REINALDO SQUILLANTE JÚNIOR

DIAGNÓSTICO E TRATAMENTO DE FALHAS CRÍTICAS EM SISTEMAS INSTRUMENTADOS DE SEGURANÇA

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

SÃO PAULO

2011

REINALDO SQUILLANTE JÚNIOR

DIAGNÓSTICO E TRATAMENTO DE FALHAS CRÍTICAS EM SISTEMAS INSTRUMENTADOS DE SEGURANÇA

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
2011

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

São Paulo, de dezembro de 2011.

Assinatura do autor _____

Assinatura do orientador _____

FICHA CATALOGRÁFICA

Squillante Júnior, Reinaldo
Diagnóstico e tratamento de falhas críticas em sistemas instrumentados de segurança / R. Squillante Júnior. – ed. rev. São Paulo, 2011.
158 p.

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

1. Indústrias (Processos) 2. Redes de Petri 3. Falha (Diagnóstico, Tratamento) I. Universidade de São Paulo. Escola Politécnica. Departamento de Engenharia Mecatrônica e de Sistemas Mecânicos II. t.

A minha esposa Sandra
e ao meu filho Stefano como
declaração do meu amor e carinho.

AGRADECIMENTOS

Aqui expresso um profundo sentimento de gratidão, deixando registrado de forma simples, minhas palavras a todos que de forma direta ou indireta, me incentivaram a alcançar este grande passo na minha vida. Primeiramente agradeço a Deus pela minha vida e saúde, permitindo-me atingir este grande objetivo.

Agradeço também o meu orientador Prof. Dr. Diolino José dos Santos Filho, pelo trabalho, esforço e dedicação aplicados e pela pessoa extraordinária que é em todos os sentidos, sempre me incentivando e me encorajando a superar os obstáculos e me mostrando que a vida é um eterno aprendizado e que a humildade é uma das virtudes fundamentais para a obtenção do conhecimento e respeito mútuo.

Sou eternamente grato a minha esposa e companheira Sandra, que me incentivou e sempre me apoiou a atingir este objetivo, e pela imensurável paciência em suportar minha ausência em vários momentos ao longo destes anos, cabendo a ela, a responsabilidade e paciência no cuidado do nosso filho Stefano, o maior presente de Deus.

Agradeço ao Prof. Dr. Paulo Eigi Miyagi, Prof. Dr. Luis Alberto Martinez Riascos e ao Prof. Dr. Fabricio Junqueira pela confiança, interesse, sugestões e apoio fundamentais para o sucesso deste trabalho.

Agradeço também ao Prof. Dr. Newton Maruyama que contribuiu para que meu trabalho pudesse ser publicado na revista IEEE Latino Americana.

Quero expressar também um agradecimento especial ao Engº Roberto Lazzari e a todos meus colegas de trabalho da empresa Unicontrol International Ltda, pelo apoio e incentivo ao desenvolvimento deste trabalho.

Finalizando, agradeço aos eternos amigos do grupo de pesquisas da Mecatrônica; Prof. Dr. José Isidro Garcia Melo e doutorandos MSc Eng. Marcosiris Pessoa, MSc Eng. Caio Fattori, MSc Eng. André Cavalheiros e MSc Eng. Osvaldo Asato, que tanto me incentivaram e me ajudaram no desenvolvimento deste trabalho.

RESUMO

Sistemas Instrumentados de Segurança (SIS) são projetados para prevenir e/ou mitigar acidentes, evitando indesejáveis cenários com alto potencial de risco, assegurando a proteção da saúde das pessoas, proteção do meio ambiente e economia de custos com equipamentos industriais. Desta forma, é extremamente recomendado neste projeto de SIS o uso de métodos formais para garantir as especificações de segurança em conformidade com as normas regulamentadoras vigentes, principalmente para atingir o nível de integridade de segurança (SIL) desejado. Adicionalmente, algumas das normas de segurança como ANSI / ISA S.84.01; IEC 61508, IEC 61511, entre outras, recomendam uma série de procedimentos relacionados ao ciclo de vida de segurança de um projeto de SIS. Desta forma, destacam-se as atividades que compreendem o desenvolvimento e a validação dos algoritmos de controle em que se separam semanticamente os aspectos voltados para o diagnóstico de falhas críticas e o tratamento destas falhas associado a um controle de coordenação para filtrar a ocorrência de falhas espúrias. Portanto, a contribuição deste trabalho é propor um método formal para a modelagem e análise de SIS, incluindo o diagnóstico e o tratamento de falhas críticas, baseado em rede Bayesiana (BN) e rede de Petri (PN). Este trabalho considera o diagnóstico e o tratamento para cada função instrumentada de segurança (SIF) a partir do resultado do estudo de análise de riscos, de acordo com a metodologia de HAZOP (*Hazard and Operability*).

