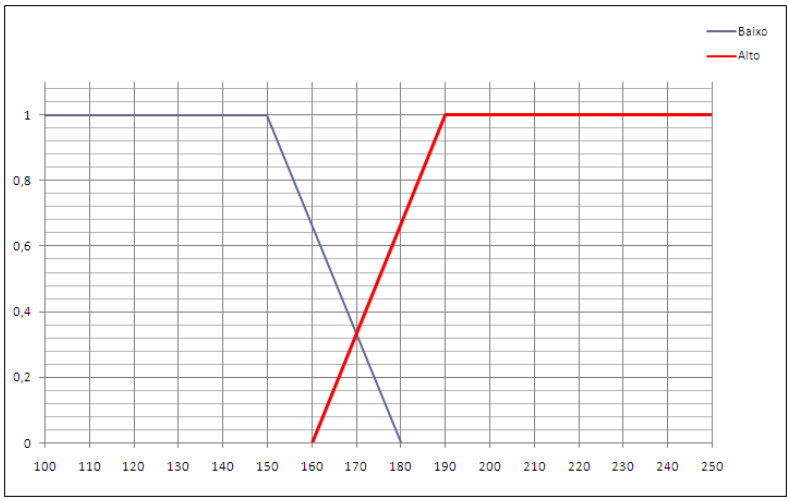



Figura 2.21 - Função de pertinência para altura.

A função de pertinência é uma função em termos matemáticos, isto é, dado seu domínio, se tem o valor de sua imagem.

A Equação 2.3 representa as funções de pertinência para a função altura da Figura 2.21.

$$\mu Baixo(x) = \begin{cases} 1 & \rightarrow 100 \leq x \leq 150 \\ -0{,}0334x + 6 & \rightarrow 150 \leq x \leq 180 \end{cases}$$

$$\mu Alto(x) = \begin{cases} 0{,}0334x - 5{,}33 & \rightarrow 160 \leq x \leq 190 \\ 1 & \rightarrow 190 \leq x \leq 250 \end{cases} \tag{2.3}$$

### 2.4.3.1 Fuzzificação

O processo de conversão de dados de entrada para um número fuzzy se chama fuzzyficação (IEC, 2000) (SIMÕES e SHAW, 2007) (YONEYAMA, 2000), cujo objetivo é converter números reais em números fuzzy.

Os números fuzzy são processados em um módulo de inferência que usa uma base de regras, esse módulo então gera novos números fuzzy. Esses novos números fuzzy passam por um processo chamado de defuzzificação, que converte um número fuzzy em um número real (IEC, 2000) (SIMÕES e SHAW, 2007) (YONEYAMA, 2000).

Para o exemplo da Figura 2.21, os resultados para a fuzzificação da variável altura são apresentados na Tabela 2.5.

Tabela 2.5 – *Fuzzificação* da variável altura

| **Valor real** | **Valor fuzzy** |
|---|---|
| μBaixo(140) | 1 |
| μBaixo(165) | 0,5 |
| μBaixo(180) | 0 |
| μAlto(140) | 0 |
| μAlto(165) | 0,2 |
| μAlto(180) | 1 |

O conhecimento é assim representado como uma função de pertinência.

### 2.4.3.2 Módulo de Inferência

A inferência é o módulo mais importante da lógica fuzzy. E ela é quem decide que atitude tomar, similar ao ser humano quando toma uma decisão.

(LEE, 1990) classificou os métodos (ou módulos) de inferência fuzzy em:

- Raciocínio fuzzy tipo 1 (Mamdani)
- Raciocínio fuzzy tipo 2 (Larsen)
- Raciocínio fuzzy tipo 3 (Tsukamoto)
- Raciocínio fuzzy tipo 4 (Takagi e Sugeno)

Os métodos mais utilizados em sistema de inferência em aplicações práticas são o de Mamdani e o Takagi e Sugeno.

Na Figura 2.22 é descrito o método de Mamdani.

- Regra semântica: máx-min

3. **Condicionais**: Intersecção nebulosa entre os graus de pertinência das entradas atuais nos termos primários-> coeficiente de disparo $D^k$, para cada regra k.

$$\mu_{B'i}(y) = \mathbf{max}\,[\min(D^k, \mu_{Bi}(y))],\ \forall y \in U_{yj}$$

8. Todas as regras com D[k] > 0 disparam.

9. **Consequentes**: limitados pelo coeficiente de disparo nos seus valores máximos dos conjuntos de saída.

10. Operação global de *união* compõe um conjunto fuzzy para cada variável de saída (informações de todas as regras)

$$D^k = \mathbf{min}\,[\mu_{A1k}(x_1),\ \mu_{A2k}(x_2),\ \ldots\ \mu_{Apk}(x_p)]$$

Figura 2.22 - Inferência Mandani. Adaptado de (SIMÕES; SHAW, 2007).

Depois de efetuada a inferência, o mesmo gera um número fuzzy. A conversão deste resultado em um número real é realizada em um processo denominado de defuzzificação (LEE, 1990) (IEC, 2000) (SIMÕES e SHAW, 2007).

### 2.4.3.3 Base de Regras

As bases de regras são um conjunto de condicionais e consequentes, estruturadas na forma **Se *<condicionais>* então *<consequente>.***

A vantagem da lógica fuzzy é valorizar o conhecimento do operador no processo. Esse conhecimento pode ser descrito em uma base de regras (IEC, 2000) (SIMÕES e SHAW, 2007).

Observe o exemplo a seguir de conhecimento do operador:

*"Se a temperatura está alta e aumentando,*
*então, deve-se aumentar um pouco o resfriamento".*

Traduzido para a regra:

*Se* ***temp*** *= Alta e* ***delta-temp*** *= Positivo,*
*então* ***delta-resfr*** *= PositivoPequeno.*

As variáveis ***temp***, ***delta-temp*** e ***delta-resfr*** são representadas por funções de pertinência. Por exemplo, a função ***temp*** pode ser composta de vários termos, tais como: baixa, média e alta. A subdivisão desses termos tem o objetivo de melhor classificar a transição de um conjunto para outro. Ou em outras palavras, para se definir melhor a transição de uma temperatura da condição baixa para a média e depois para alta.

As bases de regras têm o objetivo de organizar o conhecimento contido dentro da descrição dos conjuntos definidos pelas funções de pertinência (ZADEH, 1996) (IEC 61131-7, 2000).

### 2.4.3.4 Defuzzificação

O processo de defuzzificação é a transformação de um número fuzzy em um número real. Existem diversos métodos, tais como: centro de massa, também conhecido como centroide, o centro da soma, média dos máximos, entre outros (LEE, 1990) (TSOUKALAS e UHRIG, 1997).

A norma IEC 61131-7 implementa alguns métodos, são eles:

- Centro de gravidade (GOC): centro geométrico da figura que é definida por meio da Equação 2.4.

$$U = \frac{\int_{Min}^{Max} u.\mu(u)\ \partial u}{\int_{Min}^{Max} \mu(u)\ \partial u} \qquad (2.4)$$

A resposta da Equação 2.4, aplicada à figura resultante da intersecção de $\mu_{C1}$, $\mu_{C2}$, $\mu_{C3}$, e $\mu_{C4}$ pode ser visualizada na Figura 2.23.

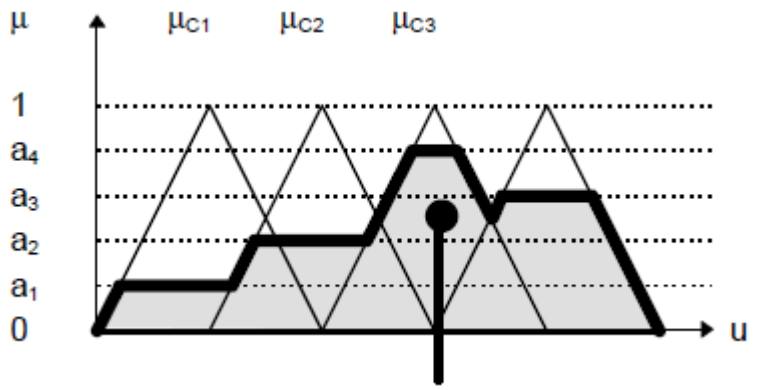



Figura 2.23 - Exemplo da saída com centro de gravidade (IEC, 2000).

### 2.4.4 IEC 61131-7

A norma IEC 61131-7 (IEC, 2000) descreve a implementação do algoritmo de controle fuzzy em controladores programáveis, definindo a linguagem de programação denominada FCL - *fuzzy control language*, que possui sintaxe similar à linguagem ST – *Structured Text.*, definida na IEC 61131-3. (IEC, 2003a).

A implementação do algoritmo é representada a seguir:

- Definição do bloco fuzzy
    - 1 - Declaração das variáveis de entrada
    - 2 - Declaração das variáveis de saída
    - 3 - Fuzzyficação
        - 3.1 - Definição de função de pertinência a partir das variáveis de entrada
            - 3.1.1 - Definição dos termos existentes de cada pertinência
            - 3.1.2 - Definição dos pontos ou curva para cada um dos termos
    - 4 - Defuzzyficação
        - 4.1 - Definição de função de pertinência a partir das variáveis de saída
            - 4.1.1 - Definição dos termos existentes de cada pertinência
            - 4.1.2 - Definição dos pontos ou curva para cada um dos termos
        - 4.2 - Definição de acumulação
        - 4.3 - Definição do método de defuzzyficação
        - 4.4 - Definição de valor mínimo ou padrão
    - 5 - Bloco de regras “Se-Então”

Na Figura 2.24 é apresentado um exemplo de código em linguagem FCL, em que se pode observar passos definidos no bloco fuzzy.

A norma IEC 61131-7 prevê que o CP também deve ser compatível com a norma IEC 61131-3 nos seguintes pontos:

- Tipos de dados (INT, WORD, REAL, etc.).
- Integração com as demais linguagens de programação da IEC 61131-3.

```
FUNCTION_BLOCK Fuzzy_FB
        VAR_INPUT
                temp : REAL;
                pressure : REAL;
        END_VAR

        VAR_OUTPUT
                valve : REAL;
        END_VAR

        FUZZIFY temp
                TERM cold := (3, 1) (27, 0);
                TERM hot := (3, 0 (27, 1);
        END_FUZZIFY

        FUZZIFY pressure
                TERM low := (55, 1) (95, 0);
                TERM high:= (55, 0) (95, 1);
        END_FUZZIFY
```

Figura 2.24 - Exemplo de código FCL (IEC, 2000).

# 3. SISTEMÁTICA PROPOSTA

Para a implementação da sistemática proposta tem-se como pré-requisito fundamental a participação de uma equipe técnica multidisciplinar de especialistas na planta ou processo. O conhecimento consolidado por esta equipe deve ser resultado de atividades envolvendo a coleta de dados obtidos por meio de experimentos de campo, dados de registros históricos das equipes de manutenção, dados de instalações similares – *benchmarking* - e dados de simulação computacional da planta em estudo.

De acordo com os requisitos das normas IEC 61508/61511, a arquitetura de controle para implementar a camada SIS de mitigação proposta é representada na Figura 3.1.

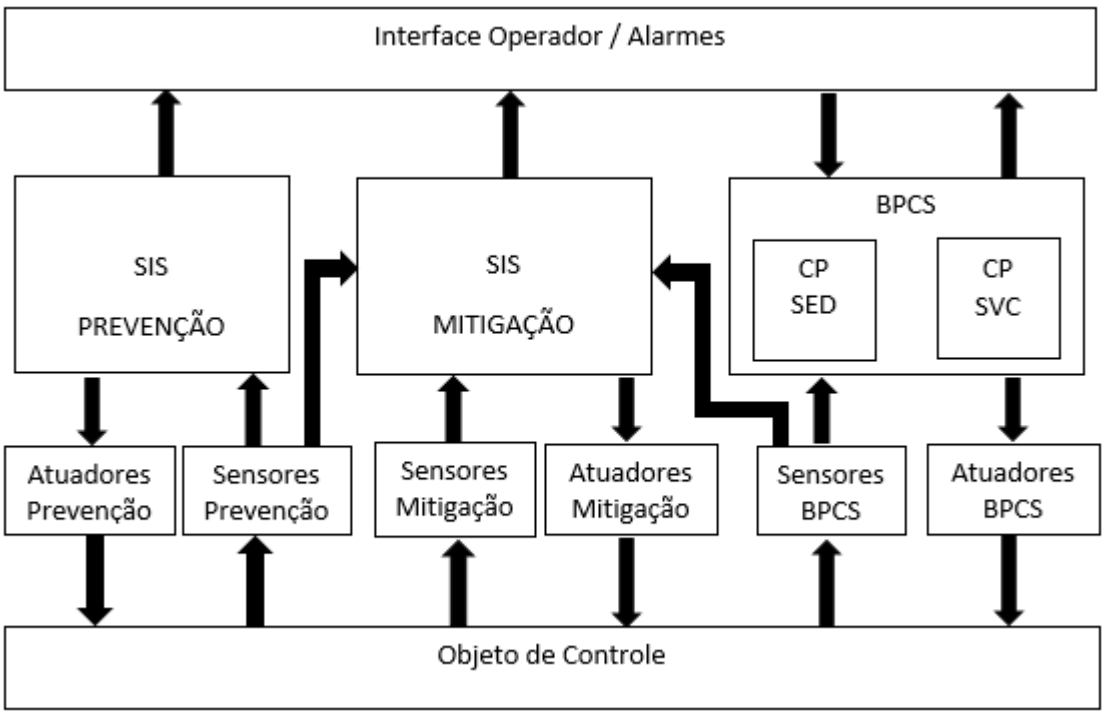



Figura 3.1 - Arquitetura SIS para implemetação da sistemática proposta.

.

Conforme pode ser observado, os sensores e atuadores da camada SIS de mitigação são independentes das camadas BPCS e SIS de prevenção podendo-se,

para o caso de sensores, utilizarmos duplicadores de sinal, conforme referência da norma.

A estrutura básica do sistema de controle para a camada SIS de mitigação é representada na Figura 3.2.

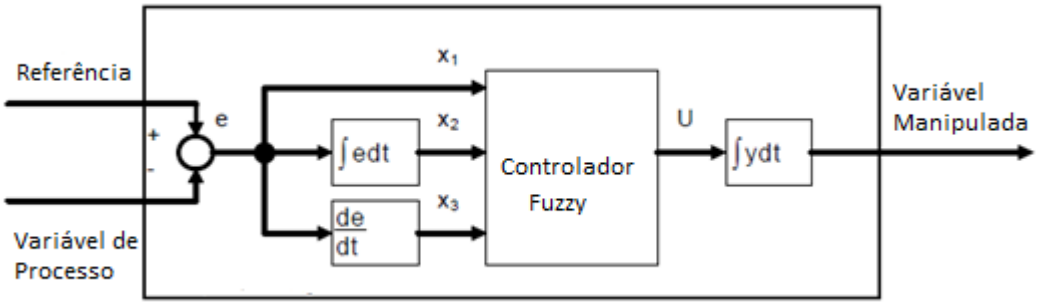



Figura 3.2 - Dispositivo de realização de controle fuzzy (IEC, 2000).

O controlador fuzzy é um tipo de controle recomendado para problemas não lineares, ou em que o comportamento dinâmico não é bem compreendido (IEC, 2000) (SIMÕES e SHAW, 2007) (POPA, 2008). Baseado na lógica fuzzy, pode ser utilizado para o controle de processos. Dependendo do tipo do fenômeno que se deseja controlar, um controle tradicional pode ser bem mais complexo para ser ajustado (IEC, 2000) (SIMÕES e SHAW, 2007).

Como pode-se observar na Figura 3.2, o controle fuzzy utiliza, para cada variável de entrada do processo, três componentes, que são o seu valor absoluto, a integral da variável e a derivada temporal desta variável, que podem ser representadas no mesmo conjunto de pertinências. A representação gráfica das funções de pertinência pode ser apresentada de forma adimensional, demonstrando o valor mínimo e máximo de fundo de escala na faixa de -1 à +1. De acordo com Popa (2008) e Lee (1990), a variável associada ao gradiente temporal da variável associada à ocorrência de uma falha crítica possui a função de pertinência, representado na Figura 3.3.

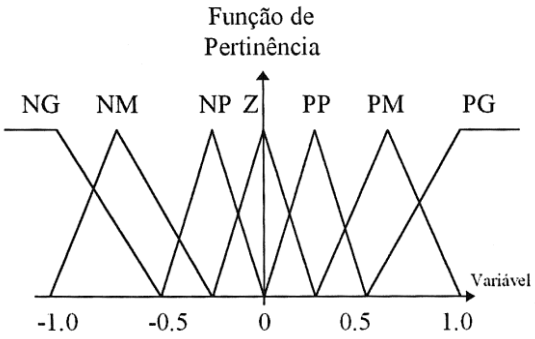



Figura 3.3 - Função de pertinência da variável “erro” (POPA, 2008).

Os termos da função de pertinência associada ao gradiente são: Zero (Z), Positivo Pequeno (PP), Positivo Médio (PM) e Positivo Grande (PG). As siglas NG, NM e Np referem-se aos gradientes Negativo Grande, Negativo Médio e Negativo Pequeno, respectivamente.

A componente da derivada temporal pode ser interpretada como uma medida da tendência do parâmetro da variável de entrada, que na sistemática aqui proposta indica o comportamento temporal da falha, ou seja, indica se uma variável de monitoração, associada a um estado de falha, possui comportamento crescente no tempo. Isto pode ser interpretado como um estado de falha que necessita ser mitigado. De acordo com os resultados das técnicas de análises de riscos, os efeitos da ocorrência de falhas críticas podem levar a um estado de catástrofe.

Um gradiente positivo de uma variável associada a uma falha crítica pode ser um indicativo de um estado de falha que pode evoluir para a catástrofe, caso não seja mitigado. A análise, portanto, tanto do valor absoluto da variável quanto de seu gradiente podem contribuir para uma ação antecipativa à ocorrência de catástrofes, contribuindo para uma maior eficácia da camada SIS de mitigação.

Definidos os sinais de entrada para o controlador fuzzy tem-se, na Figura 3.4, a estrutura básica do Dispositivo de Realização de Controle fuzzy considerado.

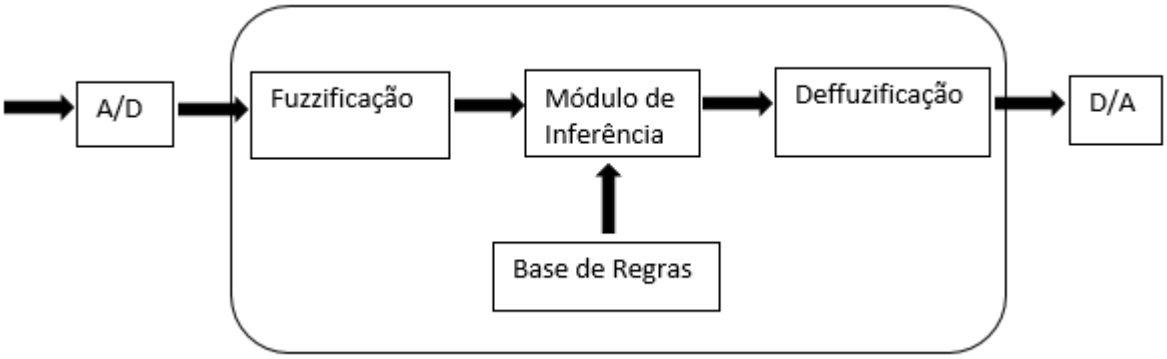



Figura 3.4 - Controlador fuzzy básico (Adaptado da (IEC, 2000).

A partir dos resultados da aplicação das técnicas de análise de riscos pode-se determinar os intervalos para o processo de fuzzificação das variáveis de entrada e também para determinação da base de regras do controlador fuzzy, com ênfase à técnica *What-If*. A Figura 3.5 ilustra o encadeamento lógico desta técnica com a lógica fuzzy:

*O QUE...SE....(What-If)*

*SE....ENTÃO (condicional...consequente)*

Figura 3.5 – Relação da técnica *What-If* com a base de regras fuzzy.

Definindo-se o tipo de controlador utilizado, o “ciclo de vida” para o projeto e desenvolvimento de sistemas de automação (MIYAGI, 1996), a sequência de passos para a implementação da sistemática é apresentada na Figura 3.6:

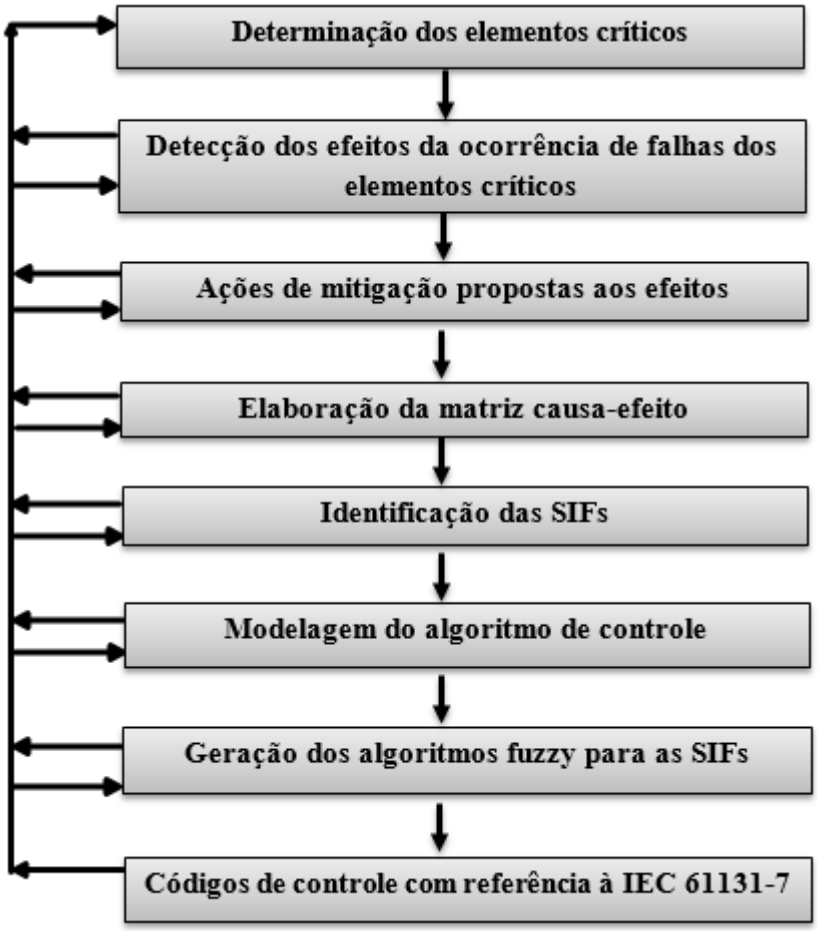



Figura 3.6 – Ciclo de vida do projeto e desenvolvimento da sistemática proposta. Adaptado de Miyagi (1996)

O passo inicial consiste na determinação dos elementos críticos do SP, ou seja, os elementos que em estado de falha podem gerar consequências (efeitos) que podem levar à ocorrência de catástrofes. Para tanto, é feita a aplicação de técnicas de análises de riscos.

Com os resultados obtidos, inicia-se a determinação de sensores que possam diagnosticar a ocorrência de falhas nos elementos críticos, por meio de monitoração de componentes, para o caso de falhas aleatórias, ou para a monitoração de desvios de processo, para o caso de falhas catastróficas.

Ainda de acordo com a equipe de especialistas, obtêm-se a determinação das ações de mitigação necessárias, desempenhadas por atuadores específicos, com o objetivo de se evitar o cenário de catástrofe.

Uma matriz causa-efeito é então elaborada, na qual os eventos inicializadores da ação de mitigação representam os sinais dos sensores, aqui representados nas linhas da matriz, correspondentes às causas, e, nas colunas da matriz, os efeitos, que são as ações de mitigação desempenhadas por meio de atuadores específicos. Da matriz causa-efeito, pode-se determinar as funções instrumentadas de segurança – SIFs, a partir dos eventos inicializadores, associando-se, para cada SIF, um nível de integridade de segurança – SIL, que por sua vez pode ser associado a uma determinada probabilidade de falha sob demanda – PFD.

As seções 3.1 a 3.7 apresentam de forma detalhada cada uma destas atividades.

## 3.1 Determinação dos elementos críticos

Para determinar os elementos críticos do processo em estudo, utiliza-se as técnicas de análise de riscos com ênfase no FTA, FMEA e *What-If*, a partir dos resultados apresentados por uma equipe especialista no processo.

O FMEA, por associar um nível de severidade para a(s) consequência(s) da ocorrência da falha do componente, nos dá uma medida de quais são os componentes críticos do processo, ou seja, aqueles em que é atribuído nível de severidade máximo, e as formas de se monitorar seus possíveis modos de falha.

Porém pelo fato de estar focado em um único componente, a aplicação desta técnica não é capaz de fornecer uma relação lógica ou o sequenciamento de falhas de demais componentes, ou ainda erros humanos de processo que possam explicar o porquê de uma determinada falha, que não está relacionada à ocorrência dos modos de falhas de um único componente, elaborado no estudo do FMEA.

Desta forma, é necessária a aplicação de outras técnicas de análise de riscos, tais como o FTA e o Hazop, além da técnica *What-If*.

A técnica *What-If* é particularmente importante pois apresenta os resultados de uma análise prática e direta dos resultados dos estudos da equipe de especialistas, principalmente para se determinar os valores, absolutos ou percentuais, das variáveis de monitoração dos componentes ou de processo para a determinação da amplitude da falha e quais as ações sugeridas para mitigar os efeitos da ocorrência das falhas.

O comportamento dinâmico de um processo sob estado de falha é pouco conhecido, devido à própria criticidade do processo em estudo, pois jamais é levado a um estado de falha para se determinar seu comportamento dinâmico, ficando restrito a simulações computacionais ou ações de mitigação propostas por especialistas no processo.

## 3.2 Detecção dos efeitos da ocorrência de falhas dos elementos críticos

Após a determinação dos elementos críticos do processo em estudo, deve-se realizar um estudo para a determinação de dispositivos capazes de detectar a ocorrência dos possíveis modos de falha associados no estudo do FMEA, ou ainda capazes de detectar a ocorrência de falhas latentes e/ou catastróficas, cujos efeitos resultam em alterações em variáveis de processo que a camada de controle básico BPCS não é capaz de regenerar.

A sistemática considera um sistema de controle para a mitigação, utilizando controladores programáveis - CPs – e assim os dispositivos capazes de detectar a ocorrência de falhas e seus efeitos são sensores, associados aos sinais de entrada do controlador.

Para evitar-se a ocorrência de falsos alarmes, que podem ser gerados no caso de regimes transitórios do sistema, ou ainda a ruídos de medição, fenômeno comum associado a sensores, algumas estratégias devem ser adotadas para se evitar o que é denominado de falhas espúrias (IEC 61508, parte IV (IEC, 2010)). Dentre tais estratégias, existem filtros temporizados (SQUILLANTE JR, 2011), e critérios de votação para a confirmação do sinal. Dentre os critérios mais utilizados pode-se citar o critério 2oo3 (lê-se 2 de 3), em que o sinal é confirmado pelo resultado lógico de pelo menos 2 sensores. Para o escopo deste trabalho, uma falha é confirmada quando 2 de três sensores indicarem que um determinado limiar foi ultrapassado. O diagrama lógico da votação é representado na Figura 3.7:

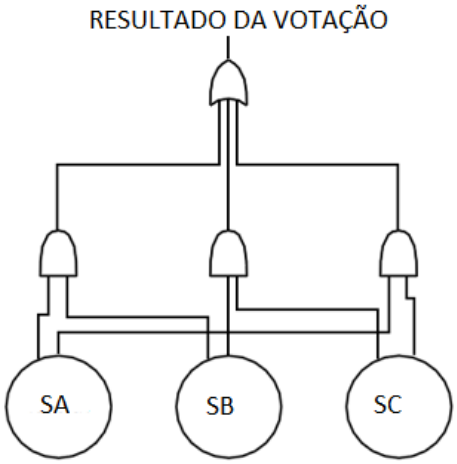



Figura 3.7 – Lógica 2oo3 para sensores. Fonte: Ferrarezi (2014)

De acordo com as normas IEC 61508 / IEC 61511, os sensores do SIS devem ser independentes da camada BPCS, e, caso algum sensor seja comum tanto para a camada SIS de prevenção quanto para a camada SIS de mitigação, deve ser utilizado um repetidor de sinal para tais casos.

## 3.3 Ações de mitigação propostas

Para cada efeito de falha de um componente crítico, detectada pelos sensores da camada SIS de mitigação, uma ou mais ações ou atividades de mitigação devem ser implementadas por dispositivos específicos, associados aos sinais de saída do controlador, ou atuadores de mitigação.

Para a determinação das ações de mitigação, utiliza-se os resultados das técnicas de análise de riscos, particularmente os resultados da técnica What-If.

Para que a ação de mitigação seja desempenhada, é realizado um estudo sobre qual(is) atuadores é (são) necessário(s) para contemplar a ação de mitigação proposta pela análise de risco. Um ou mais atuadores podem ser necessários, realizando atividades que podem ser simultâneas e/ou sequenciais.

Não é considerado, neste trabalho, o sequenciamento de falhas e o sequenciamento de ações de mitigação. Para cada efeito de ocorrência de falha, detectado por sensores da camada SIS de mitigação, um ou mais atuadores são

requisitados de forma simultânea para mitigar o efeito da ocorrência da falha. Ações de mitigação podem ser comuns para diferentes eventos inicializadores, isto é, para diferentes sensores.

## 3.4 Elaboração da matriz causa-efeito

Para a aplicação da sistemática, elabora-se uma matriz causa-efeito, em que os sensores, ao detectarem o efeito da ocorrência de falha, representam o evento inicializador da mitigação, portanto representando a causa da matriz, alocados nas linhas da matriz.

Já nas colunas tem-se os efeitos, representados pelo acionamento dos atuadores responsáveis por mitigar os efeitos da ocorrência das falhas.

Pelo fato de muitos atuadores serem comuns para diferentes eventos inicializadores, a matriz é usada na elaboração dos algoritmos de controle, como é observado nas seções seguintes.

Um exemplo de matriz causa-efeito é representado na Tabela 3.1.

Tabela 3.1 – Exemplo de matriz causa-efeito.

| CAUSAS (sensores) | EFEITOS (atuadores) | | | |
|---|---|---|---|---|
| | ALARME MIT | ATUADOR A | ATUADOR B | ATUADOR C |
| Sensor A | X | X | | |
| Sensor B | X | | X | X |

## 3.5 Identificação das SIFs

A partir da matriz causa-efeito e dos resultados das técnicas de análise de riscos, as funções instrumentadas de segurança - SIFs - do processo são identificadas, associando-se, para cada SIF, um nível de integridade de segurança – SIL, e uma probabilidade de falha sob demanda – PFD (SQUILLANTE JR, 2011).