Palavras-chave: sistema instrumentado de segurança, diagnóstico de falha crítica, tratamento de falha crítica, rede Bayesiana, rede de Petri.

ABSTRACT

Safety Instrumented Systems (SIS) are design to prevent and/or mitigate accidents, avoiding undesirable high potential risk scenarios, assuring protection of people health, protecting the environment and saving costs of industrial equipment. It is strongly recommended in this design formal method to assure the safety specifications in accordance to standards regulations, mainly for reaching desired safety integrity level (SIL). Additionally, some of the safety standards such as ANSI/ISA S.84.01; IEC 61508, IEC 61511, among others, guide different activities related to Safety Life Cycle (SLC) design of SIS. In special, there are design activities that involves the development and validation of control algorithm that separate semantically aspects oriented to diagnosis and treatment of critical faults associated with a control coordination to filter spurious failures occurrence. In this context, the contribution of this work is to propose a formal method for modeling and analysis of SIS designed including diagnostic and treatment of critical faults based on Bayesian networks (BN) and Petri nets (PN). This approach considers diagnostic and treatment for each safety instrumented function (SIF) obtained according hazard and operability (HAZOP) methodology.

Keywords: safety instrumented system, critical fault diagnosis, critical fault treatment, Bayesian network, Petri net.

LISTA DE FIGURAS

Figura 1.1 - O SIS e o BPCS como sistemas independentes. 17
Figura 1.2 - Ciclo de vida para desenvolvimento da pesquisa (JENSEN, 1992). 24
Figura 1.3 - Ciclo de desenvolvimento considerado nesta pesquisa. 24
Figura 2.1 - Redução de riscos – conceitos gerais (baseada na Figura A.1 – IEC 61508-5;1998). 29
Figura 2.2 - Camadas de redução de riscos (adaptado da norma IEC 61511-1). 30
Figura 2.3 - Componentes de hardware de um SIS a partir do uso de PES. 31
Figura 2.4 - Arquitetura 1oo1D de um CP de segurança. 36
Figura 2.5 - Arquitetura 1oo2D de um CP de segurança. 37
Figura 2.6 - Arquitetura 2oo2D de um CP de segurança. 38
Figura 2.7 - Arquitetura 2oo3 de um CP de segurança. 39
Figura 2.8 - Normas de segurança vigentes para diferentes segmentos industriais. 40
Figura 2.9 - Ciclo de vida de segurança. Adaptado de (IEC 61508; 1998). 41
Figura 2.10 - Ciclo de vida de segurança. Adaptado de (IEC 61511; 2003). 42
Figura 2.11 - Relação entre as normas IEC 61508 e IEC 61511. Adaptado de (IEC 61511; 2003). 44
Figura 2.12 - Tipos de softwares para SIS. Adaptado de (IEC 61511; 2003). 45
Figura 2.13 - Tipos de linguagens de programação para SIS. Adaptado de (IEC 61511; 2003). 45
Figura 3.1 - Representação gráfica dos elementos de uma PN. 49
Figura 3.2 - Representação da dinâmica da PN, em que (a) é a PN antes do disparo de t e (b) é a PN depois do disparo de t. 50
Figura 3.3 - Exemplo de rede de Petri não limitada (ZURAWSKI; ZHOU, 1994). 51
Figura 3.4 - Exemplo de rede de Petri segura (ZURAWSKI; ZHOU, 1994). 51
Figura 3.5 - Exemplo de rede de Petri reinicializável e viva (ZURAWSKI; ZHOU, 1994). 53
Figura 3.6 - Exemplo de PN com transições com diferentes níveis de vivacidade (ZURAWSKI; ZHOU, 1994). 53
Figura 3.7 - Exemplo de rede de Petri não reinicializável (ZURAWSKI; ZHOU, 1994). 53
Figura 3.8 - (a) arco habilitador (b) arco inibidor. 54
Figura 3.9 - (a) PN antes do disparo de t (b) PN depois do disparo de t. 54