De forma geral, a camada SIS de mitigação é ativada quando a camada SIS de prevenção falha ou não se mostra eficaz para degenerar o sistema a um estado seguro. Por tratar-se de um sistema de controle, composta por sensores e atuadores de prevenção e um algoritmo de controle implementado por controlador programável, a camada SIS de prevenção também possui uma PFD associada não sendo, portanto, imune à ocorrência de falhas e à erros de projeto.

A falha da camada SIS de prevenção, ou sua ineficiência diante do cenário de falha, pode ser entendida como um aumento acima de um limiar permissível para a camada de prevenção. Em outras palavras, pode-se inferir que a camada de prevenção não está sendo suficiente para levar o processo a um estado seguro. Um possível cenário de catástrofe pode ocorrer, caso uma camada adicional de proteção não seja acionada.

A determinação da faixa de parâmetros a partir dos quais a camada de mitigação deve ser acionada também é determinada pelos resultados de análises de riscos, com ênfase à técnica *What-If.*

## 3.6 Modelagem do algoritmo de controle

O passo seguinte da sistemática é a geração do algoritmo de controle da camada SIS de mitigação, responsável por integrar as SIFs, seus eventos inicializadores - sensores, considerando a lógica de detecção para cada SIF, os atuadores que, conforme já comentado, podem ser comuns para diferentes SIFs, a correspondência com os modelos de prevenção (SQUILLANTE JR, 2011) e os limiares para cada variável.

Como ferramenta para esta etapa, utiliza-se a Rede de Petri - RdP. No contexto deste trabalho, pode-se considerar a ocorrência de falha como um evento discreto, na medida em que se pode associar o estado “0” como estado normal e “1” como estado de falha, a partir do limiar de uma determinada variável de processo.

Como vantagens na utilização da RdP, estão a facilidade na análise do algoritmo de controle via simulação dos modelos e na verificação formal de determinadas propriedades, tais como vivacidade (ou ausência de *deadlocks),* reiniciabilidade ou reversibilidade, e limitabilidade ou segurança.

A constatação (verificação) destas propriedades resulta em uma validação formal do modelo gerado, resultando em um algoritmo de controle adequado para desempenhar a dinâmica imposta ao sistema. A geração e a verificação das propriedades podem ser feitas por auxílio de ferramentas computacionais, tais como os softwares HPSIM (ANSCHUETZ) e PIPE2 (AKHARWARE, 2005).

Inicialmente, tem-se a construção dos modelos em RdP para cada SIF, considerando a lógica de detecção dos sensores de cada SIF, a correlação com os limiares de prevenção e o acionamento dos atuadores específicos para cada SIF.

Como já comentado, este trabalho não aborda o sequenciamento dos atuadores; caso uma falha seja diagnosticada e a camada de prevenção não seja capaz de degenerar o sistema a um estado seguro, todos os atuadores de mitigação são acionados, permanecendo neste estado até que todos os sensores responsáveis pela inicialização da respectiva atividade de mitigação retornem a patamares normais de operação. Esta condição desabilita os atuadores, porém não habilita o processo para o seu reinício de operação. De acordo com as normas IEC 61508 / IEC 61511, após a ação das camadas SIS de prevenção / mitigação, o processo em questão deve seguir uma minuciosa inspeção com o objetivo de se verificar os possíveis agentes causadores da falha e as devidas correções. Na sistemática proposta, esta lógica é representada nos modelos em RdP de cada SIF / camada de gás e fogo.

Devido ao fato de um elevado número de atuadores comuns às SIFs, fato decorrente dos resultados da elaboração da matriz causa-efeito, há a necessidade do refinamento dos modelos gerados em RdP, procedimento análogo é realizado para a camada de gás e fogo pois, como já mencionado, a camada de gás e fogo pode ser entendida como uma falha da camada de mitigação e, via de regra, além dos

atuadores específicos para gás e fogo, ocorre uma redundância no acionamento dos atuadores da mitigação, devido à independência dos controladores.

O refinamento sucessivo dos modelos resultará em um modelo geral, que contempla todas as SIFs e a camada de gás e fogo, com os respectivos sensores e atuadores, e as lógicas de verificação dos sensores para o término da mitigação e reabilitação do sistema.

## 3.7 Geração dos algoritmos fuzzy para as SIFs

Após a validação e refinamento dos modelos em RdP, o próximo passo consiste na geração das funções de pertinência fuzzy para cada SIF, considerando os resultados obtidos da equipe de especialistas para a construção da matriz causa-efeito. Isto porque os resultados daquele estudo formam a base de regras fuzzy e os intervalos dos limiares das variáveis de monitoração de componentes ou variáveis de processo que indicam os possíveis estados de falha.

De forma adicional, para a construção das funções de pertinência fuzzy considera-se gradiente ou variação temporal da variável relacionada ao evento inicializador, ou seja, sob determinadas condições, a tendência temporal do parâmetro relacionado à falha pode, em determinadas condições, estar em um limiar acima do BPCS, e portanto em um intervalo correspondente à camada SIS de prevenção, porém apresentar um comportamento temporal de incremento anormal da variável. Isto pode ser traduzido em uma não suficiência da camada de prevenção em degenerar o sistema, e portanto a camada SIS de mitigação deve atuar com o objetivo de se evitar a ocorrência do evento catastrófico.

A utilização da lógica fuzzy contempla este cenário, uma vez que se pode inserir, no conjunto de regras fuzzy, o valor absoluto e a derivada temporal da variável para a formação das funções de pertinência fuzzy. Como resultado prático, tem-se uma tradução do conhecimento humano em um algoritmo de controle que atua de forma antecipativa, resultando em uma maior eficácia do sistema, sem o uso de equações diferenciais e de outras técnicas tradicionais para se extrair o modelo matemático da planta em estudo.

Como ferramenta para a implementação das funções de pertinência fuzzy pode-se utilizar a ferramenta computacional *toolbox* fuzzy do software *Matlab*®, no qual pode-se inserir, para cada SIF, os eventos inicializadores (ou sensores), considerando o critério de votação adotado, e os patamares de valores para cada camada: BPCS ou operação normal, o da camada SIS de prevenção e o da camada SIS de mitigação.

A Figura 3.8 apresenta o ambiente do software para a geração dos algoritmos fuzzy de controle, alocando os sensores aos sinais de entrada do controlador, o controlador fuzzy, o método de inferência utilizado (Mandani ou Sugeno), e o respectivo sinal de saída, em que são alocados os atuadores de mitigação.

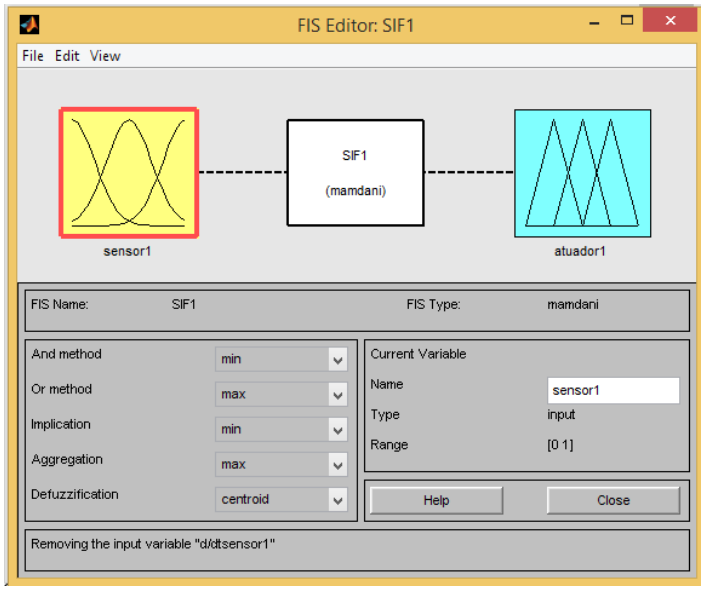



Figura 3.8 – Toolbox fuzzy MatLab®.

Para cada variável do sistema, pode-se determinar regiões de operação, em função do conhecimento humano a respeito do sistema em análise. A Figura 3.9 exemplifica as regiões de operação para os intervalos de uma variável de entrada:

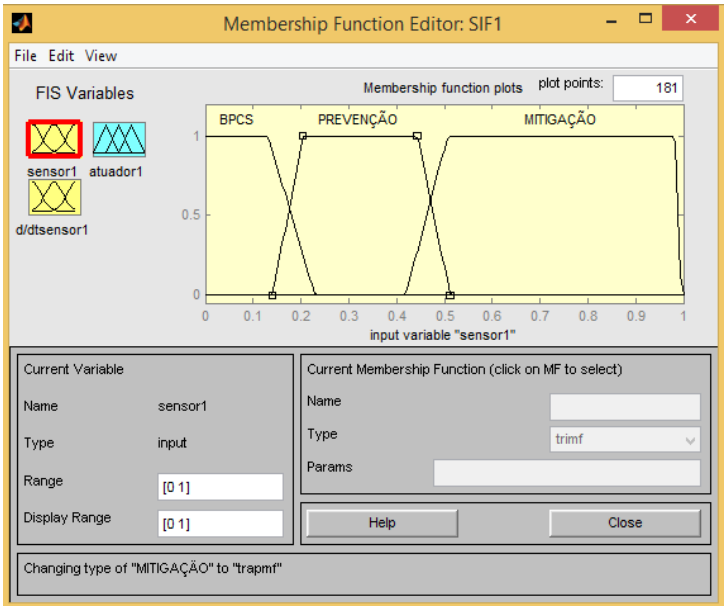



Figura 3.9 – Exemplo de regiões de operação para uma variável de entrada.

Já a Figura 3.10 faz a representação para o sinal do gradiente da variável referente ao sensor 1, na qual pode-se notar três funções: a de gradiente negativo, indicando um decréscimo da intensidade da variável, a de gradiente nulo, e a de gradiente positivo, indicando um incremento na intensidade do parâmetro.

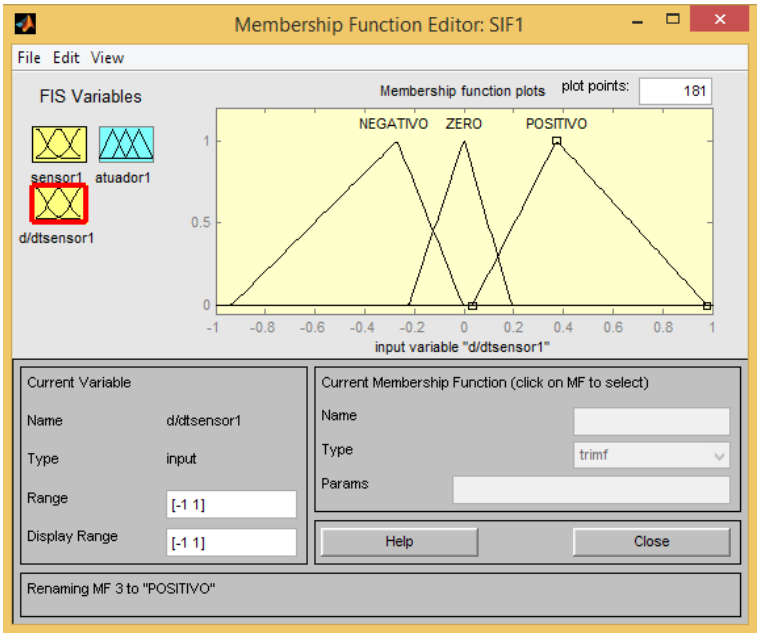



Figura 3.10 – Regiões de operação para a evolução temporal da variável.

Tais informações podem ser utilizadas no modelo para acionar uma possível ação antecipativa quanto à mitigação, pois se a variável que representa o estado de falha estiver na região de prevenção, porém com uma intensidade crescente anormal em seu parâmetro, representado por seu gradiente positivo, pode-se concluir que a camada de prevenção não está sendo capaz de degenerar o sistema a um estado seguro, logo, com o objetivo de se evitar a ocorrência de catástrofe, a camada de mitigação deve ser ativada.

O passo seguinte é a determinação do conjunto de regras fuzzy, no qual são transcritos o conhecimento humano de especialistas, obtidos pelos resultados das técnicas de análise de riscos. A Figura 3.11 ilustra a edição da base de regras no *toolbox.*

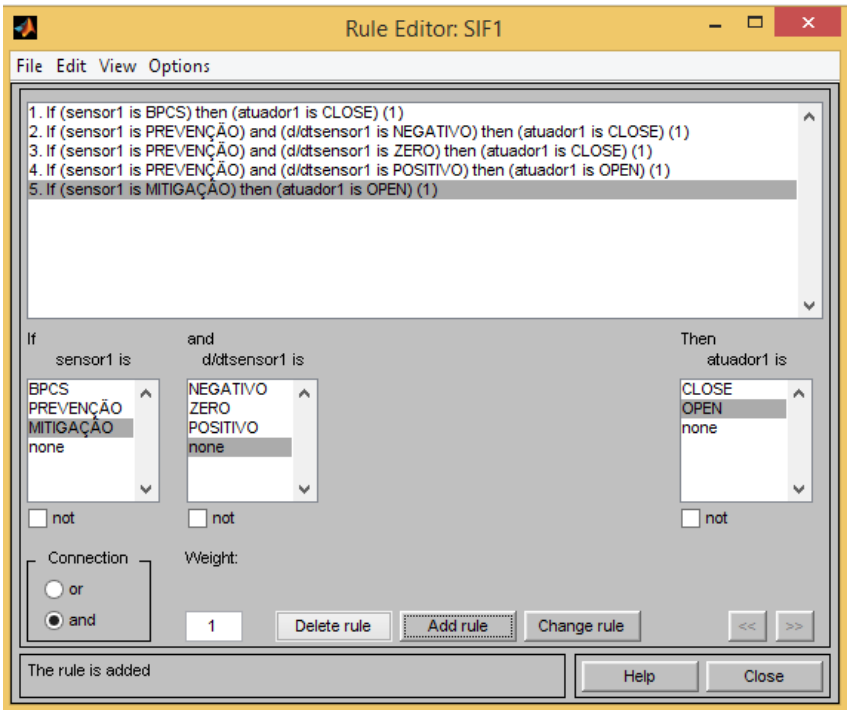



Figura 3.11 – Conjunto de regras fuzzy, extraídas do conhecimento humano.

No exemplo, tem-se um conjunto de regras em paralelo, relacionadas à ação do atuador de mitigação, supondo que o atuador na posição “close” significa operação normal do sistema e, para a posição “open” a operação da camada SIS de mitigação.

A Figura 3.12 apresenta o modelo do atuador para as condições descritas:

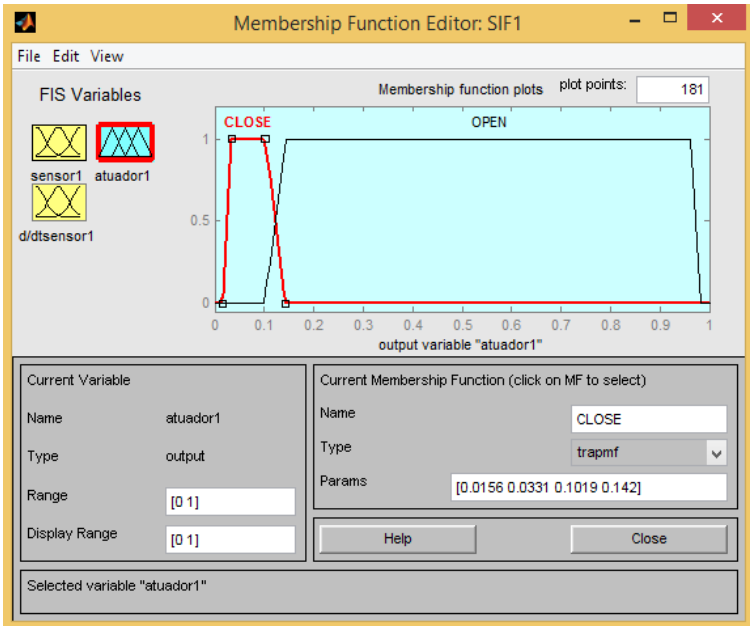



Figura 3.12 – Modelo do atuador no *toolbox.*

Desta forma, pode-se implementar todas as SIFs elencadas a partir dos modelos validados em RdP, por meio da adição de todos os sensores que indicam os eventos inicializadores, levando-se em conta o comportamento temporal da variável, a lógica de atuação (2oo3 ou lógica *or*) e os patamares estabelecidos pela equipe de especialistas, e a correlação de cada SIF com os respectivos atuadores de mitigação. A vantagem é que o refinamento sucessivo dos modelos gerados em RdP, devido ao grande número de atuadores comuns às atividades de mitigação agora são detalhados de forma com que sua implementação seja simplificada.

A edição do intervalo dos parâmetros ou a adição de sensores e atuadores no controlador pode ser feita diretamente de forma gráfica, simplificando a edição das SIFs.

Outra vantagem é a possibilidade da simulação do controlador, por meio da função de exportação e simulação no ambiente Simulink®, por meio do uso de uma placa de comunicação A/D / D/A, pode-se obter os resultados de simulação de uma planta real em estado de falha e a eficácia da camada SIS de mitigação proposta. Esta etapa de simulação não faz parte do escopo deste trabalho.

## 3.8 Códigos de controle com referência à IEC 61131-7

Após a conversão dos modelos em RdP para uma especificação viável de ser implementada em controladores fuzzy, que considera, além do valor absoluto da variável, o respectivo gradiente temporal, deve-se converter o algoritmo fuzzy em uma linguagem que possa ser implementada em controladores programáveis.

A norma IEC 61131-3 (IEC, 2003a), que trata das linguagens de programação de controladores, apresenta, dentre outras, a *ST* ou *Structured Text*, relacionada com a lógica fuzzy a partir da FCL - *fuzzy control language*, descrita na IEC 61131-7. O próximo passo da sistemática é, portanto, converter os algoritmos fuzzy gerados para a camada de mitigação, contemplando todas as SIFs para os códigos de controle para os respectivos controladores.

# 4. EXEMPLO DE APLICAÇÃO

Com o objetivo de exemplificar a aplicação da sistemática proposta, apresenta-se aqui um processo produtivo de uma estação de compressão de gás – *Ecomp*, que realiza a extração do gás natural de reservas naturais, cuja composição é uma mistura de hidrocarbonetos altamente inflamáveis, além da presença de impurezas. A Figura 4.1 apresenta a instalação do processo produtivo em estudo.

Figura 4.1 – Vista da Estação de Compressão de Gás. Fonte: http://www.bonatti.it/Projects/Mellitah-Gas-Compression-Station. Acesso: 23/11/2014

A estação de gás natural possui uma ou mais linhas de sucção do gás natural, que devem passar por um processo de filtragem antes de ser comprimido. A elevação da pressão é necessária devida à distância geográfica da reserva aos centros consumidores. O gás, sob alta pressão, é transportado por meio de gasodutos, a exemplo do gasoduto Brasil – Bolívia.

Outro fato relacionado à distância geográfica está na disponibilidade de energia elétrica para a operação da Ecomp. Desta forma, uma parte deste gás é utilizada como combustível para o funcionamento da própria unidade compressora, além de alimentar geradores de energia elétrica para o consumo de energia elétrica da estação. A unidade compressora deve controlar a pressão e a temperatura para a utilização na estação de compressão, além do gás combustível para a unidade turbo compressora, aquecedores a gás e geração de energia para a planta.

A unidade compressora deve operar sob determinados limites de pressão e temperatura, liberando o gás natural pressurizado em linhas de descarga para o gasoduto.

## 4.1 Aplicação da Sistemática Proposta – Caso de Uso 1

A próxima seção apresenta a aplicação da sistemática proposta para o caso de um evento inicializador (causa), relacionado a um possível modo de falha de um componente crítico da Ecomp, com o acionamento de atuadores de mitigação. Tal procedimento foi adotado para facilitar a interpretação dos resultados para verificar a exequibilidade da sistemática proposta. Na sequência, na seção 4.2 apresenta-se a aplicação da sistemática para todo o processo produtivo em análise.

### 4.1.1 Determinação dos Elementos Críticos

De acordo com os passos definidos na sistemática proposta, deve-se aplicar as técnicas de análise de riscos para o processo produtivo, a fim de se identificar os elementos críticos, seus possíveis modos de falha e os efeitos da ocorrência das falhas. Aplicando a técnica FMEA aos componentes da estação de compressão, verifica-se que os compressores são elementos críticos do sistema, pois operam sob alta temperatura, pressão e rotação, com fluido de trabalho altamente inflamável. A Figura 4.2 ilustra o P&ID de uma das quatro unidades compressoras do processo produtivo em análise.

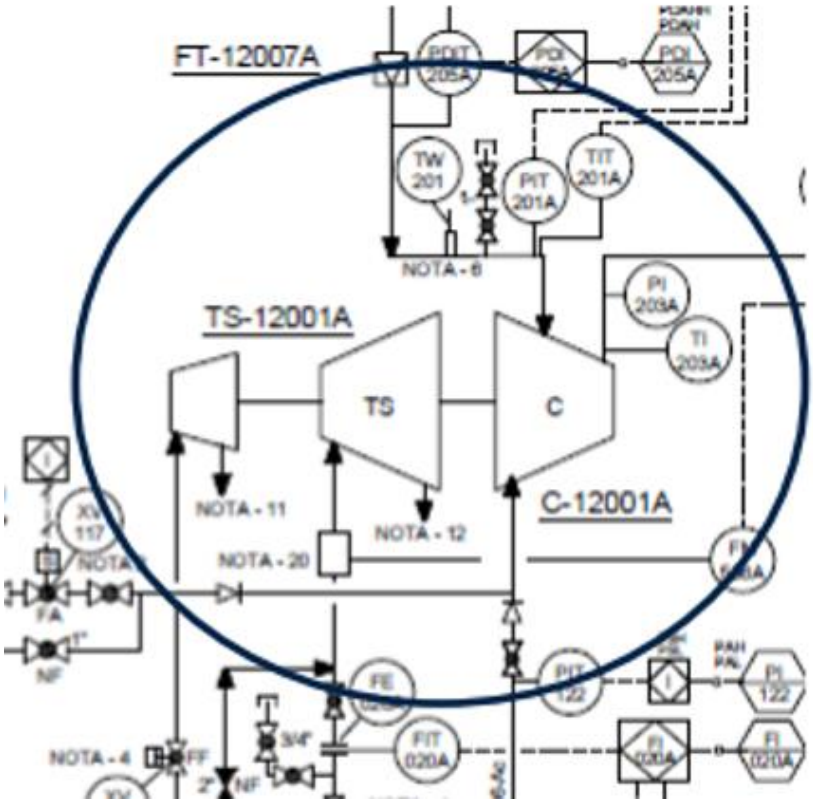



Figura 4.2 – P&ID de uma das unidades compressoras.

Uma falha em um destes equipamentos certamente colocaria os operadores da estação sob um risco inaceitável, além claro do risco para o ambiente em que se insere e o da própria instalação, o que violaria normas legais.

Aos compressores portanto atribui-se máxima severidade, e certamente devem fazer parte da camada SIS de mitigação. A Tabela 4.1 ilustra um FMEA para o modo de falha de lubrificação do equipamento em análise, com dados obtidos por uma equipe de especialistas.

Tabela 4.1 - FMEA- falha de lubrificação do eixo do mancal do compressor

| Comp | Potencial Modo de Falha | | Potencial Efeito | Potencial Causa | Detecção | Ações Recomendadas | Severidade |
|---|---|---|---|---|---|---|---|
| Turbo Compress | Lubrificação | | Alta na temperatura óleo lubr do mancal | Óleo Saturado | TIT211x | Shut-Down (Prevenir)<br>Dióxido de Carb (Mitigar) | 10 |
| | Dano | Bomba Óleo<br>Eixo CP | | Desgaste do Mancal Hardware / Sotware | | | |
| | Overload velocidade | | | Controle de Velocidade | | | |
| | Overload Torque | | | Excesso de condensado | | | |

Devido às limitações da técnica FMEA, para a compreensão de como e o porquê da ocorrência deste modo de falha no compressor, o FTA qualitativo, concebido por meio do manual técnico do fabricante, histórico de falhas do equipamento, pesquisas de *benchmarking*, e conhecimento técnico de um especialista, pode apresentar a estrutura representada na Figura 4.3.

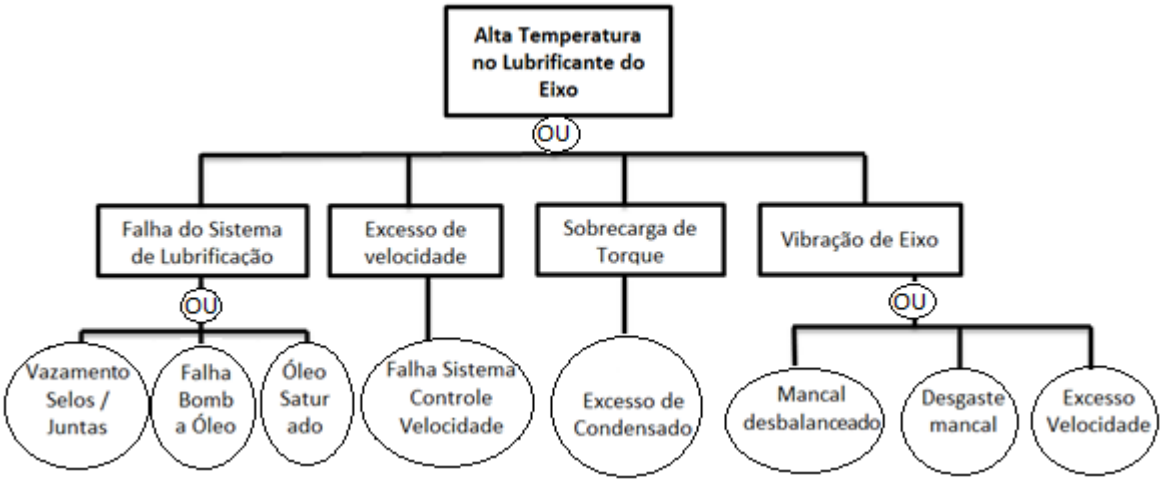



Figura 4.3 - FTA para “Alta temperatura do óleo lubrificante do mancal de eixo”.

Tanto o FMEA quanto o FTA indicam que o efeito do modo de falha “lubrificação do eixo do mancal” tem como efeito o aumento da temperatura do fluido (óleo lubrificante) do eixo da turbina, podendo também aumentar a temperatura do fluido de trabalho (gás) na linha de descarga, assim como um menor rendimento da compressão, resultando portanto em uma menor pressão na linha.

Realiza-se assim o estudo da camada SIS de mitigação em função da monitoração do parâmetro de temperatura para este componente. Outros parâmetros também podem ser monitorados, a exemplo da pressão na linha de descarga, associados ao mesmo ou a outros modos de falha.

### 4.1.2 Detecção dos efeitos da ocorrência de falhas dos elementos críticos

Considerando os efeitos das falhas apresentadas na etapa anterior, a sistemática proposta indica a necessidade de instalação de sensores de temperatura associados à temperatura do lubrificante do eixo do mancal do compressor, de forma independente dos sensores associados ao BPCS. Seguindo os padrões de identificação da norma ISA S5.1 (ANSI/ISA S5.1, 1992), o código para este sensor é o TAG TET 211 – Temperatura do Eixo da Turbina, com a designação de letras para cada unidade compressora da estação. Desta forma, tem-se os *tags* TET 211-A para o compressor A, TET 211-B para o B e assim sucessivamente até a unidade D.

Tais sensores são os responsáveis por enviar o sinal de temperatura do lubrificante do eixo do mancal das turbinas ao CP SIS de mitigação. Adota-se uma estrutura redundante para estes sensores, bem como a aplicação de algoritmos de controle para detectar e eliminar falhas espúrias.

### 4.1.3 Ações de Mitigação propostas

Para mitigar os efeitos causados pela ocorrência do(s) modo(s) de falha(s) da unidade compressora, que resultaram no evento topo de alta temperatura do óleo lubrificante do mancal, a ação sugerida, de acordo com os resultados da aplicação das técnicas de análise de riscos, são a ação de *shutdown* alocada para a camada SIS de prevenção e uma ação redundante de *shutdown* para a camada SIS de mitigação, além da refrigeração forçada dos compressores, caso a camada de prevenção não seja suficiente para degenerar o sistema a um estado seguro. A refrigeração pode ser feita por meio da abertura de válvulas de cilindros de gás carbônico já presentes na instalação, conforme o P&ID, representado na Figura 4.4. A liberação do gás carbônico, refrigera o compressor e reduz a presença de oxigênio a seu redor, reduzindo a possibilidade de combustão ou explosão.

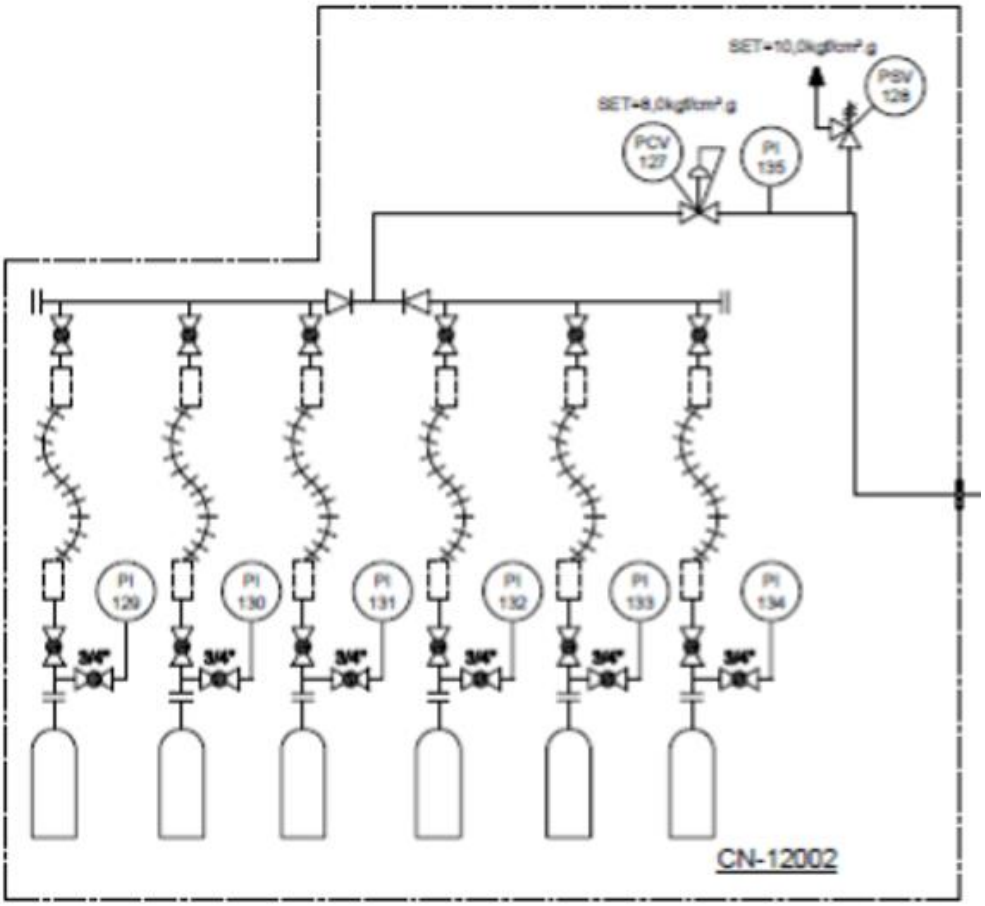



Figura 4.4 - P&ID cilindros de dióxido de carbono na *Ecomp*.