Figura 3.10 - (a) PN antes do disparo de t (b) PN depois do disparo de t. 55
Figura 3.11 - Estrutura de uma BN. 57
Figura 4.1 - Sistemática para o diagnóstico e tratamento de falhas críticas em SIS. 62
Figura 5.1 - Estação de Compressão de Gás – ECOMP. 73
Figura 5.2 - P&ID da linha de sucção 1 na entrada da ECOMP. 74
Figura 5.3 - P&ID da linha de sucção 2 na entrada da ECOMP. 75
Figura 5.4 - P&ID da linha de descarga na saída da ECOMP. 75
Figura 5.5 - Arquitetura do Sistema de Controle da ECOMP. 77
Figura 5.6 - Estrutura inicial da BN construída a partir do algoritmo K2. 81
Figura 5.7 - BN resultante. 82
Figura 5.8 - Modelo em PN interpretada – estrutura efeito → causa. 84
Figura 5.9 - Modelo em PN interpretada – diagnóstico da Falha crítica 1. 85
Figura 5.10 - Modelo em PN interpretada – diagnóstico da Falha crítica 2. 86
Figura 5.11 - Modelo em PN interpretada – diagnóstico da Falha crítica 3. 87
Figura 5.12 - Modelo em PN interpretada – diagnóstico da Falha crítica 4. 88
Figura 5.13 - Modelo em PN interpretada para simulação – diagnóstico da Falha crítica 1. 90
Figura 5.14 - Modelo em PN interpretada para simulação – diagnóstico da Falha crítica 2. 91
Figura 5.15 - Modelo em PN interpretada para simulação – diagnóstico da Falha crítica 3. 92
Figura 5.16 - Modelo em PN interpretada para simulação – diagnóstico da Falha crítica 4. 92
Figura 5.17 - Modelo em PN interpretada – tratamento da Falha crítica 1. 96
Figura 5.18 - Modelo em PN interpretada – tratamento da Falha crítica 2. 97
Figura 5.19 - Modelo em PN interpretada – tratamento da Falha crítica 3. 98
Figura 5.20 - Modelo em PN interpretada – tratamento da Falha crítica 4. 99
Figura 5.21 - Modelo em PN interpretada para simulação – tratamento da Falha crítica 1. 101
Figura 5.22 - Modelo em PN interpretada para simulação – tratamento da Falha crítica 2. 101
Figura 5.23 - Modelo em PN interpretada para simulação – tratamento da Falha crítica 3. 102

Figura 5.24 - Modelo em PN interpretada para simulação – tratamento da Falha crítica 4. 102
Figura 5.25 - Modelos em PN interpretada: Coordenação das (a) Falha crítica 1 e (b) Falha crítica 2. 104
Figura 5.26 - Modelos em PN interpretada: Coordenação das (a) Falha crítica 3 e (b) Falha crítica 4. 105
Figura 5.27 - Modelos em PN interpretada para simulação: Coordenação das (a) Falha crítica 1 e (b) Falha crítica 2. 107
Figura 5.28 - Modelos em PN interpretada para simulação: Coordenação das (a) Falha crítica 3 e (b) Falha crítica 4. 108
Figura 5.29 – Modelo em PN interpretada – SIF-01. 111
Figura 5.30 – Modelo em PN interpretada – SIF-02. 112
Figura 5.31 – Modelo em PN interpretada – SIF-03. 113
Figura 5.32 – Modelo em PN interpretada – SIF-04. 114
Figura 5.33 – Modelo em PN interpretada para simulação – SIF-01. 116
Figura 5.34 – Modelo em PN interpretada para simulação – SIF-02. 117
Figura 5.35 – Modelo em PN interpretada para simulação – SIF-03. 118
Figura 5.36 – Modelo em PN interpretada para simulação – SIF-04. 119
Figura B.1 – Fluxograma de execução do programa de controle. 137
Figura B.2 - Modelo em PN. 138
Figura B.3 - Lógica de habilitação das transições. 138
Figura B.4 - Lógica de disparo das transições. 139

LISTA DE TABELAS

Tabela 1.1 - Especificação de requisitos para algoritmo de controle de um SIS. 19
Tabela 1.2 - Projeto e desenvolvimento de Software – SIS. 20
Tabela 2.1 – Níveis de integridade de segurança (SIL) – (IEC 61508). 33
Tabela 5.1 - Relação causa → efeito. 78
Tabela 5.2 - Descrição das colunas apresentadas na Tabela 5.1. 79
Tabela 5.3 - Sistema de votação “2oo3”. 82
Tabela 5.4 – Elementos do modelo em PN interpretada para Falha 1. 85
Tabela 5.5 – Elementos do modelo em PN interpretada para Falha 2. 86
Tabela 5.6 – Elementos do modelo em PN interpretada para Falha 3. 88
Tabela 5.7 – Elementos do modelo em PN interpretada para Falha 4. 89
Tabela 5.8 – Resumo das “boas propriedades” das PN interpretadas. 93
Tabela 5.9 – Identificação das SIFs. 95
Tabela 5.10 - Elementos do modelo em PN interpretada da Figura 5.19. 96
Tabela 5.11 - Elementos do modelo em PN interpretada da Figura 5.20. 97
Tabela 5.12 - Elementos do modelo em PN interpretada da Figura 5.21. 99
Tabela 5.13 - Elementos do modelo em PN interpretada da Figura 5.22. 100
Tabela 5.14 – Resumo das “boas propriedades” das PN interpretadas. 103
Tabela 5.15 - Elementos do modelo em PN interpretada da Figura 5.25(a). 104
Tabela 5.16 - Elementos do modelo em PN interpretada da Figura 5.25(b). 105
Tabela 5.17 - Elementos do modelo em PN interpretada da Figura 5.26(a). 106
Tabela 5.18 - Elementos do modelo em PN interpretada da Figura 5.26(b). 106
Tabela 5.19 – Resumo das “boas” propriedades das PN interpretadas. 109
Tabela 5.20 – Resumo das “boas propriedades” dos modelos em PN. 120
Tabela B.1 – Lista de entradas e saídas – Diagnóstico da SIF-01 140
Tabela B.2 – Lista de entradas e saídas – Coordenação da SIF-01 141
Tabela B.3 – Lista de entradas e saídas – Tratamento da SIF-01 141