### 4.1.4 Elaboração da matriz causa-efeito

A partir dos resultados obtidos das técnicas de análise de riscos, em que são identificados os eventos inicializadores para a ocorrência de falha no componente crítico do sistema, e as ações para a mitigação de seus efeitos, elabora-se a matriz causa-efeito, em que os eventos inicializadores, representados nas linhas da matriz, indicam os sinais dos sensores, e os efeitos, representados nas colunas da matriz, representam as ações dos atuadores de mitigação. Tal matriz é resultado dos estudos da equipe de especialistas no processo em análise, a partir da aplicação das técnicas de análise de riscos. Para o presente exemplo de aplicação, a matriz causa-efeito, é representada na Tabela 4.2.

Tabela 4.2 – Matriz causa-efeito

| EFEITOS (atuadores) | PARADA EM TCA | PARADA EM TCB | PARADA EM TCC | PARADA EM TCD | ABERTURA GASCARB A | ABERTURA GASCARB B | ABERTURA GASCARB C | ABERTURA GASCARB D |
|---|---|---|---|---|---|---|---|---|
| CAUSAS (sensores) | | | | | | | | |
| TET-211A | X | | | | X | | | |
| TET-211B | | X | | | | X | | |
| TET-211C | | | X | | | | X | |
| TET-211D | | | | X | | | | X |

Uma abordagem mais conservadora considera, para o exemplo, todas as ações de mitigação simultâneas para o caso de sinais de estado crítico em qualquer um dos sensores.

### 4.1.5 Identificação das SIFs

A matriz causa-efeito resultante permite a identificação das correspondentes SIFs, com o respectivo nível de severidade SIL associado, assim como a probabilidade de falha sob demanda – PFD. A SIF1 resultante é representada na Tabela 4.3.

Tabela 4.3 – SIF 1 – derivada da matriz causa-efeito na Tabela 4.2

| | |
|---|---|
| SIF-ID | 1 |
| Descrição | Temperatura muito alta - lubrificante do eixo do mancal. |
| Consequencias da falha na demanda | · Possíveis danos na unidade compressora;<br>· Vazamento incontrolado de gás podendo ocasionar explosão;<br>· Vibração excessiva e ruído alto. |
| SIL | 1 |
| Eventos Inicializadores de Prevenção | · TIT-211A<br>· TIT-211B<br>· TIT-211C<br>· TIT-211D |
| Acões de Prevenção | · Parada de emergência dos compressores TC-12001A/B/C/D. |
| Consequências da falha da prevenção | PRESENÇA DE GÁS E FOGO, EXPLOSÕES, CENÁRIO CATASTRÓFICO |
| Eventos Inicializadores de Mitigação | · TIT-211A, TIT-211B, TIT-211C, TIT-211D ACIMA DE 20% OU FAIXA DE 20% COM GRADIENTE POSITIVO |
| Acões de Mitigação | · Parada de emergência dos TC-12001A/ B/ C/ D.<br>· Resfriamento forçado com gás carbônico. |

### 4.1.6 Modelagem do algoritmo de controle

De posse dos resultados obtidos a partir da matriz causa-efeito, e da identificação das SIFs, o próximo passo trata da modelagem, em RdP, dos algoritmos de controle e verificação e validação do modelo gerado, com o auxílio das ferramentas HPSIM e PIPE2. A Figura 4.5 representa o modelo gerado para os eventos inicializadores da SIF 1.

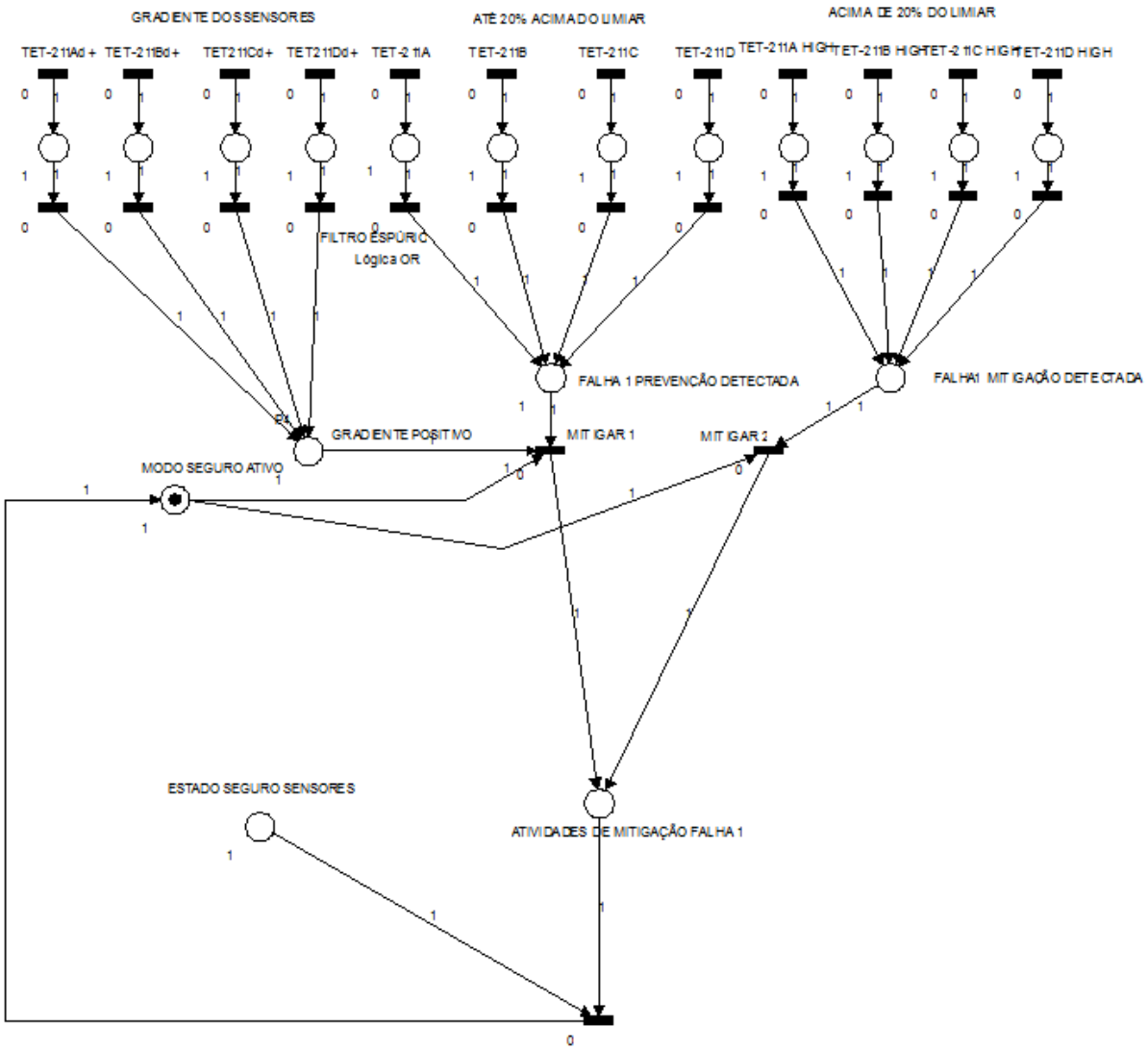



Figura 4.5 – Modelo em RdP da SIF 1.

Caso ocorra alguma falha, detectada pelos eventos inicializadres, representados pelos sensores, as respectivas ações de mitigação, representadas pelos atuadores de mitigação, são desempenhadas com o objetivo de se evitar o cenário de catástrofe. O modelo das atividades de mitigação da SIF 1, de acordo com a equipe de especialistas, é representado no modelo em RdP da Figura 4.6.

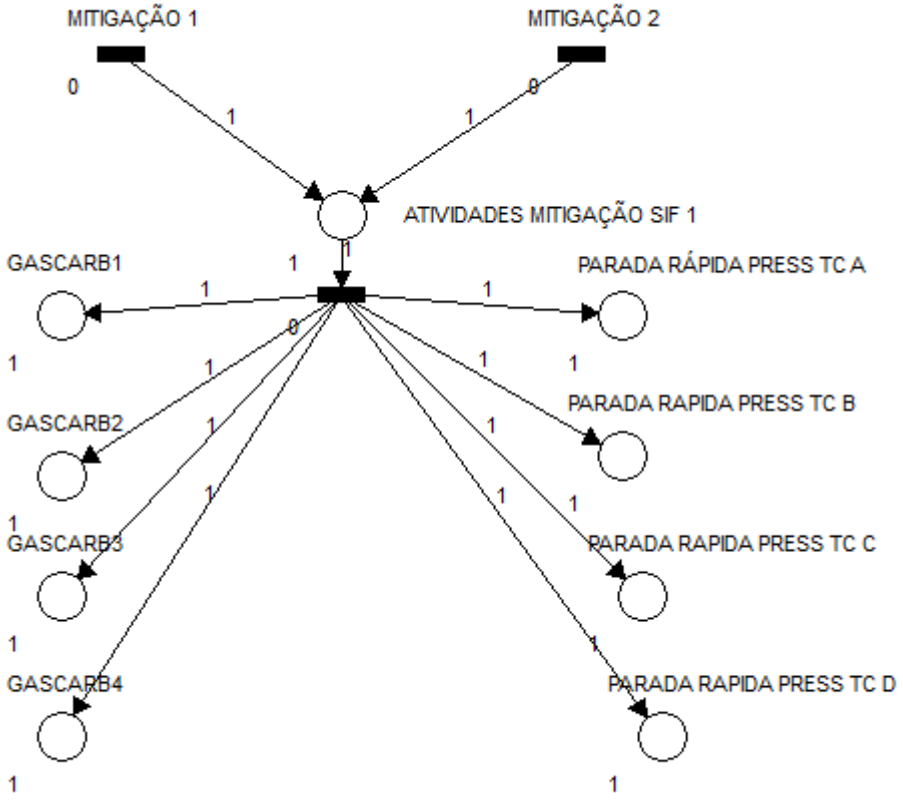



Figura 4.6 – Ações de mitigação para a SIF 1.

As ações de mitigação ocorrem até que todos os eventos inicializadores, isto é, os sensores estejam indicando condições normais de operação. O modelo em RdP, indicativo do estado seguro dos sensores, é representado na Figura 4.7.

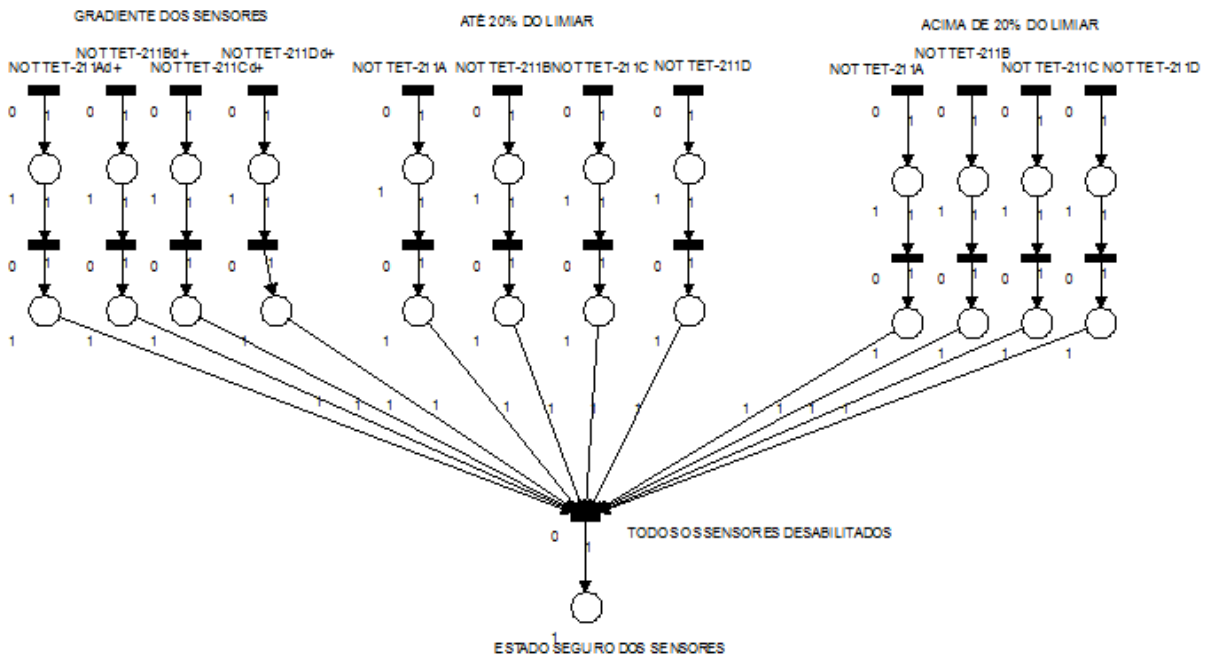



Figura 4.7 – Modelo em RdP para identificação do estado seguro dos sensores.

A verificação do estado seguro dos sensores não implica em uma condição para reinício automático da planta. De acordo com a IEC 61508/61511, após a ação de mitigação, técnicos especializados no processo devem realizar uma inspeção em toda a planta para verificação e *checklist* das condições dos equipamentos. Após esta verificação é que o processo pode ser reiniciado.

Após a edição, simulação para verificação e análise dos modelos, pôde-se concluir, com base nos resultados apresentados, que as propriedades de *vivacidade, reiniciabilidade e limitabilidade / segurança* são verificadas. Os modelos são então re-avaliados para validação em relação do SIS de mitigação considerado.

## 4.1.7 Geração dos algoritmos fuzzy para as SIFs

A partir das ações de mitigação propostas, pode-se conceber os algoritmos de controle implementados por lógica fuzzy, a partir das informações obtidas da técnica "*What-If*" que são baseadas no conhecimento de um especialista no processo.

A Figura 4.8 ilustra a caracterização proposta para o parâmetro temperatura, representando os intervalos para a camada BPCS, para a camada de prevenção e para a camada de mitigação.

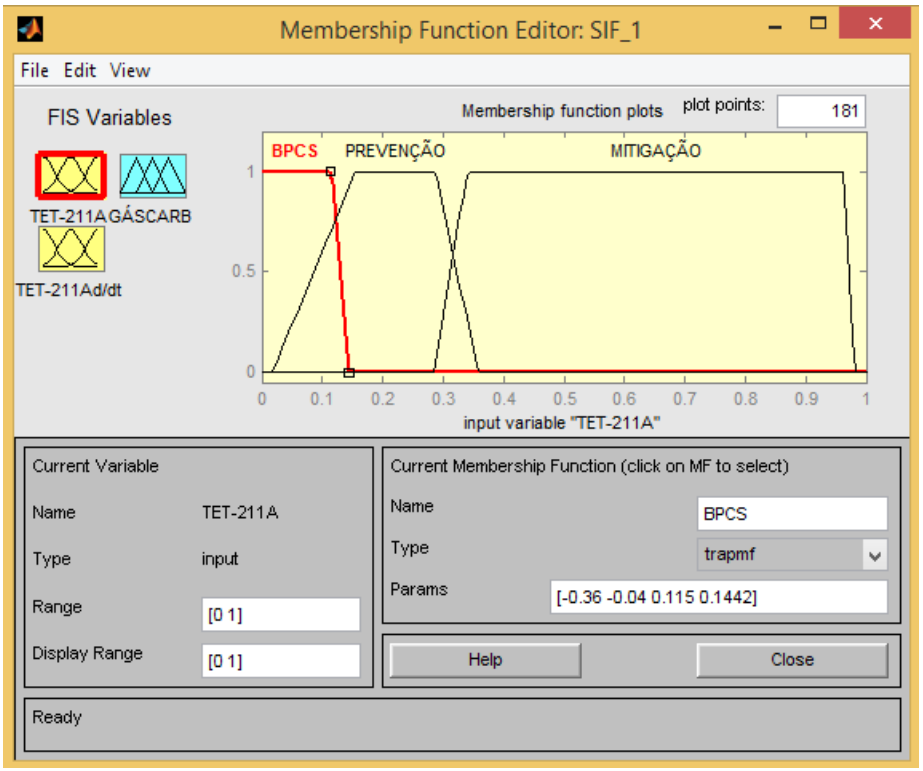



Figura 4.8 - Funções de pertinência fuzzy para a temperatura.

A entrada correspondente à derivada temporal da temperatura são atribuídos três valores: zero, positivo e negativo, representados na Figura 4.9.

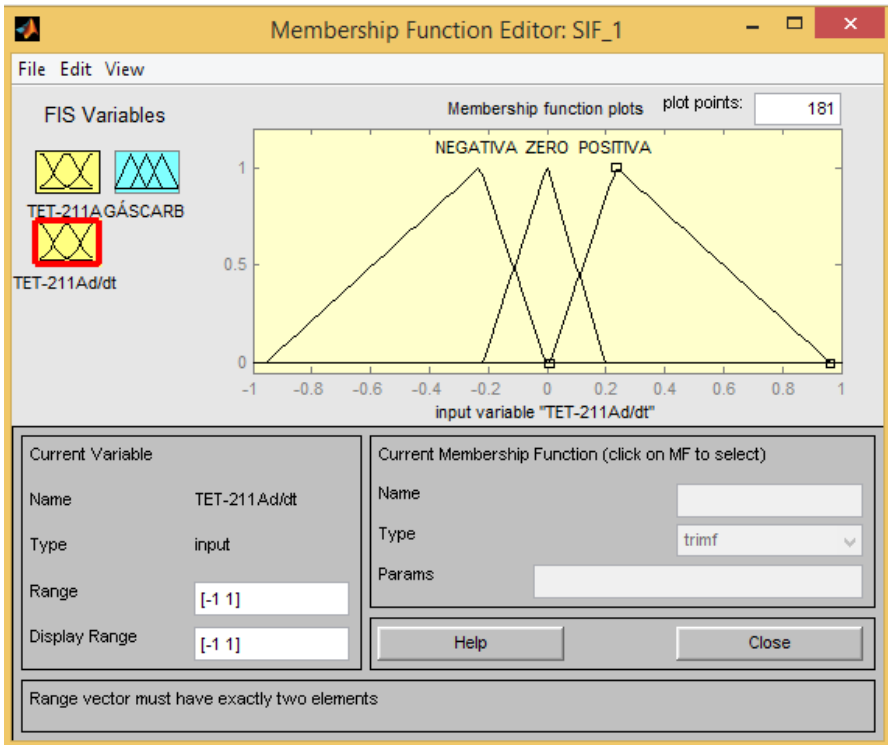



Figura 4.9 - Funções de pertinência para a derivada da temperatura.

O conjunto de regras fuzzy, de acordo com os resultados da técnica "*What-If*" são descritos na Tabela 4.4.

Tabela 4.4 - Regras fuzzy para a camada de mitigação.

| *SE* | TEMPERATURA | OPERADOR | DTEMPERATUR | ENTÃO | VALVULA |
|---|---|---|---|---|---|
| *1* | *BPCS* | | | | *ZERO – FECHADA* |
| *2* | *PREVENÇÃO* | *E* | *NEGATIVA* | | *ZERO – FECHADA* |
| *3* | *PREVENÇÃO* | *E* | *POSITIVA* | | *MEDIO – 50%* |
| *4* | *MITIGAÇÃO* | *E* | *POSITIVA* | | *ALTO - ABERTA* |
| *5* | *MITIGAÇÃO* | *E* | *NEGATIVA* | | *MÉDIO – 50%* |
| *6* | *MITIGAÇÃO* | *E* | *ZERO* | | *ALTO – ABERTA* |
| *7* | *PREVENÇÃO* | *E* | *ZERO* | | *ZERO - FECHADA* |

À saída, correspondente ao percentual de abertura da válvula, são atribuídas três posições: zero ou válvula fechada, alta ou 100 % aberta e médio, aberta a 50%. A Figura 4.10 representa as funções de pertinência para a variável de saída representada pelo percentual de abertura da válvula de liberação de gás carbônico.

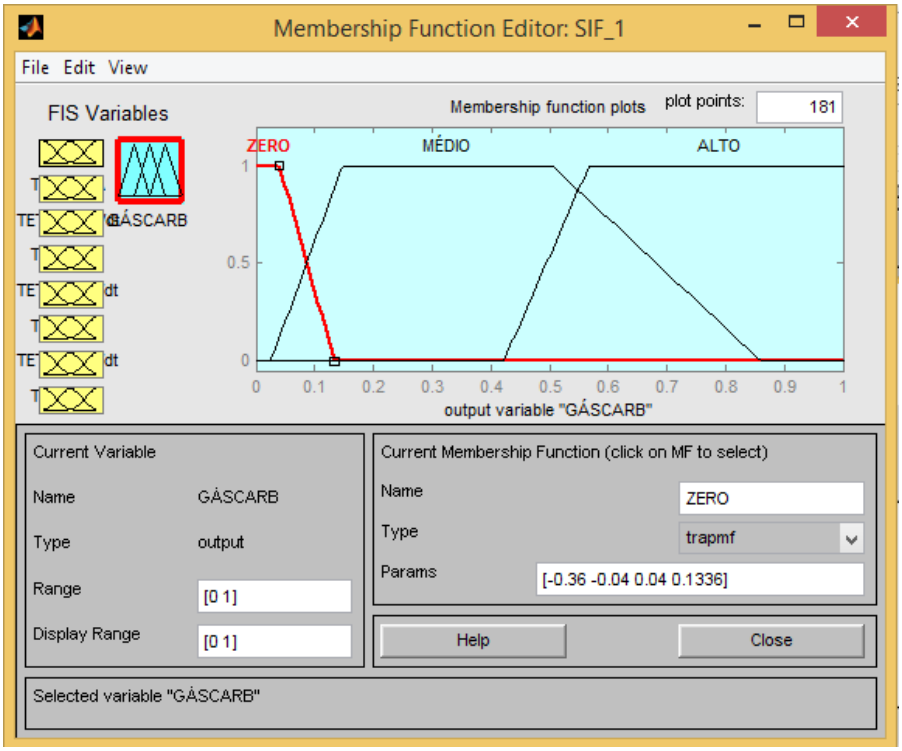



Figura 4.10 – Função de pertinência para a variável de saída.

A Tabela 4.5 apresenta o conjunto de regras utilizado.

Tabela 4.5 – Fuzzy Set

| | |
|---|---|
| ***MODELO FUZZY*** | **MANDANI** |
| ***MÉTODO AND*** | **MIN** |
| ***MÉTODO OR*** | **MAX** |
| ***IMPLICAÇÃO*** | ***MIN*** |
| ***AGREGAÇÃO*** | ***MAX*** |
| ***DEFUZZIFICAÇÃO*** | ***CENTROIDE*** |

A representação do módulo de inferência fuzzy está na Figura 4.11.

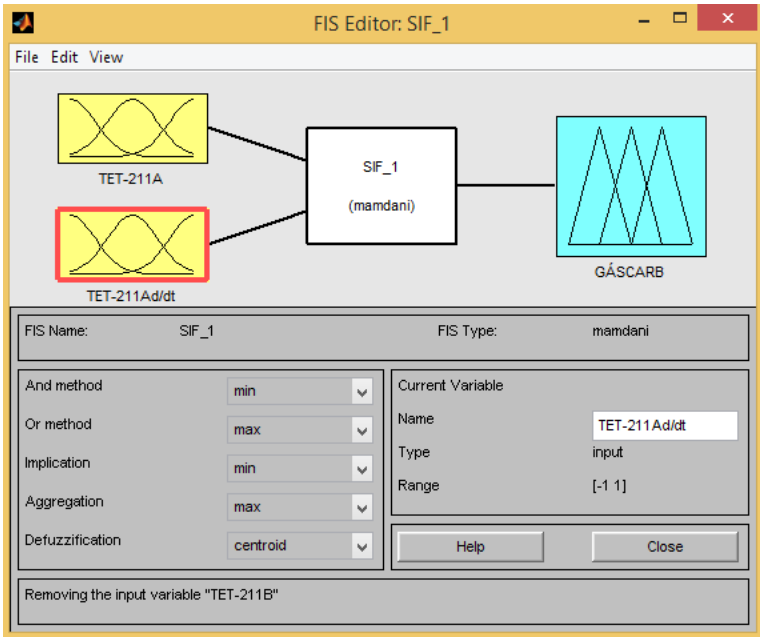



Figura 4.11 – Módulo de inferência fuzzy no *toolbox* do MatLab®

A implementação do conjunto de regras fuzzy pode ser visualizada na Figura 4.12.

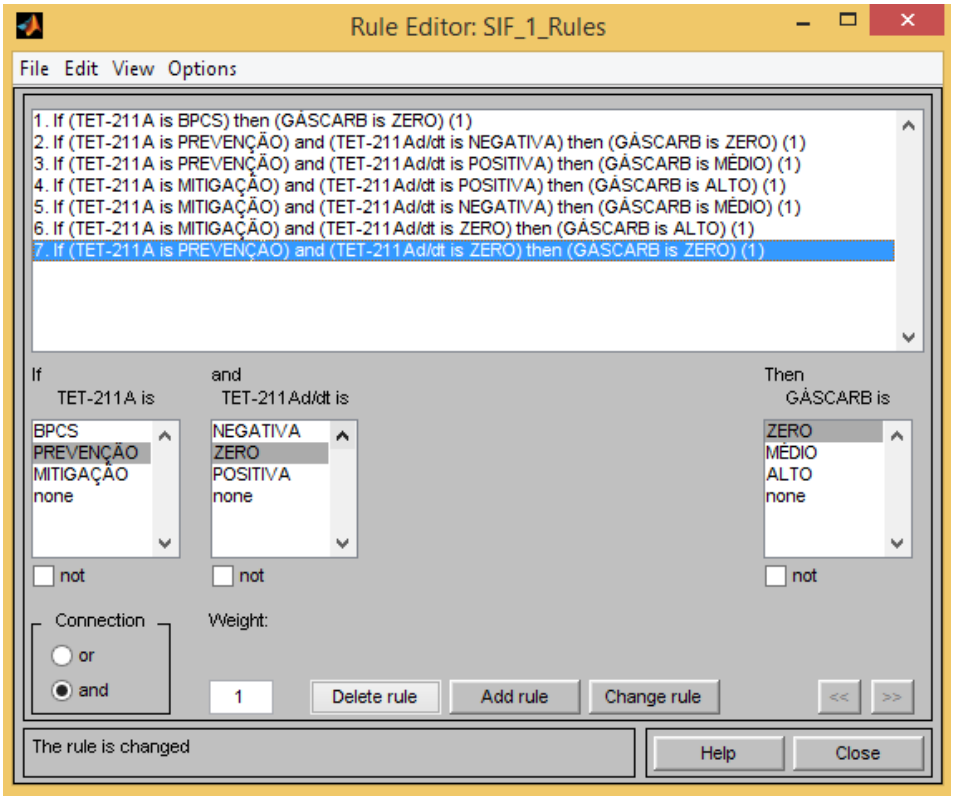



Figura 4.12 – Regras Fuzzy no *toolbox.*

De acordo com o intervalo determinado para as variáveis de entrada para as camadas BPCS, Prevenção e Mitigação e o conjunto de regras, obtidos pelos

resultados da aplicação das técnicas de análise de riscos, e do módulo de inferência adotado, tem-se como resultado uma superfície, representado na Figura 4.13, que representa, para cada par de pontos que indicam respectivamente o valor absoluto da variável e o seu gradiente temporal, o correspondente valor do atuador de mitigação, que neste exemplo é a válvula de liberação de gás carbônico.

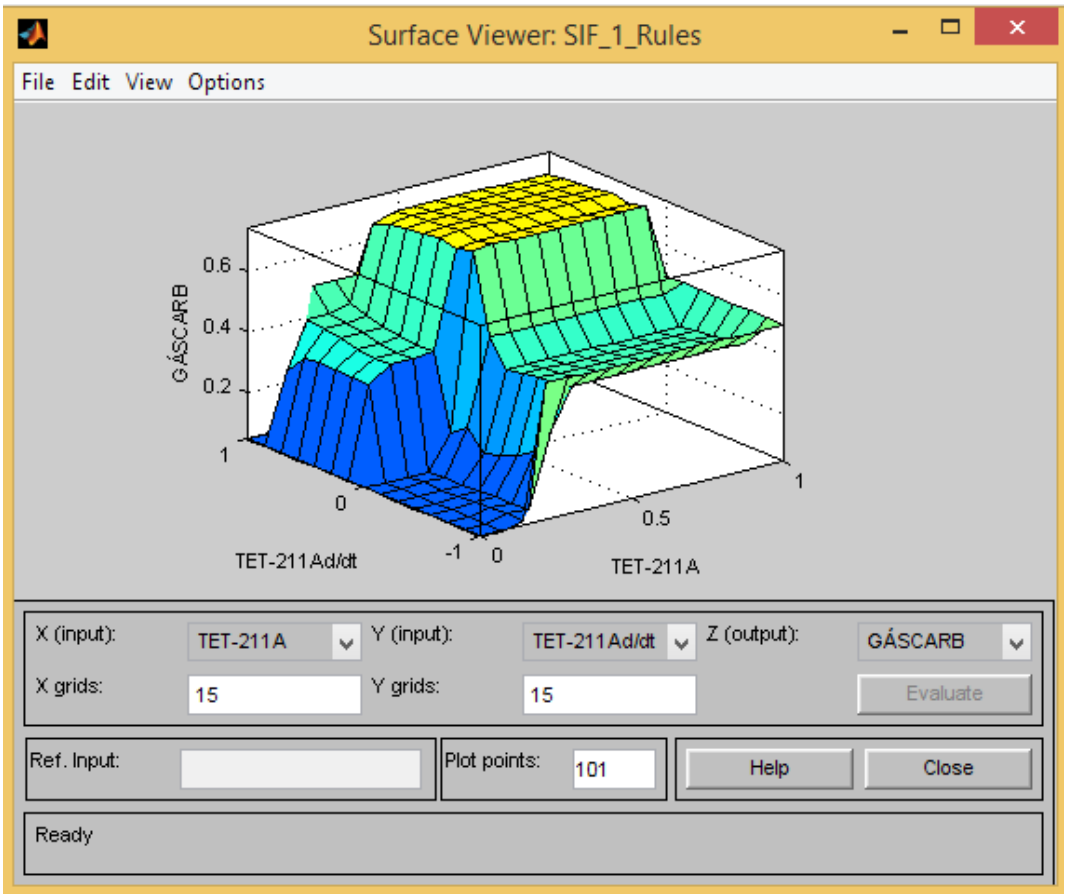



Figura 4.13 - Superfície gerada pelo algoritmo fuzzy.