LISTA DE ABREVIATURAS E SIGLAS

ANSI	*American National Standards Institute*
BN	*Bayesian network*
C/E	Condição / evento
C^3I	Sistemas de Comando, Comunicação e Controle Inteligente
CP	Controlador Programável
E/E/EP	Elétrico / eletrônico / eletrônico programável
ECOMP	Estação de Compressão de Gás
FBD	*Function Block Diagram*
FRR	Fator de redução de risco
HAZOP	*Hazard and Operability*
IEC	*International Electrotechnical Commission*
IHM	Interface Homem Máquina
ISA	*The instrumentation, Systems and Automation Society*
ISO	*International Organization for Standardization*
LD	*Ladder Diagram*
LPF	Linguagem de programação fixa
LVC	Linguagem com variabilidade completa
LVL	Linguagem com variabilidade limitada
PES	*Programmable electronic system*
PFD	Probabilidade de Falha em demanda
PN	*Petri net*
BPCS	*Basic Process Control System*
SED	Sistemas a Eventos Discretos
SFC	*Sequential Function Chart*
SIF	*Safety Instrumented Function*
SIL	*Safety Integrated Level*
SIS	Sistemas Instrumentados de Segurança
SVC	Sistemas a variáveis contínuas

LISTA DE SÍMBOLOS

Rede de Petri

P	conjunto finito de lugares da rede de Petri.
T	conjunto finito de transições da rede de Petri.
F	conjunto finito de arcos orientados da rede de Petri.
M_0	conjunto de marcas iniciais nos lugares da rede de Petri.
M	conjunto de marcas nos lugares da rede de Petri.
N	rede de Petri.

Rede Bayesiana

X_i	nó da rede Bayesiana, representado por um círculo.
$pa(X_i)$	nó pai de X_i da rede Bayesiana, representado por um círculo.
$P(X_i \mid pa(X_i))$	probabilidade de X_i ocorrer dado que $pa(X_i)$ ocorreu.
P_rC	probabilidade condicional.
V	conjunto finito de nós da rede Bayesiana.
F	conjunto finito de arcos orientados na rede Bayesiana.
G	estrutura que representa um grafo acíclico orientado.
P	distribuição de probabilidade aplicada à rede Bayesiana.
D	conjunto de dados aplicados à construção da rede Bayesiana.
π_i	representação do conjunto de pais da *i-ésima* variável X_i.
w_{ij}	representação da *j-ésima* configuração dos pais de X_i.
q_i	número total de possíveis configurações dos pais π_i.
N_{ijk}	quantidade total de observações em D onde a variável X_i está no *k-ésimo* estado e seus pais apresentam a *j-ésima* configuração.
c	constante de probabilidade *a priori*, ou seja, $P(G)$.
N_{ij}	número total de observações em D, onde se tem X_i com qualquer um de seus possíveis valores e π_i com a *j-ésima* configuração.

SUMÁRIO

1 INTRODUÇÃO 15
1.1 Motivação 18
1.2 Justificativa 20
1.3 Objetivo 20
1.4 Metodologia de Pesquisa 21
1.4.1 Definição e descrição do problema 21
1.4.2 Hipóteses e pressupostos básicos 22
1.4.3 Definição do tipo de pesquisa 22
1.4.4 Método de investigação 23
1.4.5 Ciclo de vida do projeto de pesquisa 23
1.5 Estrutura do trabalho 25

2 SISTEMA INSTRUMENTADO DE SEGURANÇA 26
2.1 Conceito de Falha crítica 27
2.2 Camadas de redução de riscos 28
2.3 Características de um SIS 31
2.3.1 Função instrumentada de segurança (SIF) 32
2.3.2 Nível de integridade de segurança (SIL) 33
2.3.3 Probabilidade de falha sob demanda (PFD) 33
2.3.4 Fator de redução de risco (FRR) 34
2.4 Controlador Programável de Segurança 35
2.4.1 Arquiteturas do CP de segurança 35
2.5 Normas aplicadas à segurança funcional 39
2.5.1 IEC 61508 40
2.5.2 IEC 61511 e ANSI / ISA SP 84.01 42
2.5.3 Requisitos para o programa de controle de um SIS 44

3 TÉCNICAS UTILIZADAS PARA MODELAGEM E VALIDAÇÃO DE ALGORÍTMOS DE CONTROLE 47
3.1 REDE DE PETRI (pn) 47
3.1.1 Formalização 48
3.1.2 Representação gráfica 49
3.1.3 Propriedades 50
3.2 Rede Bayesiana (BN) 55
3.2.1 Formalização 55
3.2.2 Construção da rede Bayesiana 57
3.2.3 Aprendizagem da estrutura da rede Bayesiana 58

4 SISTEMÁTICA PROPOSTA 61
4.1 apresentação da sistemática 61
4.2 Etapa A1: Modelagem do diagnóstico de falhas críticas 64
4.3 Etapa A2: Modelagem do tratamento e coordenação de falhas críticas 67
4.4 Etapa B: INTEGRAÇÃO E Análise doS modeloS em PN 69
4.5 Etapa C: Geração dos programas baseados nos algoritmos de controle 70
4.6 Etapa D: Testes de aceitação 71

5 APLICAÇÃO DA SISTEMÁTICA PROPOSTA 73
5.1 Descrição do processo 73
5.2 Arquitetura do sistema de controle 76
5.3 Aplicação da sistemática proposta 77
5.3.1 Etapa A1: Modelagem do diagnóstico de falhas críticas 77
5.3.2 Etapa A2: Modelagem de tratamento e coordenação de falhas críticas 93
5.3.3 Etapa B: Análise dos modelos em PN integrados 109
5.3.4 Etapa C: Geração dos programas de controle baseados nos algoritmos de controle 120
5.3.5 Etapa D: Testes de aceitação 121

6 CONCLUSÕES FINAIS 122
6.1 Contribuições do trabalho 123
6.2 Trabalhos futuros 124

REFERÊNCIAS BIBLIOGRÁFICAS 125

ANEXO A 134

ANEXO B 136
B.1 Descrição do método de conversão 137
B.2 Geração do programa de controle da SIF-01 140

1 INTRODUÇÃO

Nesta primeira década do século XXI já se preconizava que os processos de automação vêm sofrendo transformações que têm sido fortemente influenciadas pelo avanço da tecnologia e dos recursos computacionais, tornando-se cada vez mais complexos devidos à sua dinâmica e necessidade de atender aspectos como custos, qualidade, tempos de entrega, flexibilidade na produção e tecnologia usada entre outros fatores (CHEN; DAI, 2004; SANTOS FILHO, 2000; WU et al., 2008).

Uma característica intrínseca a estes processos é a explosão combinatória de estados, em especial nos processos industriais e, quanto maior forem o número de dispositivos independentes presentes no sistema, mais latente é este problema já que o número de estados globais resulta da produtória dos estados locais dos vários dispositivos (MIYAGI, 2007). Diversos trabalhos vêm sendo desenvolvidos com o objetivo de diagnosticar e tratar falhas que estão inseridos neste tipo de problema e que dependem de restringir seu espaço de estados para o controle e tratamento de uma determinada classe de falhas (MORALES; GARCIA MELO; MIYAGI, 2007; RIASCOS, 2002; RU; HADJICOSTIS, 2008; WANG et al., 2007; ZHANG; JIANG, 2008).

Paralelamente, as organizações têm se preocupado em atender políticas de segurança e saúde ocupacional, controlando seus riscos de forma consistente com seus objetivos segundo a norma de Administração de Saúde e Segurança Ocupacional (OSHA[1]). Em caso de qualquer violação da norma, a organização responsável deve ser penalizada por órgãos competentes. Desta forma, a segurança no ambiente de trabalho tem ganhado importância em indústrias de manufatura e de processos (KAMTEKAR, 2009). A norma ISO 14001[2] especifica os requisitos relativos a um sistema de gestão ambiental, permitindo a uma organização formular uma política e objetivos que levam em conta os requisitos legais e as informações referentes aos impactos ambientais significativos. A norma se aplica aos aspectos ambientais que possam ser controlados pela organização e sobre os quais se presume que ela tenha influência.