Neste exemplo foram analisados quatro sensores, um para cada unidade compressora. Desta forma, considera-se o conjunto dos quatro sensores no algoritmo, com a relação lógica ou para cada sensor. Tal relação pode ser melhor compreendida na Equação 4.1.

$$\{[(TET-211A)\wedge(TET211A\ d/dt)]\vee[(TET-211B)\wedge(TET211B\ d/dt)]\vee[(TET-211C)\wedge(TET211C\ d/dt)]\ \vee[(TET-211D)\wedge(TET-211D\ d/dt)]\} \quad (4.1)$$

Os dados dos sensores no módulo fuzzy e a relação lógica da Equação 4.1 são visualizados na Figura 4.14. Para o controlador fuzzy com dois sensores e uma válvula de saída tem-se um total de 7 regras. Considerando 4 sensores, e portanto 8 sinais de entrada e quatro atuadores, tem-se um total de 28 regras.

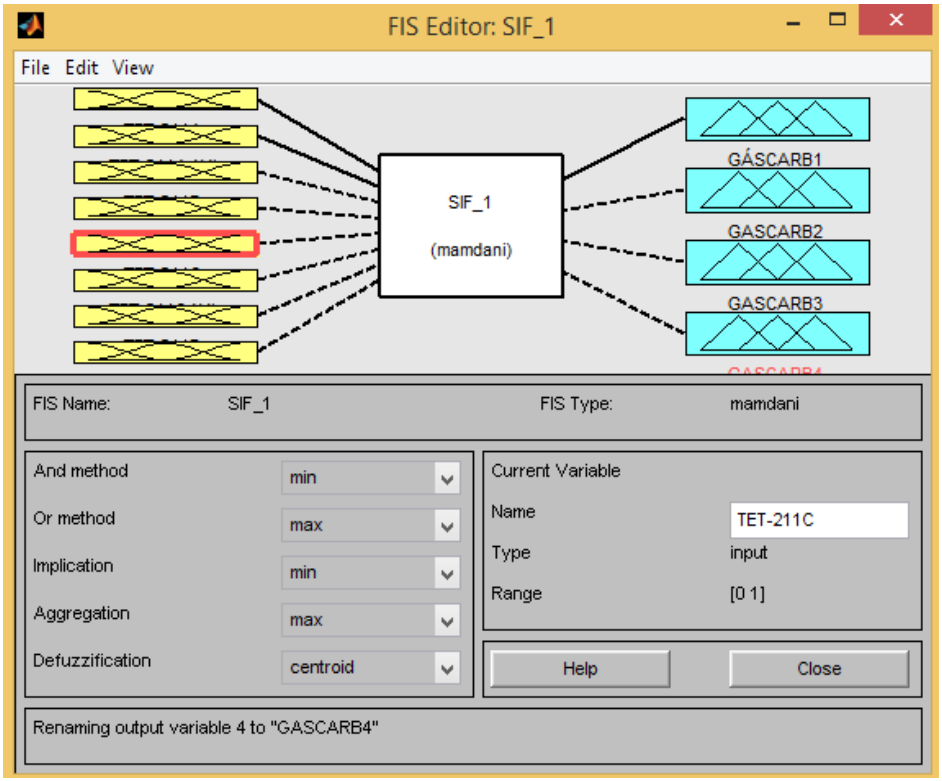



Figura 4.14 – Sinais de entrada para o controlador fuzzy.

## 4.1.8 Códigos de controle com referência à IEC 61131-7

O próximo passo consiste na conversão dos algoritmos fuzzy em programa de controle para implementação em CPs. Considera-se aqui a IEC 61131-7, que trata da conversão de programas em FCL – *Fuzzy Control Language* em linguagem ST – *Structured Text*, definida na IEC 61131-3. A conversão dos modelos e o código ST

para o exemplo de aplicação 1, considerando um sensor de entrada, com o valor absoluto da variável e seu gradiente, e um atuador, é apresentado na Figura 4.15.

```
FUZZIFY temperature

        TERM BasicControl := (0,1) (200,1) (250,0);
        TERM prevent := (200,0) (250,1) (300,1) (350,0);
        TERM mitigate := (300,0) (350,1) (1000,1);

END_FUZZIFY


FUZZIFY dtemperature

        TERM N := (-1,1) (-0.2,1) (0,0);
        TERM Z := (-0.2,0) (0,1) (0.2,0) ;
        TERM P := (0,0) (0.2,1) (1,1);

END_FUZZIFY


DEFUZZIFY valvule

        TERM zero := 0;
        TERM medium := (0,0) (20,1) (55,1) (95,0);|
        TERM high := (40,0) (100,1);

        ACCU : MAX;
        METHOD : COG;
        DEFAULT := 0;

END_DEFUZZIFY

RULEBLOCK No1
        AND : MIN;

        RULE 1 : IF temperature is mitigate THEN valvule IS high;
        RULE 2 : IF temperature is BasicControl THEN valvule IS zero;
        RULE 3 : IF (temperature is prevent) and (dtemperature is P)
                 THEN valvula IS medium;
        RULE 4 : IF (temperature is mitigate) and (dtemperature is N)
                 THEN valvula IS medium;
```

Figura 4.15 – Programa de controle implementado em FCL (IEC, 2000).

## 4.2 Aplicação da Sistemática Proposta – Caso de Uso 2

Após a aplicação da sistemática para uma SIF composta por um evento inicializador (sensor) e um atuador de mitigação, tem-se como resultado o modelo do algoritmo de controle devidamente validado para as propriedades de *vivacidade, reiniciabilidade e*

*limitabilidade / segurança*. Os patamares para as camadas de controle BPCS, prevenção e mitigação foram definidos para o sensor indicativo para estado de falha e as correspondentes ações de mitigação foram implementadas nos modelos fuzzy do *toolbox* da ferramenta Matlab®. A ação antecipatória pôde ser verificada na superfície fuzzy gerada, e o código de controle em *ST* foi obtido com referência à IEC 61131-7. De posse dos resultados obtidos, a sistemática será aplicada para todas as SIFs do processo produtivo em análise, incluindo-se as camadas de gás e de fogo, considerando a unidade compressora como elemento crítico do processo produtivo, conforme a aplicação das técnicas de análise de risco FMEA e FTA.

### 4.2.1 Detecção dos efeitos da ocorrência de falhas dos elementos críticos

De posse dos resultados da aplicação das técnicas de análise de riscos e considerando todos os resultados obtidos para os possíveis modos de falha da unidade compressora e com base no conhecimento técnico da equipe de especialistas, manuais técnicos, *benchmarking* e dados de registros históricos, a detecção dos efeitos da ocorrência de falhas são listados na Tabela 4.6, com o correspondente TAG, de acordo com a norma ISA S5.1 (ISA, 1984 (R1992)).

Tabela 4.6 – Efeitos da ocorrência de falhas e correspondentes TAGs

| FALHA | TAG do sensor |
|---|---|
| Nível muito alto no FT-12001A | LSHH-006 |
| Nível muito alto no FT-12001A | LSHH-007 |
| Pressão diferencial muito alta no FT-12001A | PDSHH-005 |
| Nível muito alto no FT-12001B | LSHH-013 |
| Nível muito alto no FT-12001B | LSHH-014 |
| Pressão diferencial muito alta no FT-12001B | PDSHH-025 |
| Pressão muito alta no header de descarga | PSHH-006A/B/C |
| Pressão muito alta na descarga do C-12001A | PSHH-207A |

| | |
|---|---|
| Temperatura muito alta a jusante do P-12001A | TSHH-209A |
| Pressão muito alta na descarga do C-12001B | PSHH-207B |
| Temperatura muito alta a jusante do P-12001B | TSHH-209B |
| Pressão muito alta na descarga do C-12001C | PSHH-207C |
| Temperatura muito alta a jusante do P-12001C | TSHH-209C |
| Pressão muito alta na descarga do C-12001D | PSHH-207D |
| Temperatura muito alta a jusante do P-12001D | TSHH-209D |
| Pressão muito baixa a jusante do P-12002A/B | PSLL-105 |
| Pressão muito alta na linha de gás combustível TS-C-12001A/B/C/D | PSHH-166 |
| Temperatura muito baixa na linha de gás combustível MC-GE-12001A/B | TSLL-122 |
| Pressão muito alta na linha de gás combustível MC-GE-12001A/B | PSHH-167 |
| Temperatura alta no CM-12001A | TSH-302A |
| Temperatura alta no CM-12001B | TSH-302B |
| Pressão muito baixa no sistema de ar de instrumento | PSLL-506 |
| Pressão muito alta no sistema de ar de instrumento | PSHH-506 |

### 4.2.2 Ações de mitigação propostas

Para os efeitos das falhas dos componentes críticos, a Tabela 4.7 indica as ações de mitigação propostas, com base no conhecimento da equipe de especialistas no processo.

Para cada ação de mitigação um ou mais atuadores são necessários. Desta forma, a Tabela 4.7 apresenta, de forma adicional, a correlação do TAG (ISA, 1984 (R1992)) do atuador com a respectiva ação de mitigação.

Tabela 4.7 – Ações de mitigação propostas e TAGs dos atuadores.

| AÇÃO DE MITIGAÇÃO | TAG do atuador |
|---|---|
| Fecha válvula da sucção 1 (XV-001) da ECOMP | XY-001B |
| Fecha válvula de equalização (XV-017) da XV-001 | XY-017B |
| Fecha válvula da sucção 2 (XV-019) da ECOMP | XY-019B |
| Fecha válvula de equalização (XV-020) da XV-019 | XY-020B |
| Fecha válvula da descarga (XV-003) da ECOMP | XY-003B |
| Fecha válvula de equalização (XV-018) da XV-003 | XY-018B |
| Fecha válvula bloqueio (XV-101A/B) gás combustível TCs | XY-101A/B |
| Fecha válvula bloqueio (XV-102A/B) gás combustível MC-GE | XY-102A/B |
| Fecha válvula bloqueio (XV-125) do FT-12002A/B | XY-125 |
| Abre válvula direcional de N2 (TV-302A) | TY-302A |
| Abre válvula direcional de N2 (TV-302B) | TY-302B |
| Parada dos motogeradores MC-GE-12001A/B | XS-4100.12102A/B |
| Parada dos compressores de ar C-12002A/B/C | |
| Fecha válvula bloqueio (XV-010A) entrada do TS-C-12001A | XY-010A |
| Fecha válvula de equalização (XV-011A) da XV-010A | XY-011A |
| Fecha válvula bloqueio (XV-010B) entrada do TS-C-12001B | XY-010B |
| Fecha válvula de equalização (XV-011B) da XV-010B | XY-011B |
| Fecha válvula bloqueio (XV-010C) entrada do TS-C-12001C | XY-010C |
| Fecha válvula de equalização (XV-011C) da XV-010C | XY-011C |
| Fecha válvula bloqueio (XV-010D) entrada do TS-C-12001D | XY-010D |
| Fecha válvula de equalização (XV-011D) da XV-010D | XY-011D |
| Fecha válvula bloqueio (XV-025A) entrada do TS-C-12001A | XY-025A |
| Fecha válvula de equalização (XV-026A) da XV-025A | XY-026A |

| | |
|---|---|
| Fecha válvula bloqueio (XV-025B) entrada do TS-C-12001B | XY-025B |
| Fecha válvula de equalização (XV-026B) da XV-025B | XY-026B |
| Fecha válvula bloqueio (XV-025C) entrada do TS-C-12001C | XY-025C |
| Fecha válvula de equalização (XV-026C) da XV-025C | XY-026C |
| Fecha válvula bloqueio (XV-025D) entrada do TS-C-12001D | XY-025D |
| Fecha válvula de equalização (XV-026D) da XV-025D | XY-026D |
| Fecha válvula bloqueio (XV-016A) saída do TS-C-12001A | XY-016 A |
| Fecha válvula bloqueio (XV-16B) saída do TS-C-12001B | XY-016 B |
| Fecha válvula bloqueio (XV-016C)saída do TS-C-12001C | XY-016 C |
| Fecha válvula bloqueio (XV-016D) saída do TS-C-12001D | XY-016 D |
| Parada do TS-C-12001A com resfriamento (*cooldown)*<br>Parada do TS-C-12001B com resfriamento (*cooldown)* | |
| Parada do TS-C-12001C com resfriamento (*cooldown)* | |
| Parada do TS-C-12001D com resfriamento (*cooldown)* | |
| Parada Rápida do TS-C-12001A (pressurizada) | |
| Parada Rápida do TS-C-12001 B (pressurizada) | |
| Parada Rápida do TS-C-12001 C (pressurizada) | |
| Parada Rápida do TS-C-12001 D (pressurizada) | |

### 4.2.3 Elaboração da matriz causa-efeito

O passo seguinte da sistemática consiste em elaborar a matriz causa-efeito, em que os efeitos da ocorrência das falhas, detectados pelos respectivos sensores, são alocados nas linhas da matriz, designados como causas ou eventos inicializadores da camada SIS de mitigação.

Já as ações de mitigação propostas, realizados pelos atuadores de mitigação, são representados nas colunas da matriz, designados como os efeitos aos eventos inicializadores.

Devido ao elevado número de eventos inicializadores e do elevado número de atuadores para cada evento inicializador, a elaboração da matriz causa-efeito é de extrema importância, pois identifica ações de mitigação comuns para diferentes eventos inicializadores. A matriz causa-efeito contribui para a melhor identificação desta simultaneidade, facilitando a execução dos passos seguintes da sistemática.

Devido à sua extensão, a matriz causa-efeito encontra-se no anexo B.

### 4.2.4 Identificação das SIFs

A partir da matriz causa-efeito, as correspondentes SIFs são identificadas, de acordo com seu grau de severidade, o nível de integridade SIL associado e sua probabilidade de falha sob demanda PFD. A identificação das SIFs de prevenção, proposta por Squillante (2011) serve de base para a camada SIS de mitigação. Conforme os requisitos da IEC 61508 / IEC 61511, os CPs das camadas SIS devem ser independentes, e portanto as ações de mitigação resultam, para cada SIF de prevenção, em uma ação redundante, caso os atuadores da camada SIS de prevenção sejam comuns à camada SIS de mitigação. As SIFs são representadas nas Tabelas 4.8 a 4.11.

Tabela 4.8 – SIF 1 Mitigação

| | |
|---|---|
| SIF-ID | 1 |
| Descrição | Pressão muito alta na descarga da ECOMP (Falha 1) |
| Consequencias da falha na demanda | · Possíveis danos na linha de descarga;<br>· Vazamento incontrolado de gás podendo ocasionar explosão;<br>· Vibração excessiva e ruído alto. |
| SIL | 3 |
| Eventos Inicializadores de Prevenção | · PIT-006A<br>· PIT-006B<br>· PIT-006C<br>votação 2oo3 |
| Acões de Prevenção | · Fechar válvulas:<br>XV-001 / XV-017;<br>XV-019 / XV-020;<br>XV-003 / XV-018.<br>· Parada de emergência dos turbos compressores TC-12001A/B/C/D. |
| Consequencias da falha da prevenção | PRESENÇA DE GÁS E FOGO, EXPLOSÕES, CENÁRIO CATASTRÓFICO |
| Eventos Inicializadores de Mitigação | PIT-006A, PIT-006B, PIT-006C ACIMA DE 20% OU FAIXA DE 20% COM GRADIENTE POSITIVO |
| Acões de Mitigação | Fechar as válvulas: XV-001, XV-017, XV-019, XV-020, XV-003, XV-018, XV-10A, XV-11A, XV-10B, XV-11B, XV-10C, XV-11C, XV-10D, XV-11D, XV-25A, XV-26A, XV-25B, XV-26B, XV-25C, XV-26C, XV-25D, XV-26D, XV-16A, XV-16B, XV-16C, XV-16D, Parada rápida pressurizada dos TC A, B, C, D. |

Tabela 4.9 – SIF 2 Mititgação

| SIF-ID | 2 |
|---|---|
| Descrição | Nível de condensado muito alto nos Filtros A e B na entrada da ECOMP (Falha 2) |
| Consequencias da falha na demanda | Arraste de condensado para os turbos compressores A, B, C e D com possibilidade de dano aos mesmos. |
| SIL | 1 |
| Eventos Inicializadores de Prevenção | LIT-006· LIT-007<br>· LIT-013<br>· LIT-014<br>· PDSHH-005<br>· PDSHH-025 |
| Acões de Prevenção | · Fechar válvulas:<br>XV-001 / XV-017;<br>XV-019 / XV-020;<br>XV-003 / XV-018.<br>XV-005 / XV-022<br>· Parada de emergência dos turbos compressores TC-12001A/B/C/D. |
| Consequencias da falha da prevenção | PRESENÇA DE GÁS E FOGO, EXPLOSÕES, CENÁRIO CATASTRÓFICO |
| Eventos Inicializadores de Mitigação | INICIALIZADORES DA PREVENÇÃO ACIMA DE 20% OU FAIXA DE 20% COM GRADIENTE POSITIVO |
| Acões de Mitigação | Fechar as válvulas: XV-001, XV-017, XV-019, XV-020, XV-003, XV-018, XV-10A, XV-11A, XV-10B, XV-11B, XV-10C, XV-11C, XV-10D, XV-11D, XV-25A, XV-26A, XV-25B, XV-26B, XV-25C, XV-26C, XV-25D, XV-26D, XV-16A, XV-16B, XV-16C, XV-16D, Parada rápida pressurizada dos TC A, B, C, D. |

Tabela 4.10 – SIF 3 Mitigação

| | |
|---|---|
| SIF-ID | 3 |
| Descrição | Pressão muito alta na descarga dos turbos compressores A, B, C e D (Falha 3) |
| Consequencias da falha na demanda | · Possíveis danos na linha de descarga;<br>· Possível fluxo reverso;<br>· Danificação dos turbos compressores. |
| SIL | 1 |
| Eventos Inicializadores de Prevenção | · PIT-207A<br>· PIT-207B<br>· PIT207C<br>· PIT207D |
| Acões de Prevenção | · Parada de emergência dos turbos compressores TC-12001A/B/C/D. |
| Consequencias da falha da prevenção | PRESENÇA DE GÁS E FOGO, EXPLOSÕES, CENÁRIO CATASTRÓFICO |
| Eventos Inicializadores de Mitigação | INICIALIZADORES DA PREVENÇÃO ACIMA DE 20% OU FAIXA DE 20% COM GRADIENTE POSITIVO |
| Acões de Mitigação | Fechar as válvulas: XV-10A, XV-11A, XV-10B, XV-11B, XV-10C, XV-11C, XV-10D, XV-11D, XV-25A, XV-26A, XV-25B, XV-26B, XV-25C, XV-26C, XV-25D, XV-26D, XV-16A, XV-16B, XV-16C, XV-16D, Parada rápida pressurizada dos TC A, B, C, D. |

Tabela 4.11 – SIF 4 Mitigação

| | |
|---|---|
| SIF-ID | 4 |
| Descrição | Temperatura muito alta na descarga dos turbos compressores A, B, C e D (Falha 4) |
| Consequencias da falha na demanda | · Possíveis danos na linha de descarga. |
| SIL | 1 |
| Eventos Inicializadores de Prevenção | · TIT-209A<br>· TIT-209B<br>· TIT-209C<br>· TIT-209D |
| Acões de Prevenção | · Parada de emergência dos turbos compressores TC-12001A/B/C/D. |
| Consequencias da falha da prevenção | PRESENÇA DE GÁS E FOGO, EXPLOSÕES, CENÁRIO CATASTRÓFICO |
| Eventos Inicializadores de Mitigação | INICIALIZADORES DA PREVENÇÃO ACIMA DE 20% OU FAIXA DE 20% COM GRADIENTE POSITIVO |
| Acões de Mitigação | Fechar as válvulas: XV-10A, XV-11A, XV-10B, XV-11B, XV-10C, XV-11C, XV-10D, XV-11D, XV-25A, XV-26A, XV-25B, XV-26B, XV-25C, XV-26C, XV-25D, XV-26D, XV-16A, XV-16B, XV-16C, XV-16D, Parada rápida pressurizada dos TC A, B, C, D. |

### 4.2.5 Modelagem do algoritmo de controle

Para cada SIF identificada na matriz causa-efeito é feita a modelagem em RdP com o auxílio da ferramenta HPSIM / PIPE2. Estas ferramentas são também utilizadas para se verificar formalmente o modelo em relação às propriedades de *vivacidade, reiniciabilidade e limitabilidade / segurança.*

O modelo em RdP para a detecção e tratamento da SIF 1 é representado na Figura 4.16. A lógica de detecção consiste no disparo das transições, que representam os respectivos sensores associados à ocorrência da SIF. Para cada transição é aplicado um filtro contra falhas espúrias, representado por um temporizador.

Caso o sensor continue a apresentar o valor anormal de processo, a falha passa então por um processo de votação. Para o caso da SIF 1 o critério adotado foi o da votação 2oo3, ou seja, a SIF 1 é diagnosticada quando ao menos 2 sensores indicarem o estado anormal da variável associada à ocorrência da falha.

Outras SIFs, dependendo da criticidade, podem ter uma relação lógica “ou”, ou seja, caso um dos sensores indicar a ocorrência do estado anormal para uma determinada variável, pode-se considerar a detecção da respectiva SIF.

Segundo Squillante (2011), o SIS de prevenção deve atuar no sentido de degenerar o sistema a um estado seguro quando da ocorrência de uma determinada SIF. No modelo em RdP apresentado, verifica-se que, no estado anormal de uma determinada variável, o modelo indica que o SIS de prevenção já está ativado.

No entanto, caso a variável de monitoração apresente um gradiente positivo mesmo com o SIS de prevenção em ação, a sistemática propõe a ativação do SIS de mitigação, com o objetivo de se ter uma ação antecipativa à ocorrência da catástrofe. Isto está representado nas transições de gradiente positivo, com uma relação lógica “e” com o SIS de prevenção.

Ou seja, caso o SIS de prevenção esteja ativo, e o gradiente da variável associada apresente um incremento, o SIS de mitigação será ativado, acionando-se os respectivos atuadores da SIF correspondente.

Por outro lado, a detecção da SIF pode ocorrer por uma condição muito anormal da variável associada à SIF, como por exemplo um valor acima de 20% do limiar aceitável para a respectiva variável.

Para tais casos, a ação antecipativa também é adotada, na medida em que o SIS de mitigação é imediatamente acionado, pois considera-se estar em uma condição próxima à ocorrência da catástrofe. O critério da velocidade de atuação passa a ser prioritário, uma vez que se a ação de prevenção, de forma isolada, pode não ser suficiente para degenerar o sistema a um estado seguro.

Para cada SIF são associadas ações de mitigação por meio dos respectivos atuadores, de acordo com a matriz causa-efeito.

As ações de mitigação são realizadas até que todos os sensores, em uma relação lógica “e” estejam indicando uma condição normal de operação.

Após estas verificações, e conforme prescrito nas normas IEC 61508 / IEC 61511, o rearme manual do sistema pode ser feito após uma análise minuciosa das instalações por uma equipe de especialistas.

Os modelos para detecção, tratamento e verificação segura dos sensores para as SIFs estão representados nas Figuras 4.16 a 4.23.

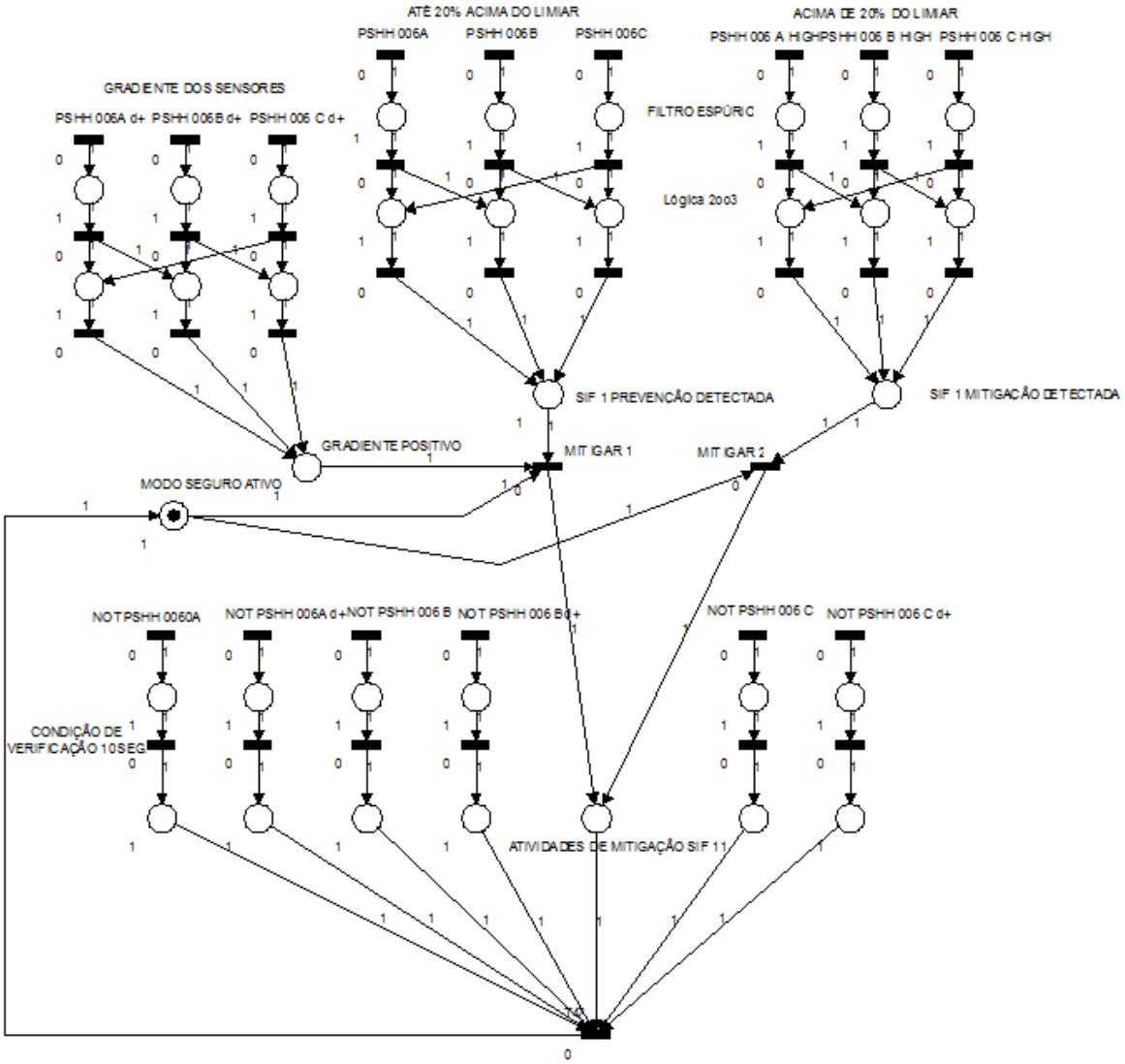



Figura 4.16 – Modelo em RdP para a detecção e tratamento da SIF 1.

As atividades de mitigação referentes à SIF 1, de acordo com a matriz causa-efeito, são apresentadas no modelo em RdP da Figura 4.17.

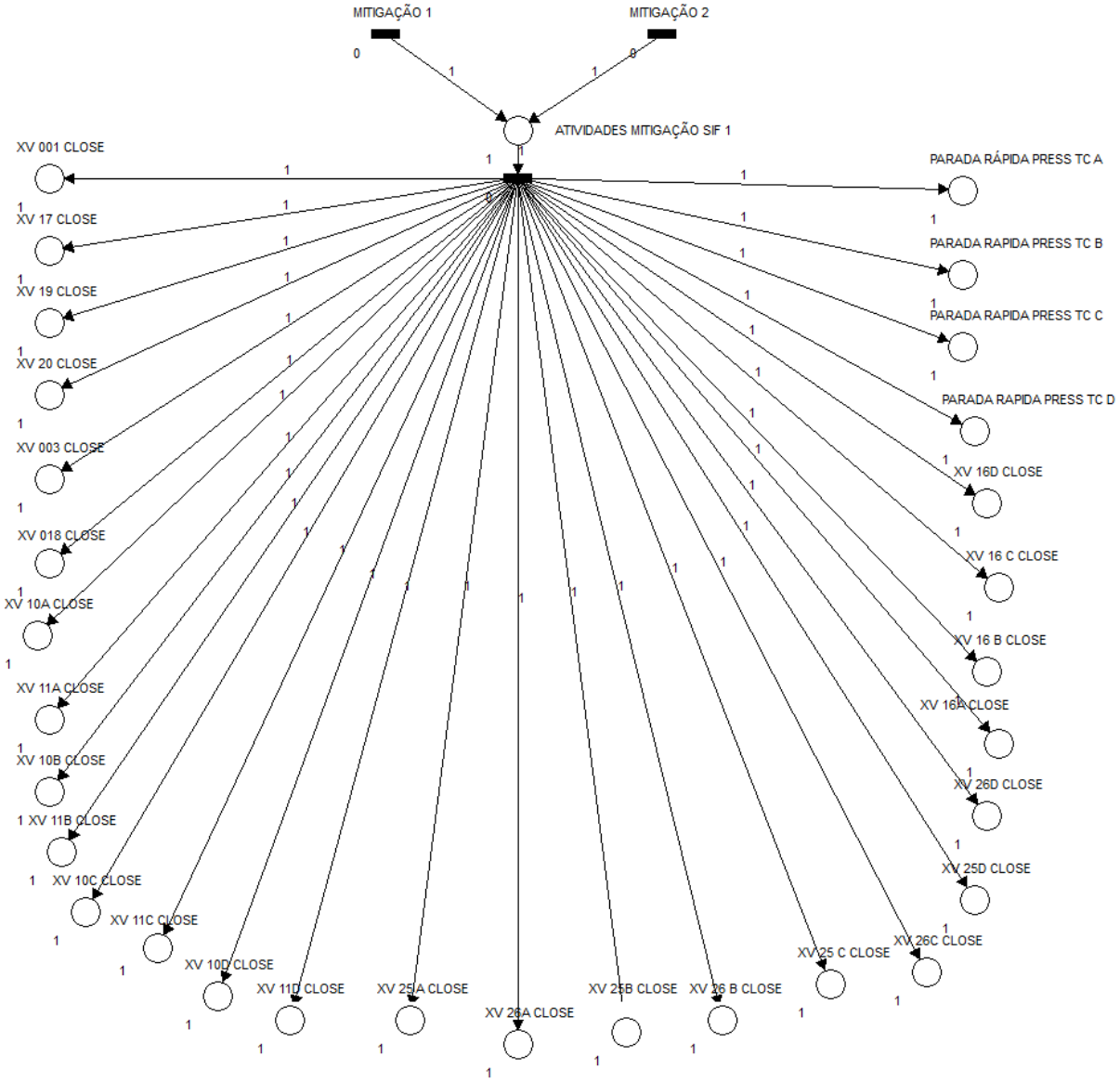



Figura 4.17 – Modelo em RdP para as ações de mitigação associadas à SIF 1.

O modelo em RdP para a detecção e tratamento da SIF 2 está na Figura 4.18.

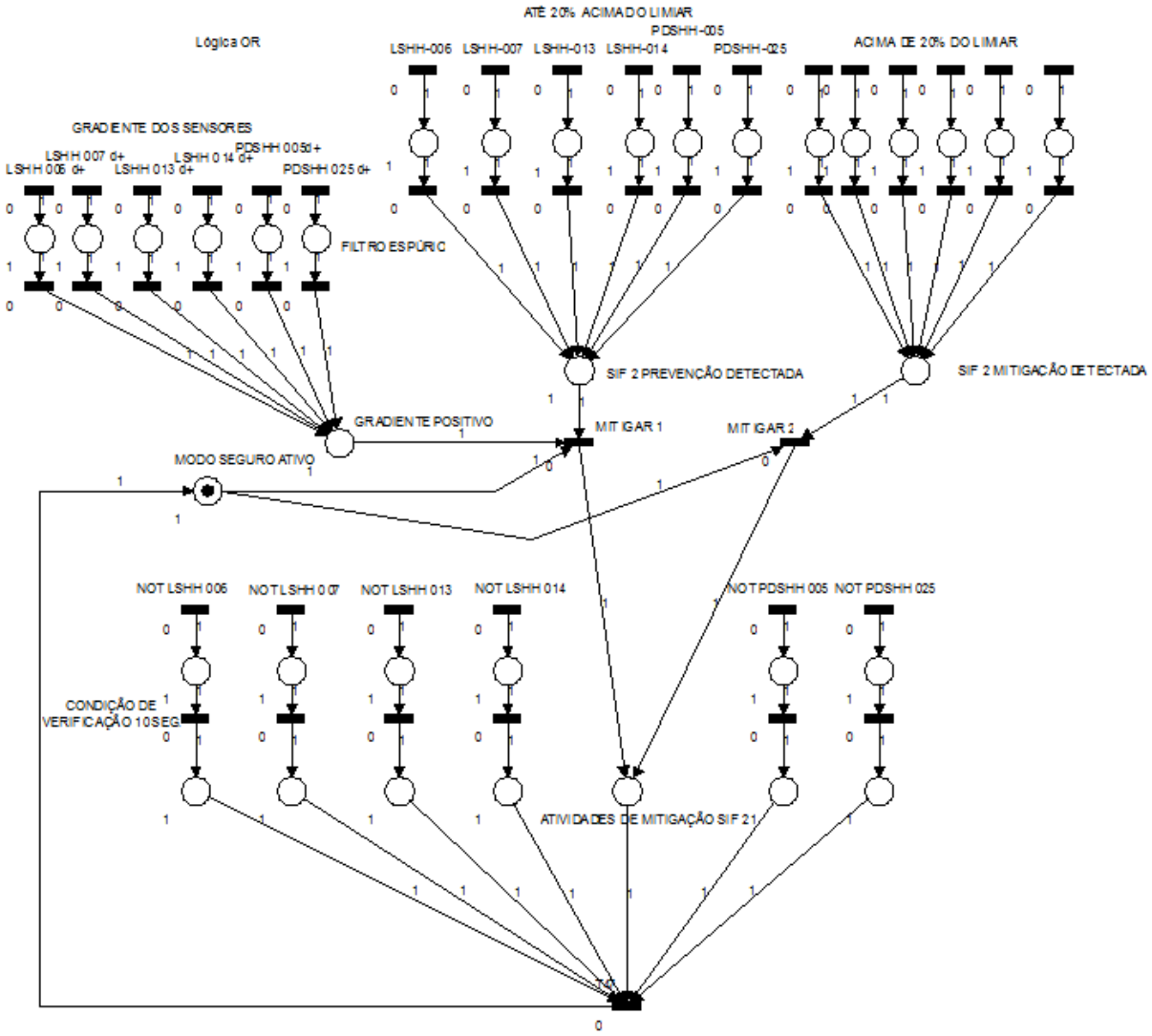



Figura 4.18 - Modelo em RdP para a detecção e tratamento da SIF 2.

As atividades de mitigação referentes à SIF 2, de acordo com a matriz causa-efeito, são apresentadas no modelo em RdP da Figura 4.19.

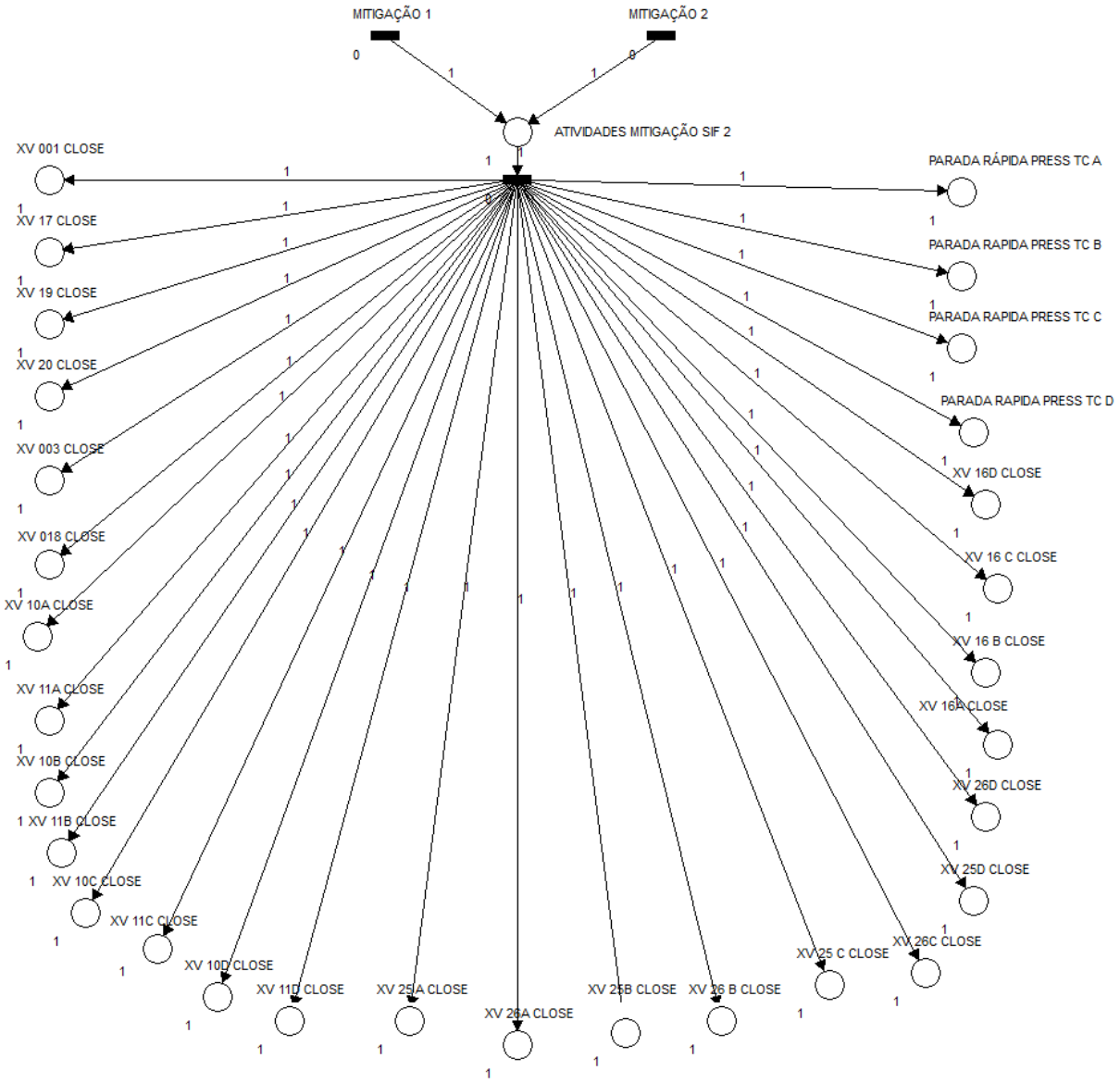



Figura 4.19 – Modelo em RdP para as ações de mitigação associadas à SIF 2.

O modelo em RdP para a detecção e tratamento da SIF 3 está na Figura 4.20.

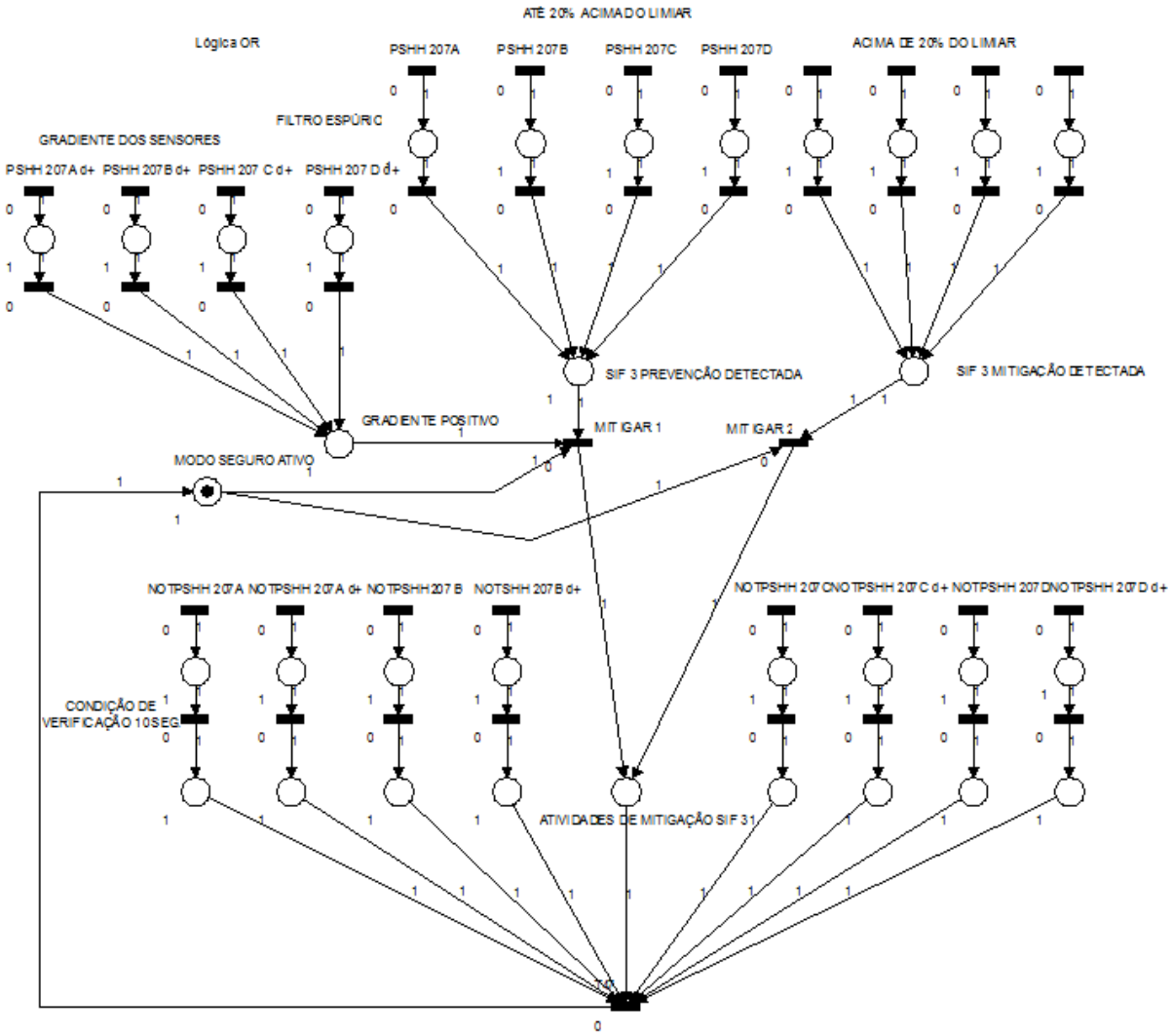



Figura 4.20 - Modelo em RdP para a detecção e tratamento da SIF 3.

As atividades de mitigação referentes à SIF 3, de acordo com a matriz causa-efeito, são apresentadas no modelo em RdP da Figura 4.21.

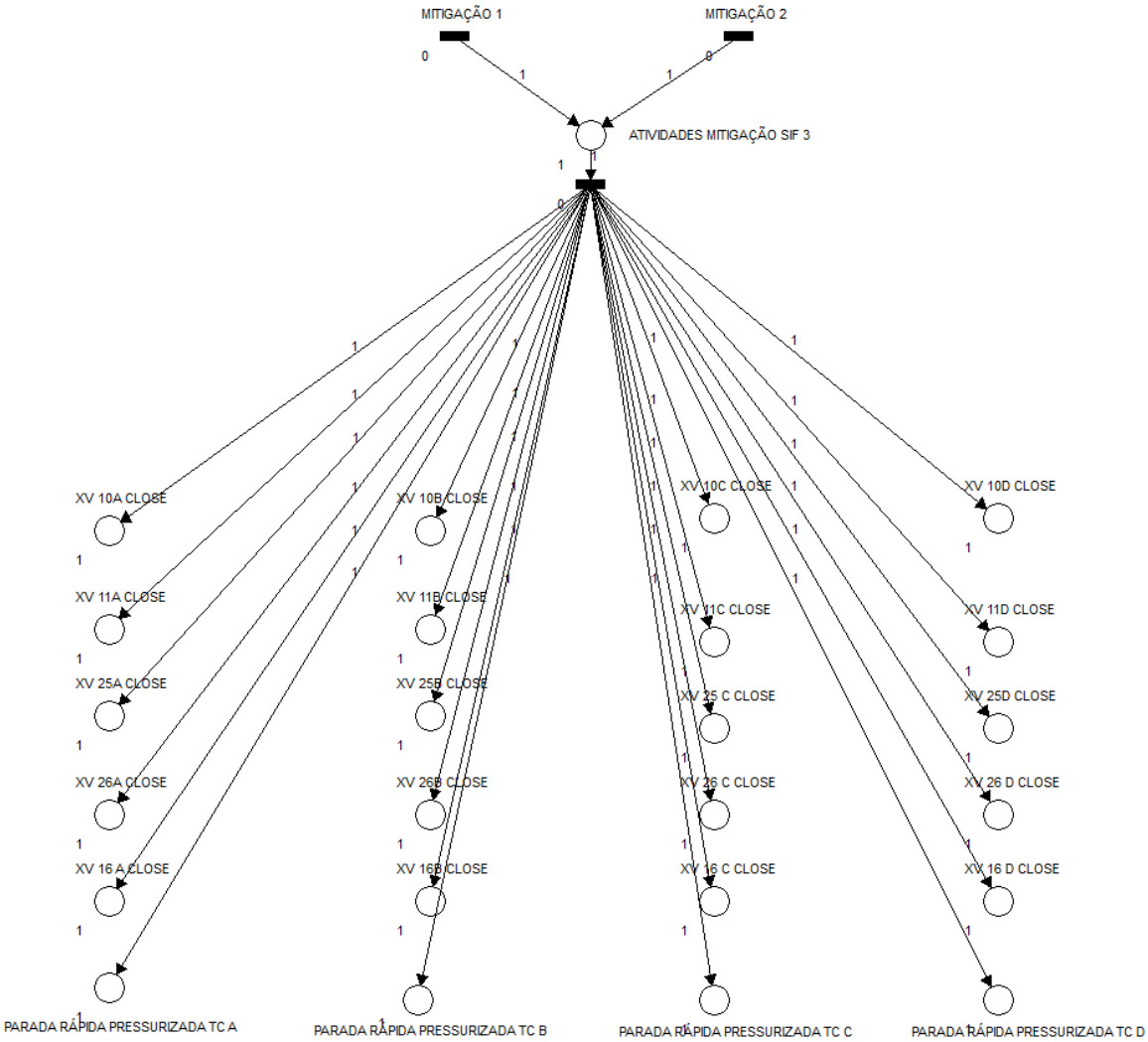



Figura 4.21 - Modelo em RdP para as ações de mitigação associadas à SIF 3.

O modelo em RdP para a detecção e tratamento da SIF 4 está Figura 4.22.

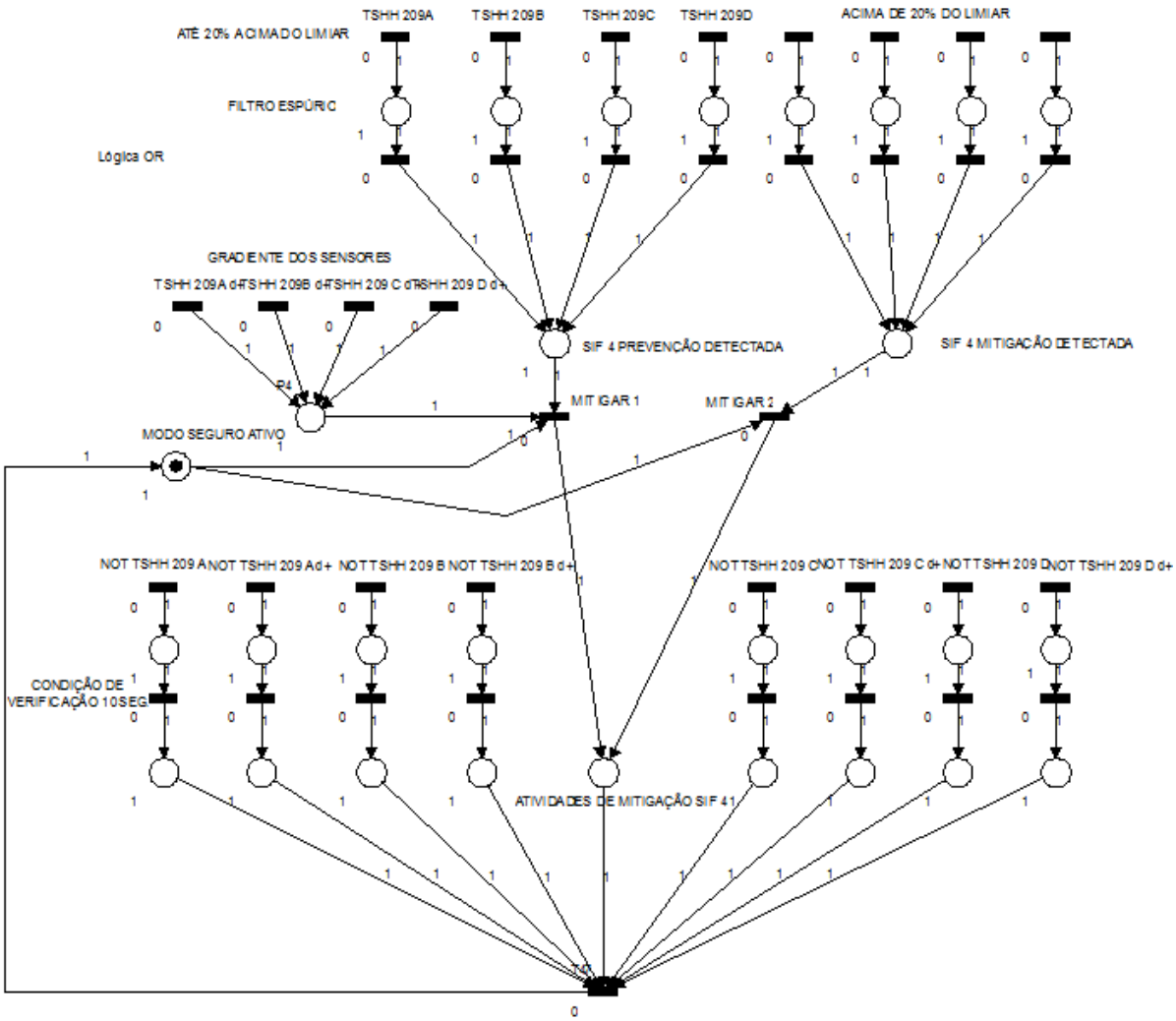



Figura 4.22 - Modelo em RdP para a detecção e tratamento da SIF 4.

As atividades de mitigação referentes à SIF 4, de acordo com a matriz causa-efeito, são apresentadas no modelo em RdP da Figura 4.23.

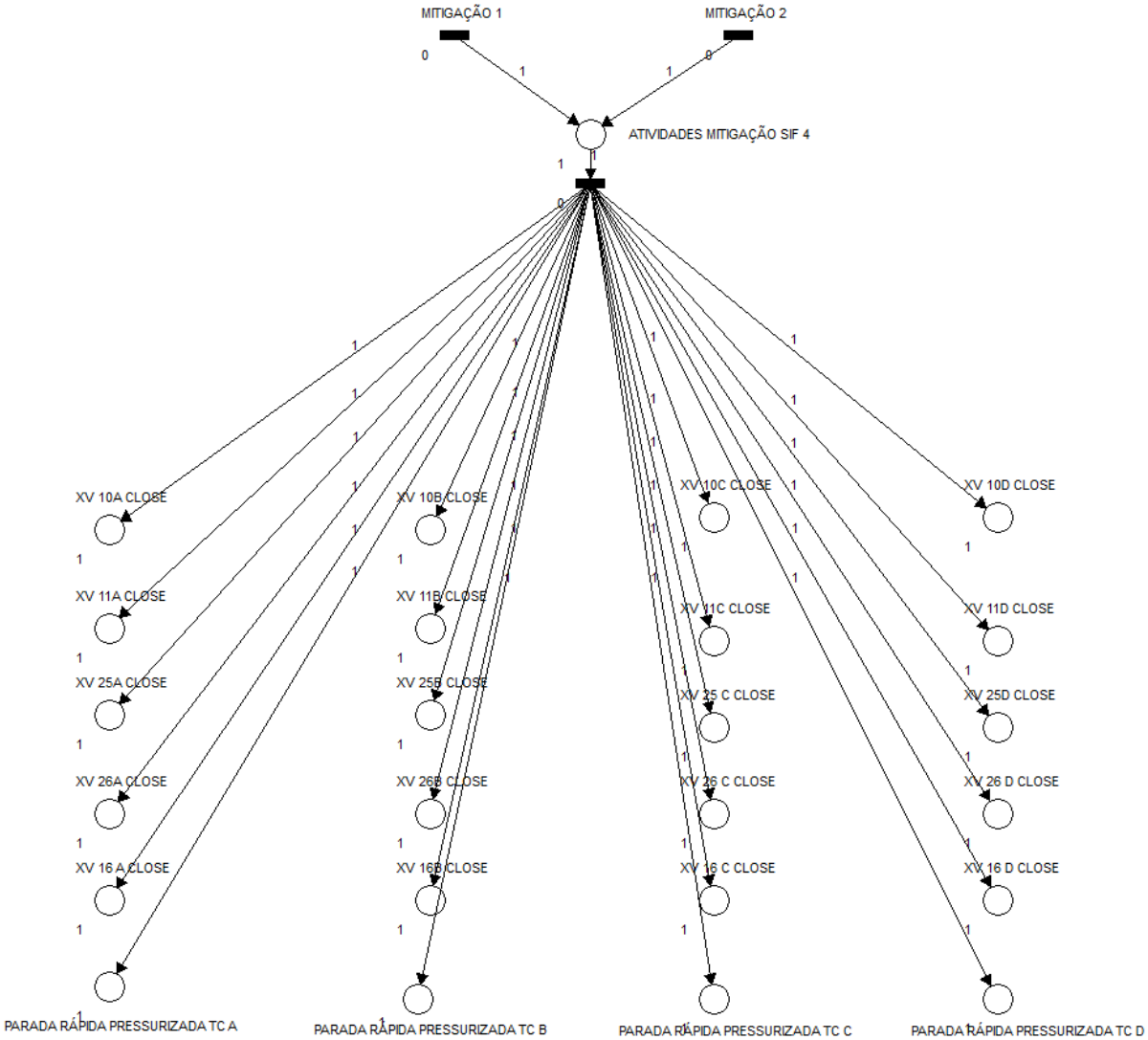



Figura 4.23 – Atividades de mitigação para a SIF 4.

O passo seguinte da sistemática compreende a geração dos algoritmos fuzzy no *toolbox* do software MatLab®.

## 4.2.6 Geração dos algoritmos fuzzy para as SIFs.

Para a implementação da solução de controle é utilizado o toolbox fuzzy do software MatLab®.

A Figura 4.24 ilustra a tela do MatLab® com a solução da SIF 1, composta por 6 entradas e 30 saídas.

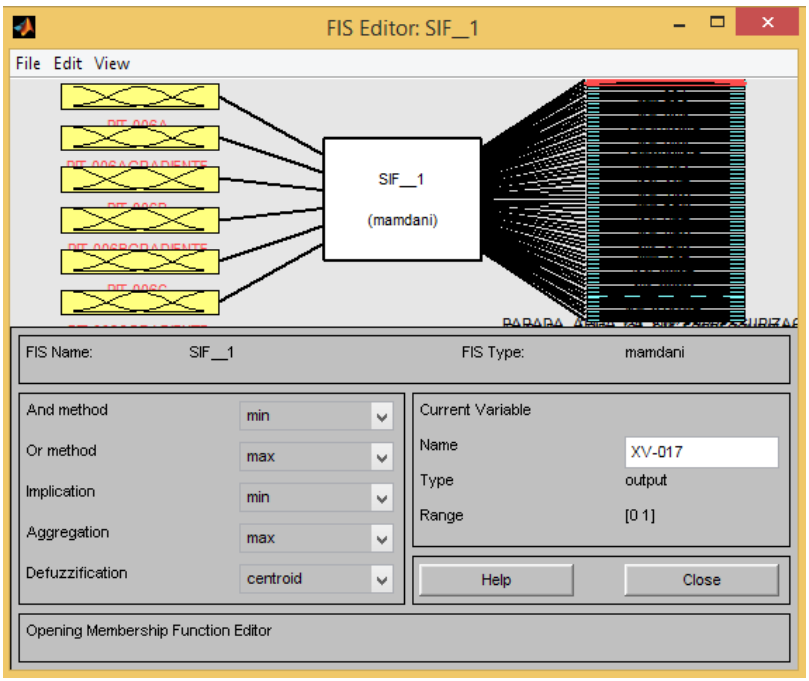



Figura 4.24 – Controlador para a SIF 1 de mitigação.

Para este conjunto de entradas e saídas, e considerando-se os resultados da matriz causa-efeito, além das bases de regras, resultados da aplicação das técnicas de análise de riscos, foram obtidos aproximadamente um total de 18 regras.

Um exemplo de implementação das regras é apresentado na Figura 4.25.

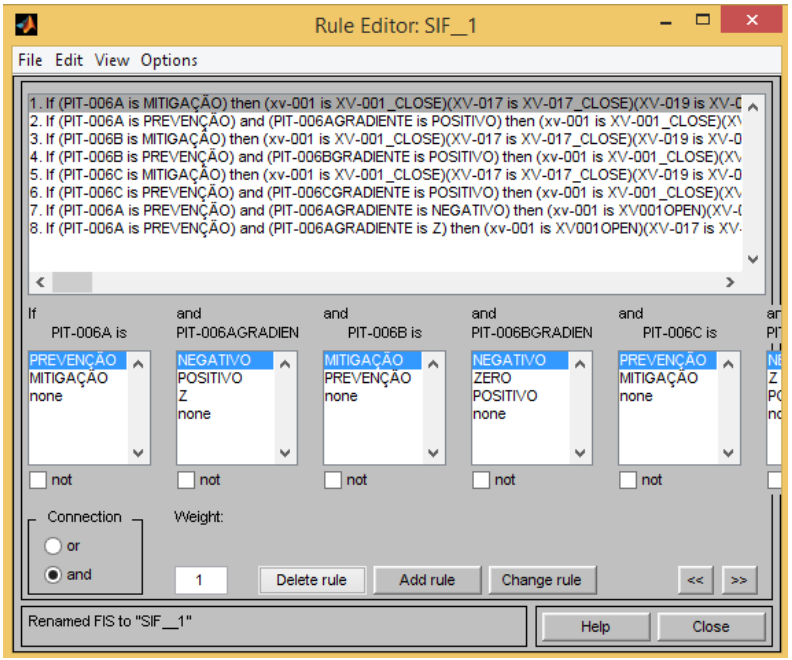



Figura 4.25 – Bases de Regras para a SIF 1 Mitigação.

As demais SIFs da camada de mitigação são implementadas de forma análoga, e o CP de mitigação, contemplando todas as SIFs, pode então ser devidamente programado. Considerando todos os eventos inicializadores, representados pelos respectivos sensores, e os atuadores de mitigação para cada SIF, resultam em uma considerável quantidade de bases de regras, evidenciando a explosão combinatória de estados, representada por meio da **Erro! Fonte de referência não encontrada.**.

## 4.2.7 Códigos de controle com referência à IEC 61131-7.

Fazendo-se uso da IEC 61131-7, que trata de programas em FCL – Fuzzy Control Language em para programas em linguagem ST – Structured Text, definida na IEC 61131-3, tem-se o programa de controle para a implementação em um CP.

# 5. OBSERVAÇÕES FINAIS

Neste trabalho foi proposta uma sistemática para a implantação de uma camada de controle adicional de redução de riscos em sistemas produtivos - SPs, utilizando o conceito de Sistemas Instrumentados de Segurança – SIS, com referência às normas IEC 61508 / IEC 61511. Tal camada é capaz de detectar os efeitos da ocorrência de falhas de elementos críticos de um SP, determinados a partir de resultados de técnicas de análise de riscos, e mitigar tais efeitos de forma antecipatória à ocorrência de catástrofes.

A sistemática baseia-se no ciclo de vida (MIYAGI, 1996) para o projeto e desenvolvimento de um sistema de controle, e adota o conceito de SED, o que permite a utilização de ferramentas para a modelagem e verificação formal de determinadas propriedades, que validam os modelos gerados para controle de um comportamento desejado.

Pelo fato de se ter pouco conhecimento a respeito da dinâmica do SP em estado de falha, foi utilizado o conceito fuzzy para se inferir regras de controle, com base no conhecimento humano, utilizando-se portanto os resultados das técnicas de análise de riscos anteriormente aplicada.