---

1 OSHA - Norma de Administração de Saúde e Segurança Ocupacional

2 ISO 14001 - Norma que especifica os requisitos relativos a um sistema de gestão ambiental

Neste contexto, se considerar que qualquer processo industrial por mais robusto que seja, mesmo com sistemas de controle reconfiguráveis tolerantes a falhas, pode representar um sério risco com relação à integridade física das pessoas, do meio ambiente e que podem acarretar em perdas econômicas com equipamentos industriais, caso falhas ocorridas durante a dinâmica do sistema não sejam diagnosticadas e tratadas corretamente (SALLAK; SIMON; AUBRY, 2008). A questão passa a ser o reconhecimento de que não existe risco zero nestes sistemas porque os dispositivos físicos não possuem risco de falha nulo, operadores humanos não possuem risco de falha nulo e não há projeto de programas desenvolvidos que possam prever todas as possibilidades.

Desta forma, surgiu o conceito de sistemas instrumentados de segurança (SIS). Segundo especialistas é uma solução para este tipo de questão que envolve a recomendação de uma camada dentro de um sistema hierárquico de controle para a redução de riscos com a finalidade de prevenção de riscos ou para levar o processo a um estado seguro. Um SIS é projetado especificamente para desempenhar funções que mantêm um estado seguro de processo quando condições perigosas ou não aceitáveis[3] são detectadas, garantindo assim a integridade das pessoas, da planta e evitando impactos ambientais (SUMMERS; RANEY, 1999). As normas de segurança, tais como, (ANSI/ISA SP 84.01, 1996; IEC 61508, 1998; IEC 61511, 2003), entre outras, orientam as diferentes atividades relacionadas ao SIS, tais como; projeto, instalação, operação, manutenção, testes, entre outros (LUNDTEIGEN, 2009). Portanto, apesar de existirem normas como a IEC 61131 e IEC 61499 para orientarem o projeto de sistemas de controle para sistemas industriais, existem normas como a IEC 61508 e a IEC 61511 para orientar o projeto de sistemas de segurança para sistemas industriais.

Segundo a IEC 61511-1, o Sistema de Controle de Processo Básico (BPCS) é definido como um sistema que responde a sinais de entrada do processo, sinais dos seus equipamentos associados, outros sistemas programáveis e/ou um operador e gera sinais de saídas fazendo com que o processo e seus equipamentos associados operem de maneira desejável, mas não realizam quaisquer funções instrumentadas de segurança.

---

3 Entende-se por condição não aceitável aquela que promove o sistema a uma situação de risco incompatível com o nível de risco aceitável inerente às normas de segurança que devem ser observadas.

Idealmente, em projetos de sistemas de controle para processos industriais, o SIS deve ser um sistema independente do BPCS (DEI-SVALDI; VAUTRIN, 1989), conforme mostrado na Figura 1.1.

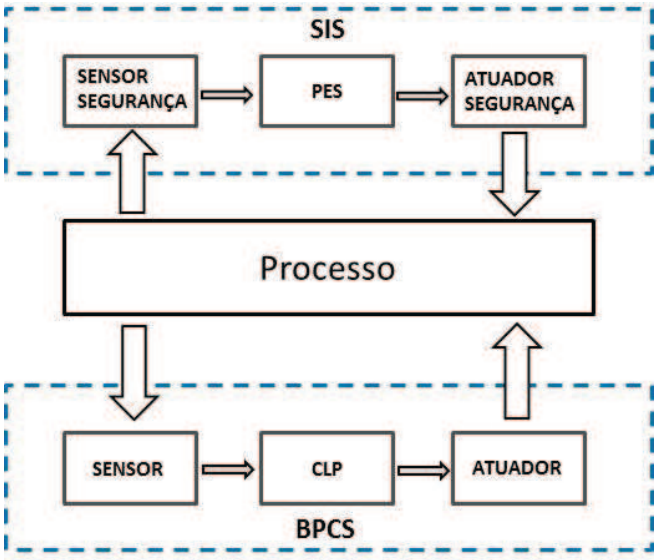


Figura 1.1 - O SIS e o BPCS como sistemas independentes.

De acordo com a norma IEC 61508, as falhas[4] em um processo industrial são identificadas a partir de metodologias classificadas como quantitativas e qualitativas. Uma das metodologias mais utilizadas é a análise de Perigos e Operacionalidade (HAZOP). Ainda segundo a IEC 61508, as falhas são definidas a partir da identificação das funções instrumentadas de segurança (SIF). Logo, uma SIF está associada a uma falha que deve ser diagnosticada e tratada pelo SIS. Um SIS implementa suas SIFs por meio de: (a) da coleta de sinais do processo por um ou mais sensores de segurança, (b) do processamento de informações por um ou mais dispositivos de realização de controle (ex.: equipamentos elétricos, eletrônicos ou eletrônicos programáveis (E/E/EP) onde o mais comum são os sistemas eletrônicos programáveis (PES) ou controladores programáveis de segurança) e (c) do envio de sinais para cada um dos atuadores de segurança. Adicionalmente, para cada SIF é definido um parâmetro chamado de *safety integrated level* (SIL) ou nível de integridade de segurança (STRAVIANIDIS; BHIMAVARAPU, 1998). Este parâmetro é a medida de segurança de componentes e/ou sistemas. O SIL reflete o que os usuários finais esperam de um dispositivo e/ou sistema na sua função de segurança

4 Este conceito está definido no ítem 2.1 do capítulo 2.

e, em caso de falha, que a mesma afete o processo de maneira segura (FALLER, 2001).