O conjunto de regras fuzzy é implementado em software, e a conversão do modelo para código de controle (IEC 61131-3 (IEC, 2003a)) é feita com referência à IEC 61131-7 (IEC, 2000).

Para ilustrar a aplicação prática da sistemática proposta foi apresentada a implementação da camada SIS de um processo industrial para a efetiva redução do risco inerente de um SP.

Desta forma, pode-se concluir que os objetivos do trabalho foram atingidos, pois com a sistemática proposta tem-se a diminuição do risco, inerente em todo SP, a um nível aceitável, resultando em uma maior segurança para as pessoas, o meio ambiente e às próprias instalações.

## 5.1 Trabalhos futuros

De acordo com todo o exposto, o desenvolvimento do trabalho evidenciou uma série de lacunas, que podem ser desenvolvidas em trabalhos futuros a respeito do tema.

Uma atividade relevante a ser desenvolvida, de acordo com o ciclo de vida de desenvolvimento de sistemas de controle (MIYAGI, 1996), é a fase de testes, operação e manutenção. Para a execução desta fase, são sugeridas as seguintes atividades:

i. Implementação da sistemática proposta em um ambiente real para verificação dos parâmetros de detecção da ocorrência de cada SIF e a efetividade das ações de mitigação propostas. A técnica HIL (*hardware in the loop*) pode ser utilizada, com o uso de conversores analógico-digitais para a simulação das entradas e saídas, e uso da ferramenta Simulink®.
ii. Consideração da evolução temporal das falhas e os possíveis efeitos de causalidade no sequenciamento de ocorrência de falhas, ou seja, o efeito de uma falha gerar a ocorrência de outras falhas.
iii. Estudo sobre o sequenciamento das ações de mitigação necessárias em função do sequenciamento das falhas.
iv. Inclusão do conceito de “barreiras” em função dos resultados obtidos a respeito do sequenciamento de falhas para se evitar o cenário de catástrofe.
v. Pesquisa sobre soluções para o caso do estado de falha sob demanda da camada SIS de mitigação.

# BIBLIOGRAFIA


ABNT. **ABNT NBR 5462 - Confiabilidade e Mantenabilidade**. 1994.

ADAM, N. R.; ATLURI, V.; HUANG, W. K. Modeling and analysis of workflows using Petri nets. **Journal of Intelligent Information System**, 1998. 131-158.

AKHARWARE, N. **PIPE2: Platform independent Petri net editor.** Imperial College of London. [S.l.]. 2005.

ANDRADE, M. T. C. D. **Uma contribuição à pesquisa em inteligência computacional - Tese de Livre Docência**. Escola Politécnica da Universidade de São Paulo. São Paulo. 2002.

ANSCHUETZ, H. HPSim. **HPSim**. Disponivel em: <http://www.winpesim.de/3.html>. Acesso em: 15 out. 2013.

ARATO JR, A. **Manutenção Preditiva**. 1. ed.: Editora Manole, 2003.

ARROFIQ, M.; SAAD, M. **PLC-based fuzzy logic controller for induction-motor drive with contant V/Hz ratio**. ICIAS - International Conference on Intelligent and Advanced Systems. 2007.

ARROFIQ, M.; SAAD, N. **Control of induced motor drives using modified-fuzzy logic methods**. IEEE International Conference on Systems Man and Cybernetics (SMC). 2010.

BELL, R. Introduction to IEC 61508. **Proc. of ACS Workshop on Tools and Standards**, Sydney, Australia, 2005.

BOBBIO, A. **Comparison of methodologies for the safety and dependability assessment of an industrial programmable logic controller**. European Safety Dependability Conf. (ESREL). N. Piccinini and E. Zio. 2001. p. 411-418.

BOJORGE, N. **Sistemas de Segurança e Controle de Prodessos Industriais**. Universidade Federal Fluminense. Rio de Janeiro. 2012.

BRAUER, W.; REISIG, W. Carl Adam Petri and Petri nets. **Informatik-Spektrum**, Heidelberg, v. 29, n. 5, p. 369-381, out. 2006.

CALVEZ, J. P. Embedded Real-Time Systems. In: CALVEZ, J. P. **Embedded Real-Time Systems**. John Wiley & Sons, 1993.

CAO, X. R. A comparison of the dynamics of continuous and discrete event systems. **Proceedings of IEEE**, 77, 1989. 7-13.

CASSANDRAS, C. G. **Discrete Event Systems:** Modeling and performance Analysis. Richard D. Irwin Inc, 1993.

CASSANDRAS, C. G.; LAFORTUNE, S. Introductions to Event Discrete Systems. [s.n.], 1999. p. 822.

CASTRUCCI, P. L.; MORALES, C. **Engenharia de Automação Industrial**. São Paulo. 2001.

CHEN, C.; DAI, J. Design and high-level synthesis of hybrid controller. **IEEE International Conference of Networking, Sensing and Control**, Taipei, Taiwan, 2004.

CHIEN, C. F.; CHEN, S. L.; LIN, Y. S. Using Bayesian network for fault location on distribution feeder. **IEEE Trans. Power Deliv.**, 17, n. 3, 2002. 785-793.

COOPER, G. F.; HERSKOVITS, E. A Bayesian method for the induction of probabilistic networks from data. **Machine Learning**, 9, 1992. 309-347.

CRUZ-CAMPA, H. J.; CRUZ-GOMES, M. J. Determine SIS and SIL using HAZOPS. **Wiley Interscience**, fev. 2009. Disponivel em: <www.interscience.wiley.com>.

CURY, J. E. R. Teoria de controle supervisório de sistemas a eventos discretos. **V Simpósio Brasileiro de Automação Inteligente**, Canela - RS, 2001. 68.

DAVID, R.; ALLA, H. Petri nets for modeling of dynamic systems. **Automatica**, 30, 1994. 175-202.

DEI-SVALDI, D.; VAUTRIN, J. P. Les automates programmables. Nouvelles Technologies, nouveaux risques, príncipes de sécurité à appliquer. **Cashiers de notes documentaires**, 1989. 467-473.

DORF, R. C.; BISHOP, R. H. **Modern Control Systems**. 12. ed. Prentice Hall, 2010.

DUTUIT, Y.; INNAL, F.; RAUZY, A.; SIGNORE, J. P. Probabilistic assessments in relationship with safety integrity levels by using Fault Trees. **Reliability Engineering and System Safety**, 2008.

DUTUIT, Y.; RAUZY, A.; SIGNORE, J. A snapshot of methods and tools to assess safety integrity levels of high-integrity protection systems. **IMechE**, 222, 2008.

EXIDA. **The Exida 61508 Certification Program - FAQ**. 2007.

FALLER, R. Project Experience with IEC 61508 and Its Consequences. **Springer Berlin**, Heidelberg, v. 2187, p. 200-210, 2001.

FERRAREZI, R. C. **Framework para modelagem e verificação formal de programas de controle de Sistemas Instrumentados de Segurança.** Dissertação de Mestrado. Escola Politécnica da Universidade de São Paulo. São Paulo. 2014.

FERREIRA, J.; RIBEIRO, L.; ONORI, M.; BARATA, J. **Challenges and Properties for Bio-inspiration in Manufacturing**. Proceedings of the 5th IFIP WG 5.5/SOCOLNET Doctoral Conference on Computing, Electrical and Industrial Systems, DoCEIS 2014. Costa de Caparica: Springer Berlin Heidelberg. 2014. p. 139-148.

FOGEL, D. B.; FUKUDA, T.; GUAN, L. Scanning the special issue/technology on computation intelligence. **Proceedings of IEEE**, Los Alamitos, 97, 1999. 1414-1422.

FRANKLIN, G. **Feedback Control of Dynamic Systems**. 6. ed. [S.l.]: Prentice Hall, 2009.

GARCIA MELO, J. I.; MORALES, R. A. G.; MIYAGI, P. E. Supervisory system for hybrid productive systems based on Bayesian networks and OO-DPT nets. **IEEE International Conference on Emerging Technologies and Factory Automation, ETFA.**, 2008. 1108-1111.

GOBLE, W. M. Control Systems Safety Evaluation & Reliability. **ISA - The Instrumentation, Systems and Automation Society**, n. 2, 1998.

GOMES, L. F. S. **Redes de Petri Reactivas e Hierárquicas - Integração de Formalismos no Projeto de Sistemas Reactivos de Tempo-Real. Tese de Doutorado.** Faculdade de Ciências e Tecnologia da Universidade Nova de Lisboa. Lisboa, Potugal. 1997.

GUILLEMIN, P. Fuzzy Logic Applied to Motor Control. **IEEE Transactions on industry applications**, 32, 1996. 51-56.

GUO, H.; YANG, X. Automatic creation of Markov models for reliability assessment of safety instrumented systems. **Reliability Engineering and System Safety**, 2007, p. 807-815.

HAMADI, R.; BENATALLAH, B. A. A Petri net-based model for web service composition. **Proceedings of the 14th Australasian Database Conference (ADC´03)**, Adelaide, 2003. 191-200.

HAN, R. A Petri net theory-based method for modeling web service-based systems. **Proceedings of 4th Intern. Conf. on Wireless Communications**, 2008. 1-7.

HELMAN, H.; ANDREY, P. R. P. **Análise de Falhas - Aplicação dos métodos de FMEA e FTA**. Fundação Cristiano Otoni. Belo Horizonte. 1995.

HO, Y. C. Performance evaluation and perturbation analysis of discrete event dynamic systems. **IEEE Transaction on Automatic control**, 32, 1987. 563-572.

HO, Y. C. Introduction to special issue on dynamics of discrete event systems. **Proceedings of IEEE**, 77, 1989. 3-6.

HO, Y. C. Discrete Event Systems Analysing Complexity and Performance in the Modern World, New York, 1992.

IEC. **IEC 61131- Programmable Controllers: part 7 - Fuzzy control programming**. IEC - International Eletrotechnical Comission. 2000.

IEC. **IEC 61882 - Hazard and operability studies (Hazop) - application guide.** IEC - International Electrotechnical Comission. London, UK, p. 58. 2001. (ISBN 0 580 37625 7).

IEC. **IEC 61511 - Safety instrumented systems for the process industry sector**. International Electrotechnical Commission. Geneva. 2003.

IEC. **IEC 61131 Programmable Controllers - part 3: Programming Languages.** IEC - International Eletrotechnical Comission. 2003a.

IEC. **IEC 60812 - Analysis techniques for system reliability - procedures for failure modes and effects analysis (FMEA)**. IEC - International Electrotechnical Commission. Geneva, Switzerland. 2006.

IEC. **IEC 61025 - Fault Tree Analysis (FTA)**. IEC - International Electrotechical Comission. Geneva, Switzerland. 2008.

IEC. **IEC 61508 - Functional safety of electrical/electronic/programmable electronic safety-related systems**. International Electrotechnical Commission. Geneva. 2010.

ISA. **ANSI/ISA-S5.1 — Instrumentation Symbols and Identification**. Instrument Society of America. Research Triangle Park. 1984 (R1992).

ITO, Y. **A Diserable Production Structure Lookin Toward the 21th Century - Anthropocentric Intelligence-Bases Manufacturing.** XI Congresso Brasileiro de Engenharia Mecânica. São Paulo. 1991. p. 23-32.

JENSEN, K. **Coloured Petri Nets:** Basic Concepts, Analysis Methods and Practical Use. Springer-Verlag, v. 1, 1992.

KAMTEKAR, D. M. **Implementation of Functional Safety in a robotic manufacturing cell using IEC 61508 Standard and Siemens Technology**. Rochester Institute of Technology. New York. 2009.

KANESHIRO, P. J.; GARCIA MELO, J. I.; MIYAGI, P. E.; CUGNASCA, C. E. Modeling of collision resolution algorithm in Lonworks Modeling of collision resolution algorithm in Lonworks networks. **Proc. of IMECE´07 the ASME International Mechanical Engineering Congress and Exposition**, Seattle, v. 9, p. 743-749, 2008.

KECECIOGLU, D. **Maintainability, Availability & Operational Readiness Engineering**. 1. ed. [S.l.]: Prentice Hall, v. I e II, 1995.

KELLY, A. **Strategic Maintenance Planning**. 1. ed. Butterworth-Heineman, 2006.

KIEPUSZEWSKI, B.; HOFSTEDE, A. H. M. T.; AALST, W. M. P. V. D. Fundamentals of Control Flow in Workflows. **Acta Informatica**, v. 39, n. 3, p. 143-209, 2002.

LAKATOS, E. M.; MARCONI, M. A. **Metodologia do Trabalho Científico**. São Paulo: Ed. Atlas, 2007.

LEE, C. C. Fuzzy logic in control systems: fuzzy logic controller part II. **IEEE Transactions on System, Man and Cybernetic**, v. 20, p. 419-435, 1990. ISSN 2.

LEE, J. S.; ZHOU, M. C.; HSU, P. L. An Application of Petri nets to supervisory control for human-computer interactive systems. **IEEE Transactions on Industrial Eletronics**, 2005. 1220-1226.

LEVITT, J.; NYMAN, D. **Maintenance Planning, Coordination and Scheduling**. 2. ed. Industrial Press, 2010.

LIU, J.; YUAN, C.; GU, F.; BILLER, S. Functional Safety Certification: Parctice and Issues. **4th IEEE COnference on Automation Science and Engineering**, 2008. 412-417.

LOPEZ ESTRADA, F. R.; PONSART, J. C.; ASTORGA ZARAGOZA, C. M.; THEILIOL, D.; ABERKANE, S. **Fault Diagnosis Based on Robust Observer for Descriptor-LPV Systems with Unmeasurable Scheduling Functions**. The 19th World Congress of the IFAC. Cape Town, África do Sul. 2014. p. 1079-1084.

LUNDTEIGEN, M. A.; RAUSAND, M. Architectural constraints in IEC 61508: Do they have the intended effect? **Reliability Engineering and System Safety**, v. 94, n. 2, p. 520-525, 2009.

MARCOS, J.; ALVAREZ, J.; FERNANDEZ, S. **Design of safety systems with Programmable Logic**. Proceedings of 2th International Conference Ship Propulsion and Railway Traction Systems – SPRTS. Bologna. 2005.

MARSEGLIA, G. R.; SCOTT, J.; MAGNI, L.; BRAATZ, R. D.; RAIMONDO, D. M. **Hybrid Stochastic-Deterministic Approach for Active Fault Diagnosis Using Scenario Optimization**. The 19th World Congress of the IFAC. Cape Town, África do Sul. 2014. p. 1102-1107.

MAZZOLINI, ; BRUSAFERRI, ; CARPANZANO, E. **An Integrated Framework for Model-based Design and Verification of discrete Automation Solutions**. Proceedings 2011 9th IEEE International Conference on Industrial Informatics. Milan: [s.n.]. 2011. p. 545-550.

MIYAGI, P. E. **Controle Programável - Fundamentos do Controle de Sistemas a Eventos Discretos**. São Paulo: Editora Edgard Blücher Ltda,1996, reimpressão 2007.

MODARRES, M. **Risk Analysis in Engineering - Techniques, Tools and Trends**. 1. ed. Florida: CRC Press, 2006.

MODARRES, M.; KAMINSKIY, M.; KRIVTSOV, V. **Reliability Engineering and Risk Analysis:** A Practical Guide. 2. ed. New York: CRC Press, 2009.

MORALES, R. A. G.; GARCIA MELO, J. I.; MIYAGI, P. E. Diagnosis and Treatment of Faults in Productive Systems based on Bayesian Networks and Petri net. **IEEE International Conference on Automation Science and Engineering (Case 7)**, 2007. 357-362.

MOUBRAY, J. **Reliability-Centered Maintenance**. 2. ed. Industrial Press, 2001.

MURATA, T. Petri nets: Properties, analysis and applications. **Proceedings of IEEE**, v. 77, n. 4, p. 541–580, 1989.

NASSAR, M. G. V.; MELO, J. I. G.; MIYAGI, P. E.; SANTOS FILHO, D. Modeling and Analysis of the Material Entry Flow System in a Pickling Line Process using Petri Net. **ABCM Symposium Series in Mechatronics**, v. 3, p. 444-453, 2008.

POPA, D. D. A PI-fuzzy controller designated for industrial motor control. **ISIE IEEE International Symposium on applications.**, 2008.

RAMADGE, P. J.; WONHAM, W. M. Modular supervisory control of discrete-event systems. **Mathematics of Control, Signals and Systems**, 1, n. 1, 1988. 13-30.

RAUSAND, M. **Risk Assessment:** theory, methods, and applications. 1. ed. John Wiley Professional, 2011.

RIASCOS, L. A. M. **Metodologia para detecção e tratamento de falhas em sistemas de manufatura através de rede de Petri**. Tese de Doutorado. Escola Politécnica da Universidade de São Paulo. São Paulo. 2002.

ROUSH, M. **What Every ENgineer Should Know About Risk Analysis**. 1. ed. Marcel Decker, 2000.

ROUVROYE, J. L.; VAN DEN BLIEK, E. G. Comparing safety analysis techniques. **Reliability Engineering and System Safety**, v. 75, n. 3, p. 289-294, 2002.

RU, Y.; HADJICOSTS, C. Fault diagnosis in discrete event systems modeled by Petri nets with outputs. **Proceedings of the 9th International Workshop on Discrete Event Systems**, Goteborg, Sweden, 2008.

SALLAK, M.; SIMON, C.; AUBRY, J. A Fuzzy probabilistic approach for determining safety integrity level. **IEEE Transaction on Fuzzy Systems**, v. 16, p. 239-248, 2008.

SAMPAIO, L. R. **Validação Visual de Programas Ladder Baseada em Modelos**. Dissertação de Mestrado - Universidade Federal de Campina Grande. Campina Grande. 2011.

SANTOS FILHO, D. J. **Aspectos do Projeto de Sistemas Produtivos**. Tese de Livre Docência - Escola Politécnica da Universidade de São Paulo. São Paulo. 2000.

SCHUYLER, J. **Risk and Decision Analysis in Projects**. 2. ed. Project Management Institute, 2001.

SEVERINO, A. J. **Metodologia do Trabalho Científico**. 23. ed. São Paulo: Cortez Editora, 2007.

SIMÕES, M. G.; SHAW, I. S. **Controle e Modelagem Fuzzy**. 2. ed. São Paulo: Edgard Blucher, 2007.

SQUILLANTE JR, R. **Diagnóstico e Tratamento de Falhas Críticas em Sistemas Instrumentados de Segurança**. Dissertação de Mestrado - Escola Politécnica da Universidade de São Paulo. São Paulo. 2011.

SQUILLANTE JR, R.; SANTOS FILHO, D. J.; JUNQUEIRA, F.; MIYAGI, P. E. Development of control systems for safety instrumented systems. **IEEE Latin America Transactions**, v. 9, n. 4, p. 451-457, Julho 2011.

SQUILLANTE JR., R.; SANTOS FILHO, D. J.; SOUZA, J. A. L. D.; MIYAGI, P. E.; JUNQUEIRA, F. **Safety in Supervisory Control for Critical Systems**. Technological Innovation for the Internet of Things. Costa de Caparica: Springer Berlin Heidelberg. 2012. p. 261-270.

SUMMERS, A.; RANEY, G. Commom cause and common sense, designing out of your safety instrumented system (SIS). **ISA Transactions**, 1999. 291-299.

TAKAYAMA, M. A. S. **Análise de Falhas aplicada ao planejamento estratégico da manutenção.** Dissertação de MEstrado. Universidade Federal de Juiz de Fora. Juiz de Fora, MG. 2008.

TSOUKALAS, L. H.; UHRIG, R. E. **Fuzzy and neural approaches in engineering**. Willey-Interscience, 1997.

VILLANI, E. **Abordagem híbrida para modelagem de sistemas de ar condicionado em edifícios inteligentes. Dissertação de Mestrado**. São Paulo: Escola Politécnica da Universidade de São Paulo, 2000.

VILLANI, E.; MIYAGI, P. E.; VALETTE, R. **Modelling and Analysis of Hybrid Supervisory Systems - A Petri Net Approach**. London: Springer-Verlag, 2007.

VILLEMEUR, A. **Reliability, Availability, Maintainability and Safety Assessment**. 1. ed. [S.l.]: John Wiley & Sons, v. 1 e 2, 1992.

WANG, X.; CHEN, G.; XIE, Y.; GUO, Z. Fault detection and diagnosis based on time Petri net. **Proceedings of 8th International COnference on Eletronic Measurement and Instruments**, Beijing, China, 2008.

WU, B.; XI, L. F.; ZHUO, B. H. Service-oriented communication architecture for automated manufacturing system integration. **International Journal of Computer Integrated Manufacturing**, v. 21, n. 5, p. 599-615, 2008.

YOE, C. E. **Principles of Risk Analysis**. Taylor & Francis, v. 1, 2012.

YONEYAMA, T. **Inteligência Artificial em Controle e Automação**. São Paulo: Edgard Blucher, 2000.

YOO, T.; JEONG, B.; CHO, H. A Petri Nets based functional validation for services composition. **Expert Systems with Applications**, v. 37, n. 5, p. 3768-3776, 2010.

ZADEH, L. A. Fuzzy Sets. **Information and Control**, v. 8, p. 338-353, 1965.

ZADEH, L. A. Fuzzy Logic = Computing with Words. **IEEE Transactions on Fuzzy Systems**, 4, 1996. 103-111.

ZHANG, Y.; JIANG, J. Bibliographical review on reconfigurable fault-tolerant control systems. **Annual Reviews in Control 32**, p. 229-252, 2008.

ZHOU, M.; DICESARE, F. **Petri Net Synthesis for Discrete Event Control of Manufacturing Systems**. Boston, MA: Kluwer Ac. Publ., 1993.

ZURAWSKI, R.; ZHOU, M. Petri nets and Industrial Applications: a Tutorial. **IEEE Transactions on Industrial Electronics**, 41, 1994. 567-583.

# ANEXO A - REDE DE PETRI – RdP

A rede de Petri (RdP) é uma representação que pode ser usada tanto no nível conceitual quanto no nível funcional, em que o sistema ou processo podem ser analisados e validados antes de prosseguir com o projeto detalhado e a implementação (ADAM, ATLURI e HUANG, 1998). A RdP é uma ferramenta de comunicação entre as pessoas relacionadas ao projeto, permitindo uma fácil interpretação e nítida identificação dos estados e ações (NASSAR, *et al.*, 2008). Possui a vantagem de um mesmo modelo pode ser usado para a análise das propriedades comportamentais e para avaliação de desempenho, assim como desenvolvimento sistemático de simuladores e controladores (ZURAWSKI e ZHOU, 1994). Possibilita a representação da dinâmica do sistema e sua estrutura em diferentes níveis de abstração (NASSAR, *et al.*, 2008). Pode ser usada para modelar propriedades de sistemas como sincronização de processos, eventos assíncronos, operações concorrentes, conflito ou compartilhamento de recursos, etc. (ADAM, ATLURI e HUANG, 1998) (MURATA, 1989) (ZURAWSKI e ZHOU, 1994). Como ferramenta gráfica, provê um meio de comunicação entre os usuários, como o engenheiro de requisitos, e o cliente (ZURAWSKI e ZHOU, 1994). Matematicamente, a RdP pode ser descrita como um conjunto de equações algébricas lineares e, por isso, pode ser usada para a verificação formal de relações de precedência entre eventos, operações concorrentes, sincronização de processos, inexistência de *deadlock*, atividades repetitivas e exclusão mútua de recursos compartilhados (NASSAR, *et al.*, 2008) (ZURAWSKI e ZHOU, 1994).

Desde sua apresentação por Carl Adam Petri (BRAUER e REISIG, 2006), a RdP tem sido usada na modelagem e análise de diferentes tipos de sistemas e aplicações tais como: protocolos distribuídos (KANESHIRO, *et al.*, 2008), aplicações industriais (ZURAWSKI e ZHOU, 1994) (NASSAR, *et al.*, 2008), diagnóstico e tratamento de falhas (MORALES, GARCIA MELO e MIYAGI, 2007), fluxo de processos (KIEPUSZEWSKI, HOFSTEDE e AALST, 2002), controle supervisório (LEE, ZHOU e HSU, 2005) (GARCIA MELO, MORALES e MIYAGI, 2008) entre outras.

## A.1 Formalização

A RdP proposta inicialmente é chamada de $\text{REDE DE PETRI CONDIÇÃO} - \text{EVENTO}\ (C/E\ \ net)$ e, matematicamente, é descrita como uma 4-tupla:

$PN_{CE} = (P, T, F, M)$

em que

$P$ é o conjunto de elementos passivos chamados de $\text{LUGARES}$,

$T$ é o conjunto de elementos ativos chamados de $\text{TRANSIÇÕES}$,

$F_{ce}$ é o conjunto de relacionamentos entre os elementos passivos e os elementos ativos chamados de $\text{ARCOS ORIENTADOS}$ e

$M_{CE}$ um vetor de recursos chamados de $\text{MARCAÇÃO}$, isto é, um vetor de números binários em que cada elemento $m_i$ indica o número de $MARCAS$ no $LUGAR$ $p_i$, isto é, $m_i = M_{CE}(p_i)$ e, $\forall p\ \in P, M_{CE}(p) \in (0,1)$.

A representação gráfica dos elementos estruturais da RdP é apresentada na Figura A 1:

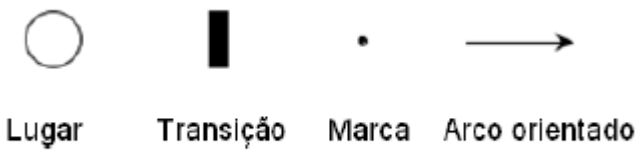



Figura A 1 - Representação gráfica dos elementos da RdP

A Figura A 2 representa um exemplo de modelagem de um SP em RdP:

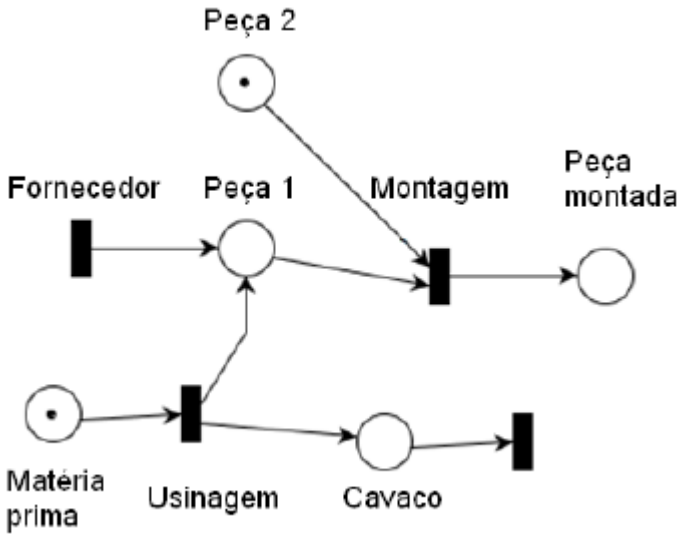



Figura A 2 - Exemplo de RdP como modelo de processo.

$P$ e $T$ são conjuntos finitos, não nulos, $(P \cup T \neq \emptyset)$ e disjuntos $(P \cap T \neq \emptyset)$ ,

$F_{CE} \subseteq (P\ X\ T) \cup (T\ X\ P)$ e

A representação gráfica dos $LUGARES$ da RdP são circunferências; já a representação das $TRANSIÇÕES$ são retângulos sólidos; a representação gráfica dos $ARCOS\ ORIENTADOS$ são setas apontando do elemento de origem para o elemento de destino; e a representação gráfica das $MARCAS$ são circunferências sólidas (círculos) dentro dos $LUGARES$, conforme a Figura A.1.

Os estados do sistema ou processo e sua evolução são representados pela distribuição das $MARCAS$ nos $LUGARES$ da rede. A dinâmica da RdP depende da alteração do estado da RdP, resultante do disparo de seus elementos ativos, isto é, do disparo das $TRANSIÇÕES$. Pode-se assim adotar a ideia de que as $MARCAS$ fluem pela rede direcionadas pelos $ARCOS\ ORIENTADOS$, isto é, fluem de um $LUGAR$ para uma $TRANSIÇÃO$ ou de uma $TRANSIÇÃO$ para um $LUGAR$.

- Para que uma $MARCA$ flua de um $LUGAR$ $p \in P$ para uma $TRANSIÇÃO$ $t \in T$ por um $ARCOS\ ORIENTADO$ $f \in F_{CE}$ , esse $LUGAR$ deve possuir uma $MARCA$, ou seja, $M_{CE}(P) = 1$. Esse $LUGAR$ $p$ é dito então uma pré-condição da $TRANSIÇÃO$ $t$ e sua representação é $p \in \cdot t$, em que $\cdot t$ é o conjunto de pré-condições da $TRANSIÇÃO$ $t$.

- Para que uma $MARCA$ flua de uma $TRANSIÇÃO$ $t \in T$ para um $LUGAR$ $p \in P$ por um $ARCOS\ ORIENTADO$ $f \in F_{CE}$, esse $LUGAR$ não deve possuir $MARCAS$, ou seja, $M_{CE}(P) = 0$. Esse $LUGAR$ $p$ é dito então uma pós-condição da $TRANSIÇÃO$ sua representação é $p \in t \cdot$ em que $t \cdot$ é o conjunto de pós-condições da $TRANSIÇÃO$ $t$.

Quando uma $TRANSIÇÃO$ possui todas as suas pré-condições e pós-condições atendidas essa $TRANSIÇÃO$ é dita habilitada para o disparo. Uma $TRANSIÇÃO$ habilitada pode disparar e esse instante é denominado passo. Quando *t* dispara:

- Todo $LUGAR$ $p_i$ tal que $p_i \in \cdot t$ tem sua $MARCAÇÃO$ alterada entre o passo $k$ e o passo $k + 1$ da seguinte maneira $M_{CE_{K+1}}(p_i) = 0$, e

- Todo $LUGAR$ $p_j$ tal que $p_j \in t \cdot$ tem sua $MARCAÇÃO$ alterada entre o passo $k$ e o passo $k + 1$ da seguinte maneira $M_{CE_{K+1}}(p_j) = 1$.

## A.2 Extensões da RdP

Para ampliar o poder de modelagem da RdP foram posteriormente propostas extensões para acrescentar novas funcionalidades e para simplificação dos modelos. Dentre as extensões, destacam-se a inclusão dos *Arcos Inibidores*, os *Arcos Habilitadores* e as *Temporizações*.