No contexto de diagnóstico e tratamento de falhas em processos industriais, as falhas não críticas[5] deverão ser diagnosticadas e tratadas pelo BPCS. As falhas críticas[6] deverão ser diagnosticadas e tratadas pelo SIS, segundo recomendações das normas aplicáveis (IEC 61508, 1998; IEC 61511, 2003).

1.1 MOTIVAÇÃO

Com relação ao diagnóstico e tratamento de falhas aplicáveis aos sistemas de controle tolerantes a falha (FTSC), cuja função é “regenerar” o processo industrial de um estado de falha para um estado normal de operação, Zhang e Jiang (2008) apresentam uma revisão bibliográfica de metodologias e aplicações destes tipos de sistemas de controle.

Por sua vez, vários autores têm abordado as considerações de SIS sob diferentes pontos de vista, como por exemplo, do ponto de vista de hardware de controle, projeto de SIS e metodologias para a determinação e avaliação do SIS e SIL. Bobbio et al. (2001), apresentam uma abordagem utilizando rede de Petri Colorida e rede Bayesiana para a definição do SIL. Em Seixas de Oliveira (2008), é apresentada uma análise de custos baseada na definição do SIL. Adicionalmente, em Dutuit et al. (2008a), é apresentada uma abordagem híbrida envolvendo rede de Petri e simulação e MonteCarlo para a quantificação da confiabilidade do SIS. Cruz-Campa e Cruz-Gomes (2009), apresentam uma metodologia simplificada para a determinação do SIS e cálculo do SIL através do estudo de HAZOP. Em Rouvroye e Bliek (2002), é apresentado um estudo de comparação das diferentes técnicas de análise para determinação da segurança atingida a partir de funções específicas para redução de riscos e propõe uma técnica de análise a partir de cadeias de Markov para a quantificação da segurança atingida pelas funções de redução de riscos instaladas. Dutuit et al. (2008b), apresentam um estudo de avaliação de SIL em SIS por meio de rede de Petri estocástica com predicados. Lundteigen e Rausand (2009), discutem as regras de restrição de arquitetura usadas pelas

5 Este conceito está definido no ítem 2.1 do capítulo 2.

6 Este conceito está definido no ítem 2.1 do capítulo 2.

normas IEC 61508 e IEC 61511 para determinação da conFiguração de hardware do SIS. Guo e Yang (2007) apresentam uma técnica para avaliação da confiabilidade de SIS, por meio da criação de modelos de Markov. Kannan (2007) propõe o uso de rede Bayesiana para criação de um modelo de probabilidade de riscos de uma planta e/ou processo e usa este modelo na fase de desenvolvimento de projeto de SIS. Em Lundteigen; Rausand e Utne (2009) é abordado um modelo para desenvolvimento de produtos considerando a confiabilidade, disponibilidade, manutenção e segurança em projeto de SIS, e integração deste modelo ao ciclo de vida de segurança definido pela IEC 61508.

Portanto, projetos de SIS demandam procedimentos e técnicas para assegurarem o atendimento às especificações de segurança. No entanto, com relação ao sistema responsável pela "degeneração" de forma controlada do processo industrial, não foi encontrada na literatura, uma sistemática ou metodologia para diagnóstico e tratamento de falhas aplicadas a SIS a partir do uso de modelos matemáticos, conforme recomendação da norma IEC 61508. Assim, dentre os trabalhos anteriormente citados, percebe-se uma lacuna com relação ao desenvolvimento de algoritmos de controle para as funções de redução de riscos SIS, onde, segundo as considerações das normas IEC 61508 e IEC 61511, uma abordagem formal é recomendada para o desenvolvimento do algoritmo de controle.

A Tabela 1.1 especifica a pertinência de aplicarem-se métodos matemáticos para o desenvolvimento do algoritmo de controle de um SIS. Adicionalmente, a Tabela 1.2 especifica a pertinência de aplicarem-se técnicas de detecção e diagnóstico de falhas ao projeto de um SIS. As Tabelas 1.1 e 1.2 apresentam quatro níveis de integridade de segurança (SIL 1 até SIL 4) propostos pela IEC 61508 e que serão abordados no próximo capítulo.