### A.2.1 Arco Inibidor

O Arco Inibidor envolve o conceito de rede dual, derivada em correspondência a cada LUGAR de RdP $C/E\ M(P_1^{'}) = 1$, e se $M(p_1) \neq 0$, então $M(P_1^{'}) = 0$. Assim, ao conectar o LUGAR dual à uma TRANSIÇÃO, esta pode ser entendida como o LUGAR da rede que inibe o disparo da TRANSIÇÃO. O ARCO INIBIDOR é representado graficamente como uma linha com uma circunferência na ponta mais próxima a TRANSIÇÃO, conforme a Figura A 3 - Complemento de arco orientado inibidor.Figura A 3:

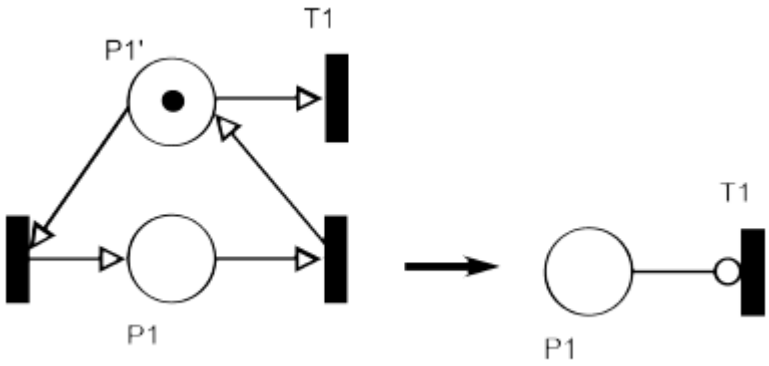



Figura A 3 - Complemento de arco orientado inibidor.

Os ARCOS INIBIDORES também são pré-condições para uma TRANSIÇÃO. Se um ARCO INIBIDOR $f_I$ relaciona o LUGAR $p$ à TRANSIÇÃO $t$, este ARCO determina que a pré-condição da TRANSIÇÃO está atendida apenas na condição de MARCAÇÃO nula, ou seja, $M(p) = 0$. Porém, diferentemente dos ARCOS

ORIENTADOS normais, os ARCOS INIBIDORES não afetam as MARCAS de seus LUGARES.

## A.2.2 Temporizações

Um fenômeno comum em sistemas dinâmicos é o uso de temporizações e agendamentos. A extensão da RdP para representar tal característica é a inclusão de um elemento que incorpora o conceito de tempo, surgindo as RdP temporizadas, em que o modelo possui um contador de tempo que baseia-se na ideia de ciclo de tempo. As RdP temporizadas podem ser de dois tipos: P-temporizadas ou T-temporizadas.

Um ciclo de tempo é estabelecido quando nenhuma TRANSIÇÃO $t \in T$ pode mais disparar. A RdP P-temporizada inclui aos LUGARES da RdP uma propriedade que define quantos ciclos de tempo uma MARCA deve permanecer dentro de um LUGAR antes de poder ser movida devido ao disparo de uma TRANSIÇÃO. A RdP T-temporizada inclui nas TRANSIÇÕES uma propriedade que define por quantos ciclos de tempo as pré-condições e pós-condições devem ser atendidas para que a TRANSIÇÃO dispare. Na RdP T-temporizada, caso uma das pré-condições ou pós-condições não esteja mais atendida durante a contagem de ciclos de tempo, o contador de ciclo de tempo desta TRANSIÇÃO é zerado. Se a TRANSIÇÃO disparar, seu contador de ciclos de tempo também é zerado. A representação gráfica da transição temporizada na RdP T-temporizada pode ser visualizada na Figura A 4:

Figura A 4 - Representação gráfica da transição temporizada na RdP.

## A.3 Propriedades

A verificação de determinadas propriedades podem caracterizar o comportamento dinâmico de uma RdP. As definições das propriedades são baseadas no trabalho de (MURATA, 1989).

### A.3.1 Alcançabilidade

A identificação dos estados alcançáveis de um sistema é fundamental para o estudo das propriedades dinâmicas de qualquer sistema. O DISPARO de uma TRANSIÇÃO habilitada muda a distribuição das MARCAS (ou MARCAÇÃO) DA RdP. Uma sequência de DISPAROS resulta em uma sequência de MARCAÇÕES. Uma MARCAÇÃO $M_n$ é dita alcançável a partir de uma MARCAÇÃO $M_0$ se existir uma sequência de DISPAROS que transforma $M_0$ em $M_n$. Uma sequência de DISPAROS é denotada por $\sigma = M_0 t_1 M_1 t_2 M_2 \dots t_n M_n$ ou simplesmente por $\sigma = t_1 t_2 \dots t_n$. Neste caso, $M_n$ é alcançável a partir de $M_0$ por $\sigma$ e é representado por $M_0[\alpha > M_n]$. O conjunto de todas as possíveis MARCAÇÕES alcançáveis a partir de $M_0$ em uma rede $(P, T_N, T_T, F_N, F_I, M_0)$ é denotado por $R(P, T_N, T_T, F_N, F_I, M_0)$ ou simplesmente de $R(M_0)$.

O problema da alcançabilidade em RdP é saber se $M_n \in R(M_0)$ para uma dada MARCAÇÃO $M_n$. Em algumas aplicações, pode ser interessante fazer o estudo de MARCAÇÕES em um subconjunto específico de LUGARES e não levar em conta o restante da rede. A Figura A 5 apresenta um exemplo de RdP para a verificação da propriedade de *alcançabilidade*:

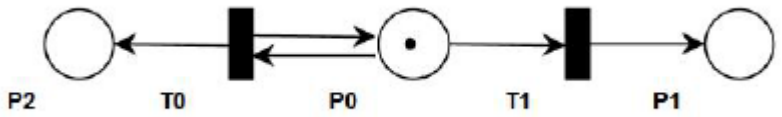



Figura A 5 - Exemplo de RdP para verificação da alcançabilidade.

## A.3.2 Limitabilidade e Segurança

A RdP $(P, T_N, T_T, F_N, F_I, M_0)$ é dita *k*-limitada ou simplesmente limitada se o número de MARCAS em cada LUGAR da rede não exceder um número finito $k$ para qualquer MARCAÇÃO alcançável a partir de $M_0$, ou seja, $\forall p \in P \mid M(p) \leq k$. Uma RdP é dita segura se esta for 1-limitada. Na prática, os LUGARES da RdP são frequentemente usados para representar *buffers* e/ou registradores de dados, itens ou materiais. Assim, assegurar que a rede que modela o sistema é limitada ou segura, é uma forma de garantir que não ocorrerá *overflow* nos *buffers* ou registradores, não importando qual sequência de eventos, isto é, em qual sequência de disparos ocorra. A Figura A 6 mostra um exemplo de RdP para a verificação da propriedade de *limitabilidade* e *segurança.*

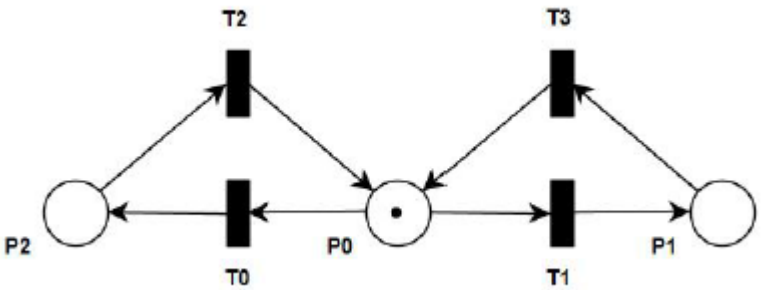



Figura A 6 - Exemplo de RdP para verificação de limitabilidade e segurança.

## A.3.4 Vivacidade

A vivacidade está intimamente relacionada à ausência de *deadlocks* (situações de autrotravamento) na operação de um sistema. Uma RdP é dita viva se,

independentemente de qual MARCAÇÃO é alcançada a partir de $M_0$, é sempre possível disparar qualquer TRANSIÇÃO da rede por alguma sequência de DISPARO. Isto significa que a RdP viva garante a operação com ausência de *deadlocks*, não importa qual sequência de DISPAROS foi seguida.

Vivacidade é a propriedade fundamental para a operação regular de muitos sistemas. Entretanto, a identificação desta propriedade nem sempre é simples e o custo de verificação para alguns sistemas pode ser muito elevado. É possível, então, relaxar a condição de vivacidade e definir diferentes níveis de vivacidade.

Neste sentido, uma TRANSIÇÃO $t$ em uma RdP é dita:

- morta ou L0-viva se nunca pode ser DISPARADA em qualquer sequência de DISPAROS a partir de $M_0$;
- L1-viva (ou potencialmente disparável) se $t$ pode ser DISPARADA ao menos uma vez em alguma sequência de DISPAROS a partir de $M_0$;
- L2-viva se, dado um número inteiro positivo $k$, $t$ pode ser DISPARADO pelo menos $k$ vezes em alguma sequência de DISPAROS a partir de $M_0$;
- L3-viva se $t$ aparece infinitamente, em alguma sequência de DISPAROS a partir de $M_0$;
- L4-viva ou viva se $t$ é L1-viva para qualquer MARCAÇÃO $M$ em $R(M_0)$.

A RdP é dita *Lk*-viva se todas as transições na rede forem *Lk*-vivas, *k=0,1,2,3,4.* A vivacidade L4 é a mais abrangente dos casos e corresponde à definição de vivacidade apresentada inicialmente. É possível verificar que vivacidade L4 implica em vivacidade L3 que implica em vivacidade L2 que implica em vivacidade L1. A Figura A 7 ilustra um exemplo de RdP para a verificação da propriedade de *vivacidade*.

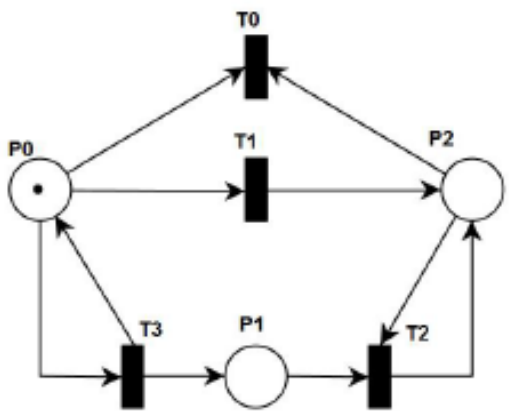



Figura A 7 - Exemplo de RdP para verificação da propriedade de vivacidade.

## A.3.5 Reversibilidade

Uma RdP é dita reversível se, para qualquer MARCAÇÃO $M$ em $R(M_0)$, $M_0$ é alcançável a partir de $M$. Assim, em uma rede reversível é sempre possível se retornar para a MARCAÇÃO inicial ou estado inicial. Em muitas aplicações, não é tão necessário retornar ao estado inicial quanto retornar a um estado desejado. Portanto, a condição de reversibilidade pode ser relaxada pela definição do estado desejado. Uma MARCAÇÃO $M'$ é considerada um estado desejado se, para cada MARCAÇÃO $M$ em $R(M_0)$, $M'$ é alcançável a partir de $M$.

## A.3.6 Cobertura

Uma MARCAÇÃO $M$ em uma RdP é coberta se existe uma MARCAÇÃO $M'$ em $R(M_0)$, tal que $M'(p) \geq M(p)$ para cada $p$ na rede. Cobertura é fortemente relacionada à vivacidade L1. Se $M$ for a MARCAÇÃO mínima para habilitar a TRANSIÇÃO *t* para o seu DISPARO, então *t* é morta se e somente se $M$ não estiver coberta. Ou seja, *t* é L1-viva se e somente se $M$ está coberta.

## A.3.7 Persistência

Uma RdP é dita persistente se, para quaisquer duas TRANSIÇÕES habilitadas, o DISPARO de uma delas não desabilita a outra. Uma TRANSIÇÃO em uma rede persistente, uma vez habilitada, permanece habilitada até que DISPARE. A noção de persistência é útil no contexto de sistemas assíncronos. A persistência é fortemente relacionada a uma rede sem conflitos. Um exemplo de RdP para a verificação da propriedade de *persistência* pode ser verificado na Figura A 8:

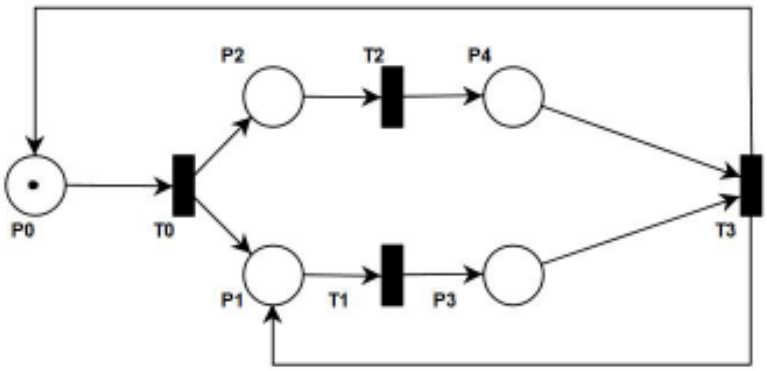



Figura A 8 - Exemplo de RdP para a verificação da propriedade de persistência.

## A.3.8 Distância Síncrona

A distância síncrona é uma métrica fortemente relacionada ao grau de dependência mútua entre duas TRANSIÇÕES em uma RdP. A distância síncrona entre duas TRANSIÇÕES $t_1$ e $t_2$ é definida na RdP como $d_{1\,2} = max\ |\bar{\sigma}(t_1 - \bar{\sigma}(t_2)\ |$, em que $\sigma$ é uma sequência de DISPAROS começando em qualquer MARCAÇÃO $M$ em $R(M_0)\ e\ \bar{\sigma}(t_i)$ é o número de vezes que a TRANSIÇÃO $t_i$, com $i = 1, 2, \ldots$ DISPARA em $\sigma$.

## A.3.9 Equidade

Diferentes noções de equidade foram propostas na literatura de RdP. Aqui serão abordados dois conceitos de equidade: equidade limitada e equidade incondicional (ou global). Duas TRANSIÇÕES $t_1$ e $t_2$ possuem uma relação igual-limitada se o máximo de vezes que uma DISPARAR enquanto a outra não DISPARAR é limitada. Uma RdP é dita igual-limitada se cada par de TRANSIÇÕES desta mantém uma relação igual-limitada. Uma sequência de DISPAROS $\sigma$ é dita incondicionalmente igual se esta é finita ou todas as TRANSIÇÕES da rede aparecem infinitamente em $\sigma$. Uma RdP é dita incondicionalmente igual se todas as sequências de DISPAROS $\sigma$ a partir de $M$ em $R(M_0)$ é incondicionalmente igual. Um exemplo em RdP para a verificação da propriedade de *equidade* pode ser verificado na Figura A 9:

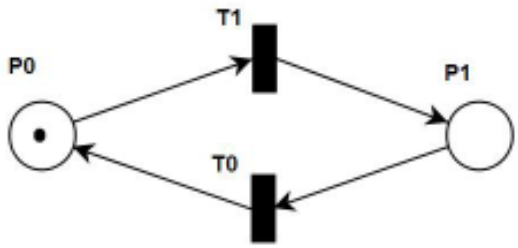



Figura A 9 - Exemplo de RdP para a verificação da propriedade de equidade.

# ANEXO B - MATRIZ CAUSA-EFEITO CASO DE USO 2

# APÊNDICE B - CAMADA SIS DE GÁS E FOGO

Adicionalmente, e com o objetivo de minimizar o risco inerente do processo a um valor aceitável, a camada de mitigação compreende mais duas camadas de proteção, que são as camadas de fogo e de gás, compreendida por sensores e controladores específicos e independentes das outras camadas de proteção, conforme os requisitos das normas IEC 61508 / IEC 61511. Algumas ações de mitigação podem ser comuns às outras camadas, porém as ações de mitigação correspondentes à esta camada são específicas para os respectivos eventos inicializadores.

Ainda de acordo com as referidas normas, não há como atribuir uma função instrumentada de segurança – SIF para esta camada, e nem uma probabilidade de falha sob demanda – PFD, pois os respectivos eventos inicializadores não estão diretamente ligados a desvios de variáveis de processo que poderiam indicar uma ocorrência de falha. Estamos, sim, associando uma camada de proteção adicional caso a camada de mitigação não seja suficiente para evitar o cenário catastrófico ou ainda quando ocorreu alguma falha na ação de mitigação.

Por este motivo, as camadas de gás e fogo, além de atuadores específicos para mitigar os possíveis efeitos da presença de gás e fogo, possuem ações redundantes da camada de mitigação, sendo desempenhadas por um controlador independente.

## B1 Detecção dos efeitos da ocorrência de falhas dos elementos críticos

De acordo com especialistas, e também com pesquisas de *benchmarking*, os sensores para gás e fogo, geralmente utilizando lógica *or* com filtros espúrios, dispostos geograficamente de forma dispersa na planta, de acordo com o devido estudo de análise de risco do processo, utilizam o critério de 20% acima do limiar de não presença de gás e fogo para a detecção, gerando os respectivos alarmes para a planta.

Para valores acima de 20% acima do limiar, é considerada a presença de gás e / ou fogo, iniciando-se as devidas ações de mitigação relativas à esta camada. A

detecção da presença de gás e de fogo são listados na Tabela B 1, com o correspondente TAG, de acordo com a norma ISA S5.1 (ANSI/ISA-S5.1, 1992).

Tabela B 1 - Efeitos da ocorrência de falhas e correspondentes TAGs

| FALHA | TAG do sensor |
|---|---|
| Gás na Casa dos TCs | ASH-201<br>ASH-202<br>ASH-203<br>ASH-204 |
| Fogo na Casa dos TCs | BSH-501<br>BSH-502<br>BSH-503<br>BSH-504 |
| Gás na ERP | ASH-101 |
| Gás na EMED | ASH-102 |
| Gás no P-12002ª | ASH-103ª |
| Gás no P-12002B | ASH-103B |
| Gás na Casa dos MGEs | ASH-505ª<br>ASH-505B |
| Gás no sistema de VAC da Casa de Controle | ASH-506 |
| Gás no P-12001ª | ASH-512ª |
| Gás no P-12001B | ASH-512B |
| Gás no P-12001C | ASH-512C |
| Gás no P-12001D | ASH-512D |

## B2 Ações de mitigação propostas

Para a detecção da presença de gás e de fogo, os resultados das técnicas de análises de riscos sugerem ações de mitigação que podem coincidir com as ações de mitigação da camada SIS de mitigação, representando, portanto, uma ação redundante, que pode ser interpretada como uma falha da camada SIS de mitigação, além de ações adicionais, consequentes dos efeitos da presença de gás e fogo no SP. A Tabela B 2 ilustra os TAGs, de acordo com a norma ISA S5.1 (ISA, 1984 (R1992)) das ações de mitigação propostas e os respectivos atuadores de mitigação da camada SIS de gás e fogo.

Tabela B 2 – Ações de Mitigação para a camada gás e fogo.

| AÇÃO DE MITIGAÇÃO | TAG do atuador |
|---|---|
| Alarme de Abandono na Ecomp | |
| Alarme no Supervisório | |
| Alarme de Emergência | |
| Fecha válvula da sucção 1 (XV-001) da ECOMP | XY-001B |
| Fecha válvula de equalização (XV-017) da XV-001 | XY-017B |
| Fecha válvula da sucção 2 (XV-019) da ECOMP | XY-019B |
| Fecha válvula de equalização (XV-020) da XV-019 | XY-020B |
| Fecha válvula da descarga (XV-003) da ECOMP | XY-003B |
| Fecha válvula de equalização (XV-018) da XV-003 | XY-018B |
| Fecha válvula bloqueio (XV-130) gás partida TCs | XY-130 |
| Fecha válvula bloqueio (XV-101A/B) gás combustível TCs | XY-101A/B |
| Fecha válv bloqueio (XV-102A/B) gás combustível MC-GE | XY-102A/B |
| Fecha válvula bloqueio (XV-127) passo1 P-12002A | XY-127 |
| Fecha válvula bloqueio (XV-129) passo1 P-12002B | XY-129 |
| Fecha válvula bloqueio (XV-126) passo2 P-12002A | XY-126 |
| Fecha válvula bloqueio (XV-128) passo2 P-12002B | XY-128 |
| Fecha válvula bloqueio (XV-104A) passo3 P-12002A | XY-104A |
| Fecha válvula bloqueio (xv-104B) passo3 P-12002B | XY-104B |
| Fecha válvula bloqueio (XV-125) do FT-12002A/B | XY-125 |
| Fecha válvula de bloqueio (XV-510) de ar de serviço | XY-510 |
| AbreXV-004 (BDV) despressurização header 1 | XY-004 |
| Abre XV-021 (BDV) despressurização header 2 | XY-021 |
| Abre XV-002A/B (BDV) despressurização descrga | XY-002A/B |
| Abre XV-116 (BDV) despress gás comb para os TCs | XY-116 |
| Abre XV-131 (BDV) despress gás de partida para os TCs | XY-131 |
| Abre XV-132 (BDV) despress gás de utilidades para os TCs | XY-132 |
| Parada dos motogeradores MC-GE-12001A/B | XS-4100.12102A/B |
| Impede partida dos motogeradores MC-GE-12001A/B | |
| Parada do motogerador afetado | |
| Shutdown Aquecedor P-12002A | |
| Shutdown Aquecedor P-12002B | |
| Parada dos compressores de ar C-12002A/B/C | |
| Fecha válvula bloqueio (XV-010A) entrada do TS-C-12001A | XY-010A |
| Fecha válvula de equalização (XV-011A) da XV-010A | XY-011A |
| Fecha válvula bloqueio (XV-010B) entrada do TS-C-12001B | XY-010B |
| Fecha válvula de equalização (XV-011B) da XV-010B | XY-011B |
| Fecha válvula bloqueio (XV-010C) entrada do TS-C-12001C | XY-010C |
| Fecha válvula de equalização (XV-011C) da XV-010C | XY-011C |
| Fecha válvula bloqueio (XV-010D) entrada do TS-C-12001D | XY-010D |
| Fecha válvula de equalização (XV-011D) da XV-010D | XY-011D |

| | |
|---|---|
| Fecha válvula bloqueio (XV-025A) entrada do TS-C-12001A | XY-025A |
| Fecha válvula de equalização (XV-026A) da XV-025A | XY-026A |
| Fecha válvula bloqueio (XV-025B) entrada do TS-C-12001B | XY-025B |
| Fecha válvula de equalização (XV-026B) da XV-025B | XY-026B |
| Fecha válvula bloqueio (XV-025C) entrada do TS-C-12001C | XY-025C |
| Fecha válvula de equalização (XV-026C) da XV-025C | XY-026C |
| Fecha válvula bloqueio (XV-025D) entrada do TS-C-12001D | XY-025D |
| Fecha válvula de equalização (XV-026D) da XV-025D | XY-026D |
| Fecha válvula bloqueio (XV-016A) saída do TS-C-12001A | XY-016 A |
| Fecha válvula bloqueio (XV-16B) saída do TS-C-12001B | XY-016 B |
| Fecha válvula bloqueio (XV-016C)saída do TS-C-12001C | XY-016 C |
| Fecha válvula bloqueio (XV-016D) saída do TS-C-12001D | XY-016 D |
| Fecha válvula bloqueio (XV-008A) gás partida TS-C-12001A | XY-008A |
| Fecha válvula bloqueio (XV-008B) gás partida TS-C-12001B | XY-008B |
| Fecha válvula bloqueio (XV-008C) gás partida TS-C-12001C | XY-008C |
| Fecha válvula bloqueio (XV-008D) gás partida TS-C-12001D | XY-008D |
| Fecha válvula bloqueio (XV-009A) gás combustível TS-C-12001A | XY-009A |
| Fecha válvula bloqueio (XV-009B) gás combustível TS-C-12001B | XY-009B |
| Fecha válvula bloqueio (XV-009C) gás combustível TS-C-12001C | XY-009C |
| Fecha válvula bloqueio (XV-009D) gás combustível TS-C-12001D | XY-009D |
| Abre XV-012A/B (BDV descarga) do TS-C-12001A | XY-012A/B |
| Abre XV-013A/B (BDV descarga) do TS-C-12001B | XY-013A/B |
| Abre XV-014A/B (BDV descarga) do TS-C-12001C | XY-014A/B |
| Abre XV-015A/B (BDV descarga) do TS-C-12001D | XY-015A/B |
| Parada Rápida do TS-C-12001A (com despressurização) | |
| Parada Rápida do TS-C-12001 B (com despressurização) | |
| Parada Rápida do TS-C-12001 C (com despressurização) | |
| Parada Rápida do TS-C-12001 D (com despressurização) | |

## B3 Elaboração da matriz causa-efeito

Para a elaboração da matriz causa-efeito, são elencados os eventos inicializadores para gás e para fogo, representados nas linhas da matriz por sensores específicos, e as ações de mitigação propostas, representados nas colunas da matriz por atuadores. A matriz causa-efeito para a camada SIS de gás e fogo encontra-se no Anexo C deste trabalho.

## B4 Identificação das SIFs

A partir dos resultados da matriz causa-efeito, as SIFs para gás e fogo são identificadas, com seus respectivos níveis de integridade de segurança SIL. As correspondentes SIFs estão representadas nas Tabelas B1 à B5.

Tabela B 3 – SIF 1 Gás

| | |
|---|---|
| SIF-ID | GÁS 1 |
| Descrição | Gás na Casa dos Compressores |
| SIL | 1 |
| Eventos Inicializadores de Prevenção | ASH 201; ASH 202; ASH 203; ASH 204 ATÉ 20% -> DETECÇÃO DE GÁS |
| Acões de Prevenção | · Parada de emergência dos turbos compressores TC-12001A/B/C/D. |
| Consequencias da falha da prevenção | A PRESENÇA DE GÁS PODE RESULTAR EM EXPLOSÕES NA ECOMP |
| Eventos Inicializadores de Mitigação | INICIALIZADORES DA PREVENÇÃO ACIMA DE 20% OU FAIXA DE 20% COM GRADIENTE POSITIVO -> CONFIRMAÇÃO DA PRESENÇA DE GÁS |
| Acões de Mitigação | Fechar as válvulas: XV-001, XV-017, XV-019, XV-020, XV-003, XV-018, XV-101A/B, XV-102 A/B,XV-125, XV-510, XV-10B, XV-11B, XV-10C, XV-11C, XV-10D, XV-11D, XV-25A, XV-26A, XV-25B, XV-26B, XV-008A, XV-008B, XV-008C, XV-008D, XV-009A, XV-009B, XV-009C, XV-009D, XV-16A, XV-16B, XV-16C, XV-16D, XV-25C, XV-26C, XV-25D, XV-26D, XV-10A, XV-11A |
| Acões de Mitigação | Abrir as válvulas: XV-131, XV-132, XV-116, XV-117, XV-118, XV-119, XV-120, XV-2A, XV-2B, XV-004, XV-021, XV-012A/B, XV-013A/B, XV-014A/B, XV-015A/B<br>PARADA RÁPIDA DOS COMPRESSORES |

Tabela B 4 – SIF 2 Gás

| SIF-ID | GÁS 2 |
|---|---|
| Descrição | Gás na ERP, Gás na EMED, Gás no P-12002A, Gás no P-12002B |
| SIL | 1 |
| Eventos Inicializadores de Prevenção | ASH 101; ASH 102; ASH 103A; ASH 103B ATÉ 20% -> DETECÇÃO DE GÁS |
| Acões de Prevenção | · Parada de emergência dos turbos compressores TC-12001A/B/C/D. |
| Consequencias da falha da prevenção | A PRESENÇA DE GÁS PODE RESULTAR EM EXPLOSÕES NA ECOMP |
| Eventos Inicializadores de Mitigação | INICIALIZADORES DA PREVENÇÃO ACIMA DE 20% OU FAIXA DE 20% COM GRADIENTE POSITIVO -> CONFIRMAÇÃO DA PRESENÇA DE GÁS |
| Acões de Mitigação | Fechar as válvulas: XV-001, XV-017, XV-019, XV-020, XV-003, XV-018, XV-101A/B, XV-102 A/B,XV-125, XV-510, XV-10B, XV-11B, XV-10C, XV-11C, XV-10D, XV-11D, XV-25A, XV-26A, XV-25B, XV-26B, XV-008A, XV-008B, XV-008C, XV-008D, XV-009A, XV-009B, XV-009C, XV-009D, XV-16A, XV-16B, XV-16C, XV-16D, XV-25C, XV-26C, XV-25D, XV-26D, XV-10A, XV-11A |
| Acões de Mitigação | Abrir as válvulas: XV-131, XV-132, XV-116, XV-117, XV-118, XV-119, XV-120, XV-2A, XV-2B, XV-004, XV-021, XV-012A/B, XV-013A/B, XV-014A/B, XV-015A/B<br>PARADA RÁPIDA DOS COMPRESSORES |

Tabela B 5 – SIF 3 Gás

| SIF-ID | GÁS 3 |
|---|---|
| Descrição | Gás nos Motogeradores, Gás no sistema de VAC. |
| SIL | 1 |
| Eventos Inicializadores de Prevenção | ASH-505A; ASH-505B; ASH 506 ATÉ 20% -> DETECÇÃO DE GÁS |
| Acões de Prevenção | · Parada de emergência dos turbos compressores TC-12001A/B/C/D. |
| Consequencias da falha da prevenção | A PRESENÇA DE GÁS PODE RESULTAR EM EXPLOSÕES NA ECOMP |
| Eventos Inicializadores de Mitigação | INICIALIZADORES DA PREVENÇÃO ACIMA DE 20% OU FAIXA DE 20% COM GRADIENTE POSITIVO -> CONFIRMAÇÃO DA PRESENÇA DE GÁS |
| Acões de Mitigação | Fechar as válvulas: XV-001, XV-017, XV-019, XV-020, XV-003, XV-018, XV-101A/B, XV-102 A/B,XV-125, XV-510, XV-10B, XV-11B, XV-10C, XV-11C, XV-10D, XV-11D, XV-25A, XV-26A, XV-25B, XV-26B, XV-008A, XV-008B, XV-008C, XV-008D, XV-009A, XV-009B, XV-009C, XV-009D, XV-16A, XV-16B, XV-16C, XV-16D, XV-25C, XV-26C, XV-25D, XV-26D, XV-10A, XV-11A |
| Acões de Mitigação | Abrir as válvulas: XV-131, XV-132, XV-116, XV-117, XV-118, XV-119, XV-120, XV-2A, XV-2B, XV-004, XV-021, XV-012A/B, XV-013A/B, XV-014A/B, XV-015A/B<br>PARADA RÁPIDA DOS COMPRESSORES |

Tabela B 6 – SIF 4 Gás

| | |
|---|---|
| SIF-ID | GÁS 4 |
| Descrição | Gás em P-12001A, P-12001B, P-12001C, P-12001D |
| SIL | 1 |
| Eventos Inicializadores de Prevenção | ASH-512A; ASH-512B; ASH-512C; ASH-512D ATÉ 20% -> DETECÇÃO DE GÁS |
| Acões de Prevenção | · Parada de emergência dos turbos compressores TC-12001A/B/C/D. |
| Consequencias da falha da prevenção | A PRESENÇA DE GÁS PODE RESULTAR EM EXPLOSÕES NA ECOMP |
| Eventos Inicializadores de Mitigação | INICIALIZADORES DA PREVENÇÃO ACIMA DE 20% OU FAIXA DE 20% COM GRADIENTE POSITIVO -> CONFIRMAÇÃO DA PRESENÇA DE GÁS |
| Acões de Mitigação | Fechar as válvulas: XV-001, XV-017, XV-019, XV-020, XV-003, XV-018, XV-101A/B, XV-102 A/B,XV-125, XV-510, XV-10B, XV-11B, XV-10C, XV-11C, XV-10D, XV-11D, XV-25A, XV-26A, XV-25B, XV-26B, XV-008A, XV-008B, XV-008C, XV-008D, XV-009A, XV-009B, XV-009C, XV-009D, XV-16A, XV-16B, XV-16C, XV-16D, XV-25C, XV-26C, XV-25D, XV-26D, XV-10A, XV-11A |
| Acões de Mitigação | Abrir as válvulas: XV-131, XV-132, XV-116, XV-117, XV-118, XV-119, XV-120, XV-2A, XV-2B, XV-004, XV-021, XV-012A/B, XV-013A/B, XV-014A/B, XV-015A/B<br>PARADA RÁPIDA DOS COMPRESSORES |

Tabela B 7 – SIF 5 FOGO

| | |
|---|---|
| SIF-ID | FOGO |
| Descrição | FOGO NA CASA DOS COMPRESSORES |
| SIL | 3 |
| Eventos Inicializadores de Prevenção | BSH-501; BSH-502; BSH-503; BSH-504 ATÉ 20% -> DETECÇÃO DE FOGO |
| Acões de Prevenção | · Parada de emergência dos turbos compressores TC-12001A/B/C/D. |
| Consequencias da falha da prevenção | A PRESENÇA DE FOGO É UM INDICATIVO IMINENTE DE CATÁSTROFE |
| Eventos Inicializadores de Mitigação | INICIALIZADORES DA PREVENÇÃO ACIMA DE 20% OU FAIXA DE 20% COM GRADIENTE POSITIVO -> CONFIRMAÇÃO DA PRESENÇA DE FOGO |
| Acões de Mitigação | Fechar as válvulas: XV-001, XV-017, XV-019, XV-020, XV-003, XV-018, XV-101A/B, XV-102 A/B,XV-125, XV-510, XV-10B, XV-11B, XV-10C, XV-11C, XV-10D, XV-11D, XV-25A, XV-26A, XV-25B, XV-26B, XV-008A, XV-008B, XV-008C, XV-008D, XV-009A, XV-009B, XV-009C, XV-009D, XV-16A, XV-16B, XV-16C, XV-16D, XV-25C, XV-26C, XV-25D, XV-26D, XV-10A, XV-11A |
| Acões de Mitigação | Abrir as válvulas: XV-131, XV-132, XV-116, XV-117, XV-118, XV-119, XV-120, XV-2A, XV-2B, XV-004, XV-021, XV-012A/B, XV-013A/B, XV-014A/B, XV-015A/B<br>PARADA RÁPIDA DOS COMPRESSORES |

## B5 Modelagem do algoritmo de controle

Para cada SIF identificada na matriz causa-efeito é feita a modelagem em RdP com o auxílio da ferramenta HPSIM / PIPE2, com o objetivo de verificar-se formalmente o modelo em relação às propriedades de *vivacidade, reiniciabilidade e limitabilidade / segurança.* As Figuras B1 à B5 representam os modelos em RdP para o algoritmo de controle da camada SIS de mitigação de gás e fogo.

O modelo em RdP para a detecção e tratamento da SIF GÁS1 é representado na Figura B 1.

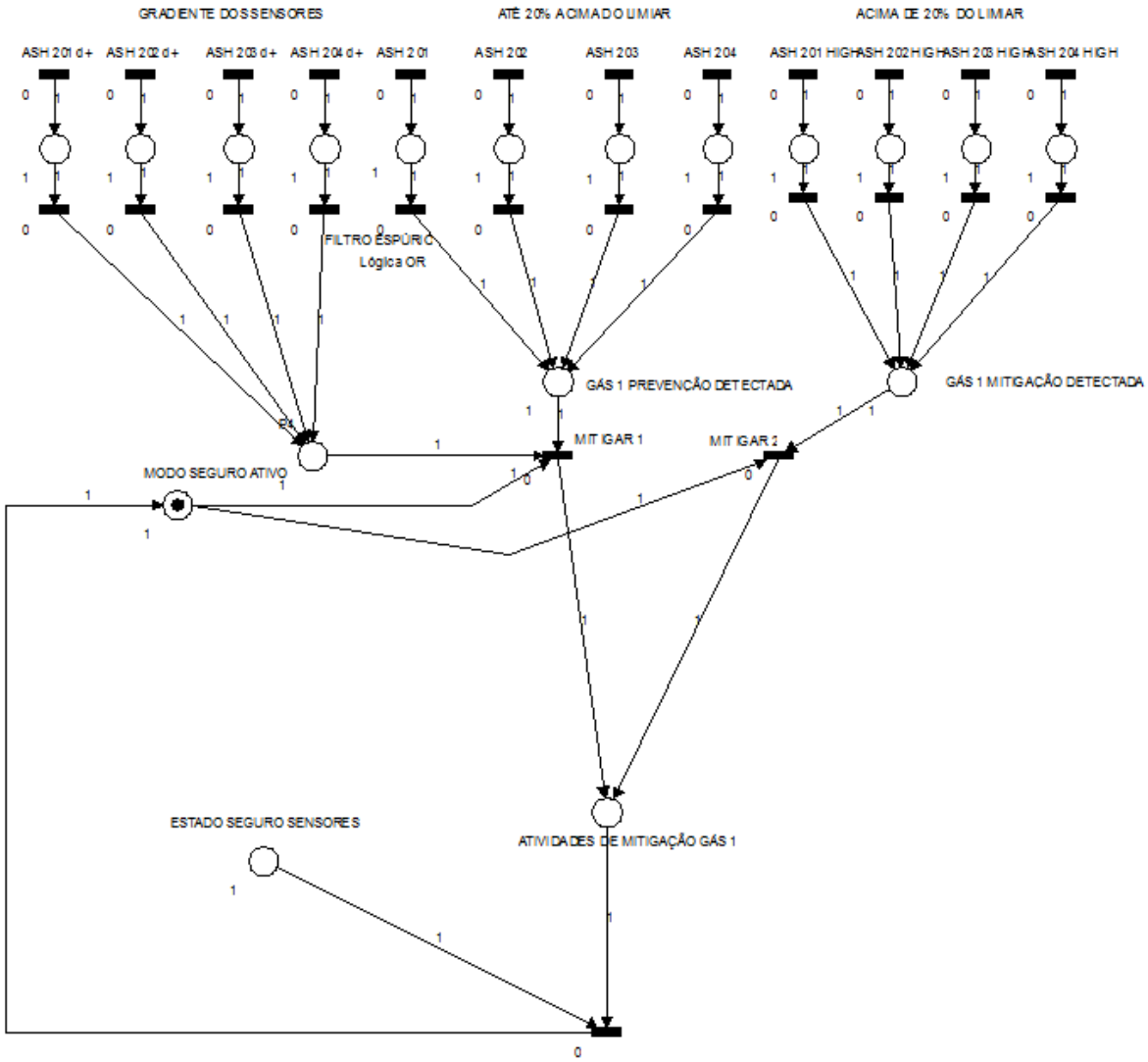



Figura B 1 – Modelo em RdP para detecção e tratamento da SIF Gás1.

O modelo em RdP para a detecção e tratamento da SIF Gás 2 é representado na Figura B 2.

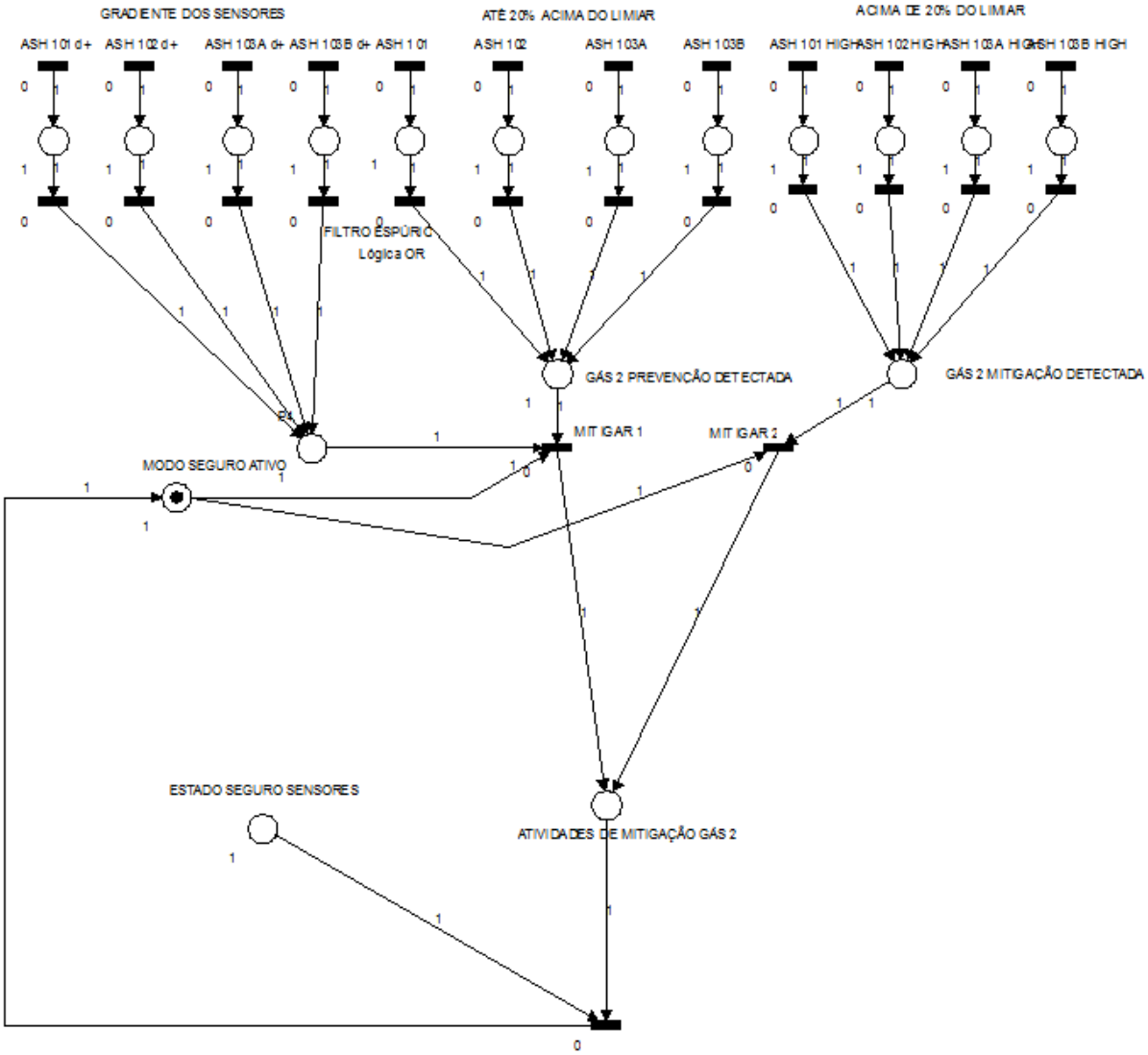



Figura B 2 - Modelo em RdP para detecção e tratamento da SIF Gás 2.

O modelo em RdP para a detecção e tratamento da SIF Gás 3 é representado na Figura B 3.

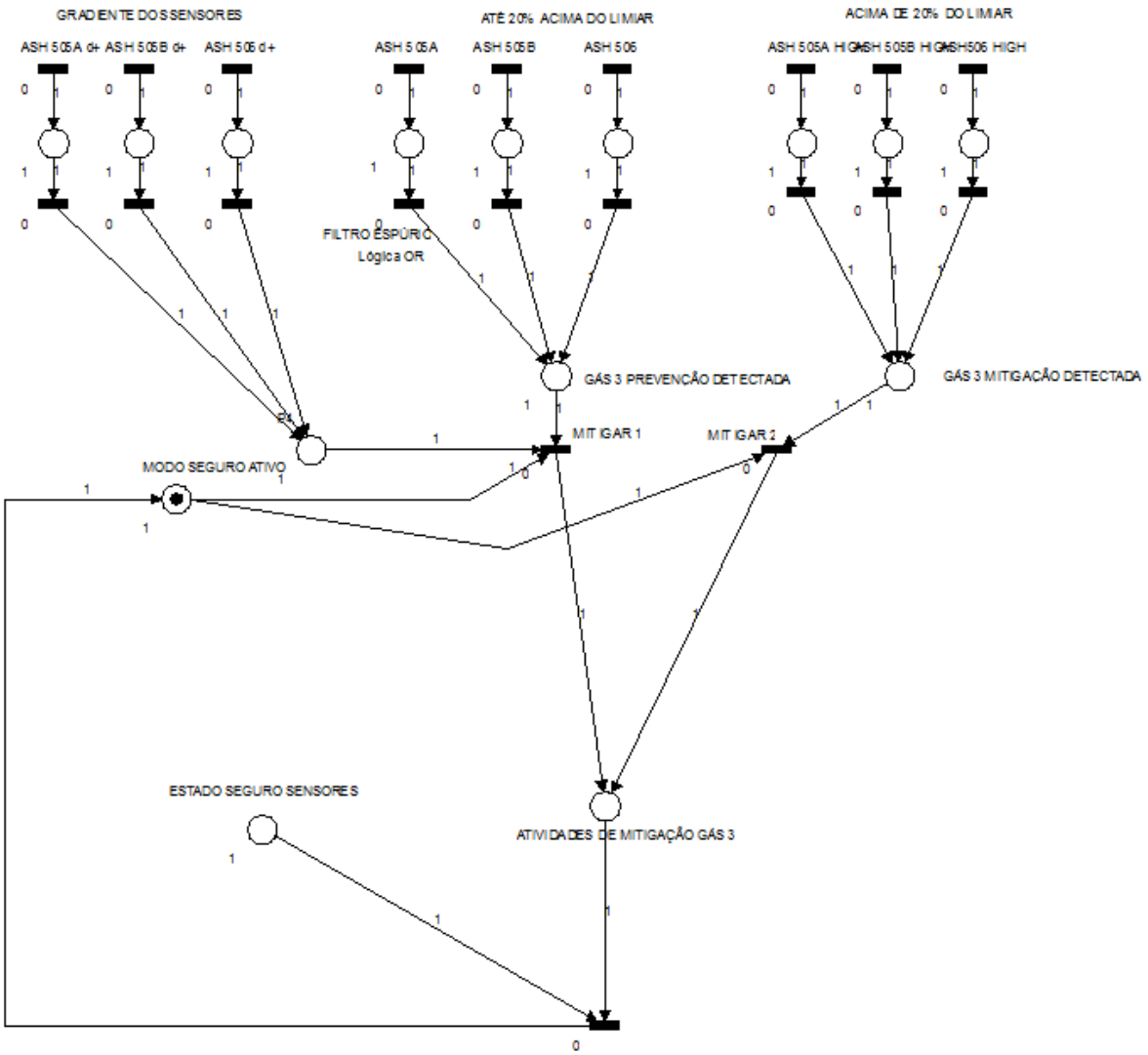



Figura B 3 - Modelo em RdP para detecção e tratamento da SIF Gás 3.

O modelo em RdP para a detecção e tratamento da SIF Gás 4 é representado na Figura B 4.

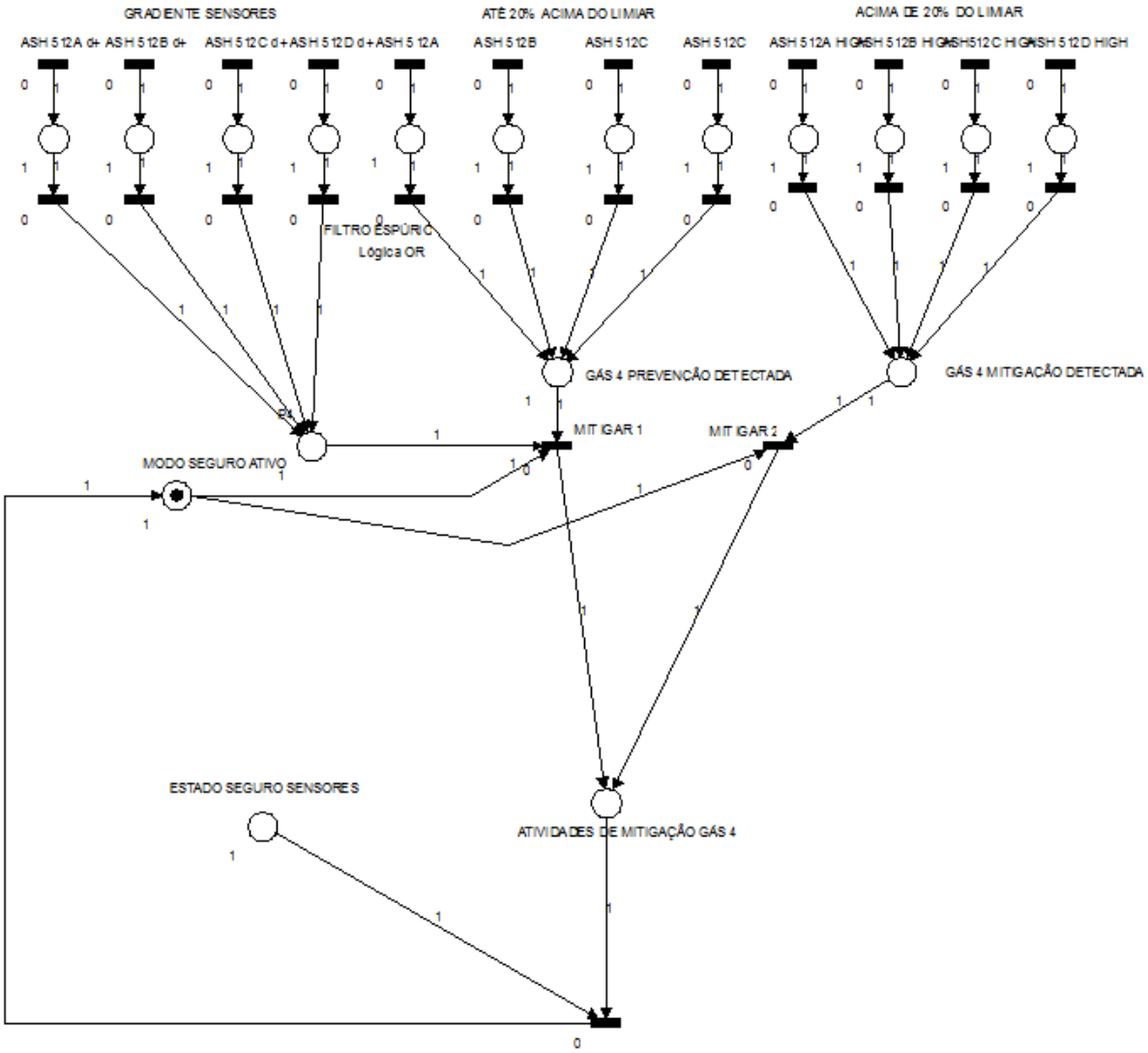



Figura B 4 - Modelo em RdP para detecção e tratamento da SIF Gás 4.

O modelo em RdP para a detecção e tratamento da SIF Fogo é representado na Figura B 5.

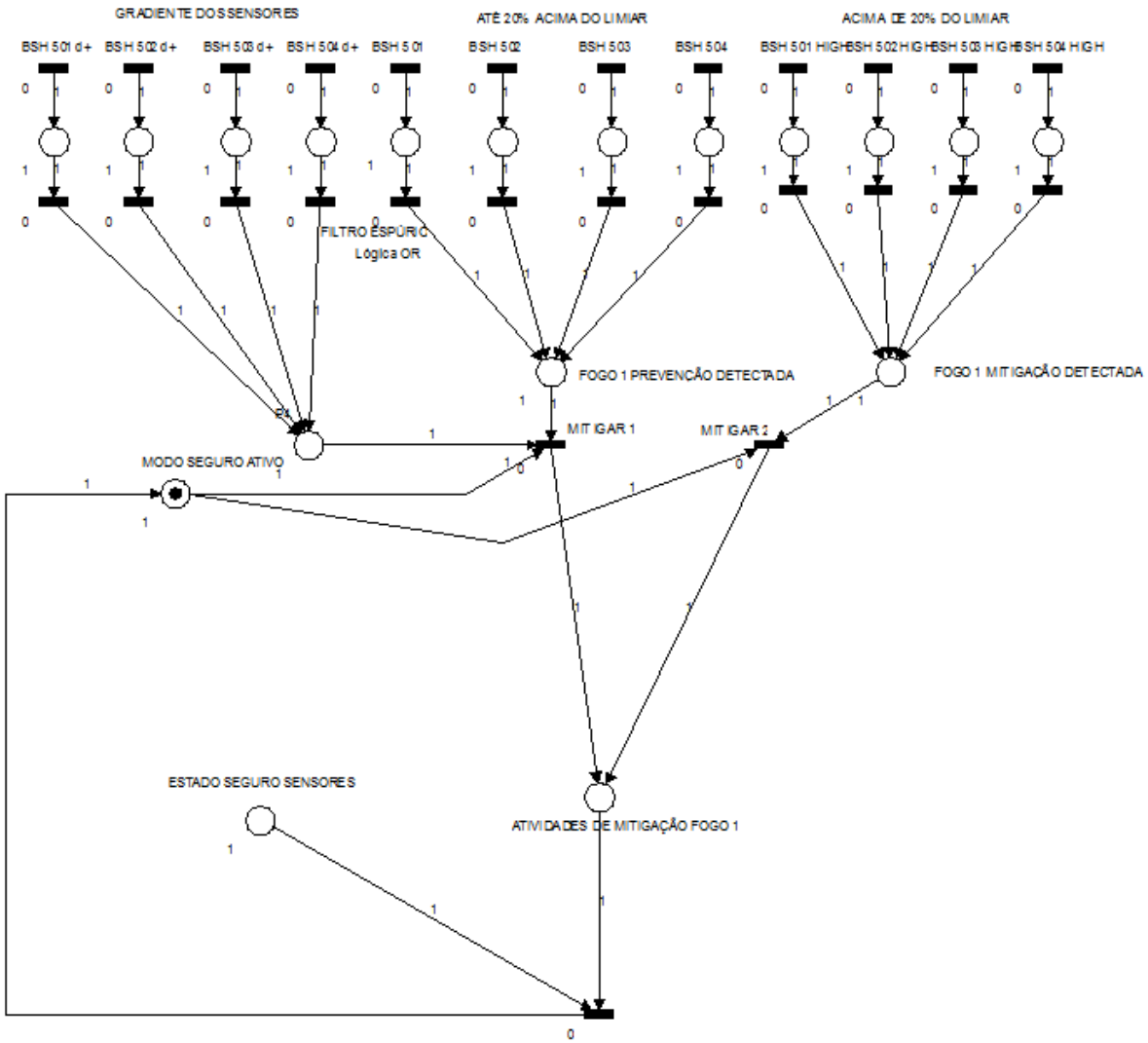



Figura B 5 - Modelo em RdP para detecção e tratamento da SIF Fogo.

## B6 Geração dos algoritmos fuzzy para as SIFs

Para a implementação do próximo passo da sistemática será utilizado o toolbox fuzzy do software MatLab®.

A Figura B 6 ilustra a implementação da SIF Gás 1, composta por 8 entradas e 51 saídas.

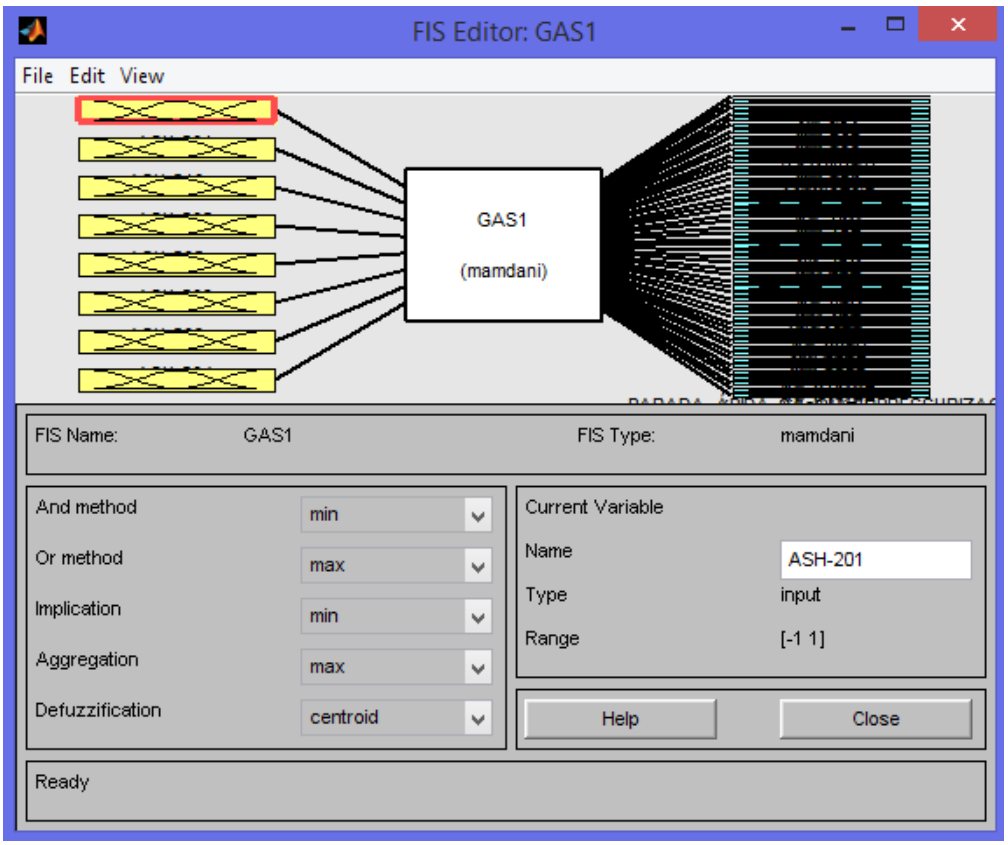



Figura B 6 – Controlador fuzzy para a SIF Gás 1.

Para este conjunto de entradas e saídas, e considerando-se os resultados da matriz causa-efeito, além das bases de regras, resultados da aplicação das técnicas de análise de riscos, foram obtidos aproximadamente um total de 24 regras (apenas para a SIF Gás 1). Um exemplo de implementação das regras é apresentado na Figura B 7.

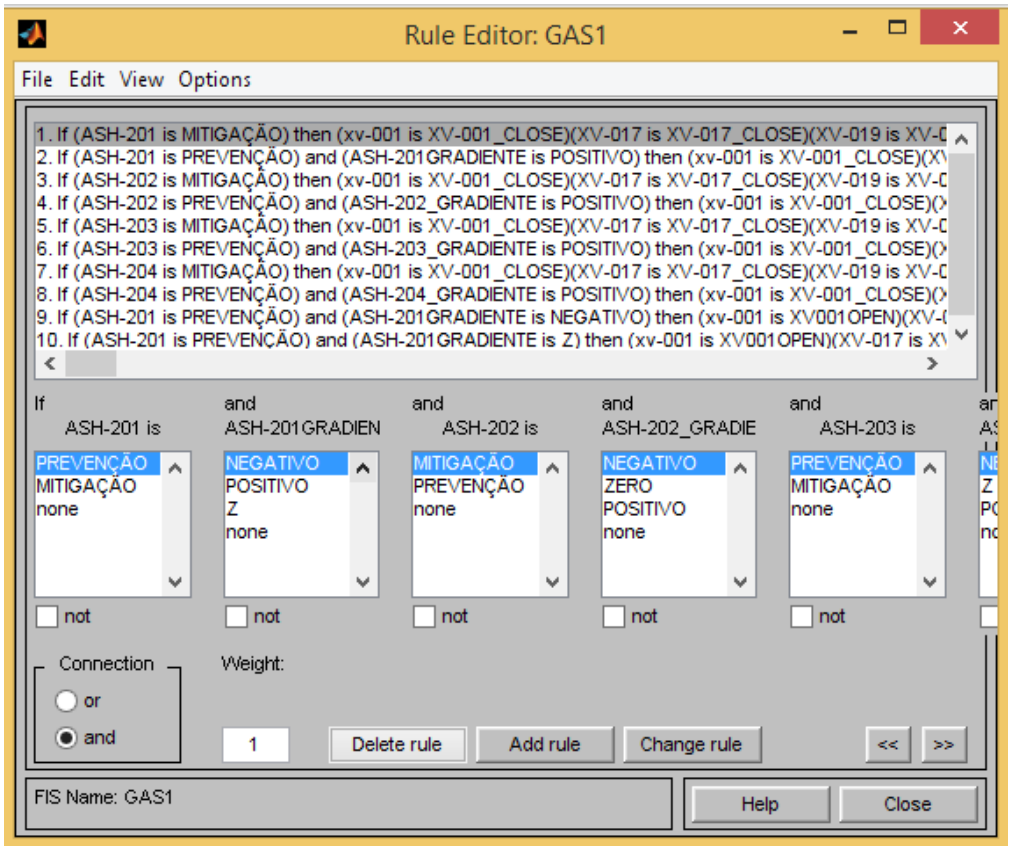



Figura B 7 – Bases de regras para a SIF Gás 1.

A implementação das demais SIFs para gás e fogo são implementadas de forma análoga à da SIF Gás 1, considerando-se os respectivos sensores e atuadores, bem como o conjunto de regras definido para cada SIF.

O CP da camada SIS de mitigação para gás e fogo resulta da implementação de todas as SIFs, ou seja, todos os eventos inicializadores, representados pelos sensores, e todas as ações de mitigação, representados pelos atuadores de mitigação, relacionados pelas respectivas bases de regras.

Como as ações de mitigação podem ser comuns para diferentes SIFs, o conjunto final de bases de regras se torna bastante elevado, evidenciando a explosão combinatória dos estados, decorrente da Equação 1.1, dos elementos presentes na camada SIS de mitigação.

## B7 Códigos de controle com referência à IEC 61131-7

Fazendo-se uso da IEC 61131-7, que trata da conversão da FCL – Fuzzy Control Language em linguagem ST – Structured Text, definida na IEC 61131-3, tem-se o código de controle para a implementação em um CP.

# ANEXO C – Matriz Causa-Efeito Camada SIS Gás e Fogo