Tabela 1.1 - Especificação de requisitos para algoritmo de controle de um SIS.
Fonte: Tabela A.1 – IEC 61508-3 (1998)

Técnica	SIL 1	SIL 2	SIL 3	SIL 4
Métodos matemáticos	R	R	HR	HR

Legenda:

R → recomendado

HR → altamente recomendado

Tabela 1.2 - Projeto e desenvolvimento de Software – SIS.

Fonte: Tabela A.2 – IEC 61508-3 (1998)

Técnica	SIL 1	SIL 2	SIL 3	SIL 4
Detecção e diagnóstico de Falhas	--	R	HR	HR

Legenda:

-- → irrelevante

R → recomendado

HR → altamente recomendado

1.2 JUSTIFICATIVA

Do exposto, considera-se caracterizada a necessidade de se estabelecer uma sistemática para o desenvolvimento do algoritmo de controle a ser inserido na camada de redução de riscos SIS, dentro da estrutura hierárquica de controle de processos industriais. As funções nesta camada devem considerar controladores programáveis de segurança, a partir do desenvolvimento, análise e validação de modelos matemáticos para diagnóstico e tratamento de falhas, conforme recomendação das normas de segurança aplicáveis; justificando a proposta do presente trabalho (IEC 61511, 2003).

1.3 OBJETIVO

Embora exista a especificação de SIL para hardware de sensores de segurança, atuadores de segurança e sistemas eletrônicos programáveis (PES), torna-se fundamental estabelecer uma sistemática baseada em modelos matemáticos como a rede Bayesiana e a rede de Petri para o desenvolvimento, análise e validação de algoritmos[7] de controle inseridos na camada de redução de riscos (SIS) baseada em PES.

7 Sequência finita e não ambígua de instruções computáveis que, aplicadas a um conjunto de dados, conduzem à solução de um problema ou permitem realizar certa tarefa.

Este trabalho visa desenvolver uma sistemática para modelagem de diagnóstico e tratamento de uma classe de falhas em um processo industrial onde se considera uma camada de redução de riscos (SIS) baseada em sistemas eletrônicos programáveis (PES). Neste contexto, este trabalho contempla como ponto de partida, a descrição criteriosa do conceito de falha que está sendo aplicada e como as falhas são classificadas de acordo com o escopo deste trabalho. Na sequência, considera o problema de especificação das funções instrumentadas de segurança (SIFs), com a finalidade de mitigar ou prevenir riscos com acidentes potencialmente altos. Os modelos matemáticos gerados, visam a análise e validação das SIFs e do SIS através de recursos computacionais garantindo uma especificação SIL 3 ou SIL 4 para o algoritmo de controle, de acordo com os requisitos das normas de segurança IEC 61508 e IEC 61511.

1.4 METODOLOGIA DE PESQUISA

A metodologia de pesquisa aplicada neste trabalho foi baseada nas seguintes questões:

- Definição e descrição do problema,
- Hipóteses e pressupostos básicos considerados,
- Definição do tipo de pesquisa,
- Definição do método de investigação,
- Ciclo de vida do projeto de pesquisa.

1.4.1 Definição e descrição do problema

Atualmente, os processos industriais vêm sofrendo transformações, tornando-se cada vez mais complexos. Uma das soluções para se reduzir riscos em processos industriais é a implementação de sistemas de controle de segurança, denominados de SIS. Projetos de SIS demandam a aplicação de métodos matemáticos para assegurar o atendimento às especificações de controle necessárias para garantir os níveis de segurança exigidos pelas normas vigentes como a IEC 61508 e a IEC 61511. Embora os fabricantes de equipamentos eletrônicos programáveis, neste

contexto denominados de Controladores Programáveis (CP) de segurança, tenham desenvolvido tecnologias de hardware robustas com níveis de segurança (SIL) aprovados por órgãos certificadores baseados na norma IEC 61508, resta uma questão a ser resolvida: como assegurar que o projeto de um SIS contemple, além do hardware, um algoritmo de controle que aborde de fato todas as fases de validação, de acordo com a norma, baseando-se em análise formal utilizando modelos matemáticos capazes de lidarem com assincronismos, paralelismos, conflitos e volatilidade de eventos espúrios?

1.4.2 Hipóteses e pressupostos básicos

A fim de assegurar a redução de riscos de processos industriais para níveis aceitáveis definidos por regras corporativas, o projeto de SIS deve contemplar o diagnóstico e tratamento de falhas com o objetivo de prevenção de riscos ou mitigação das consequências provocadas por estes riscos. Desta forma, o desenvolvimento de uma sistemática que utilize modelos matemáticos para o desenvolvimento de algoritmos de controle para diagnóstico e tratamento de falhas, implica na definição de algumas hipóteses:

- ✓ Do ponto de vista de segurança em um processo industrial, as falhas são assumidas como binárias, isto é, apresentam somente dois estados (ex.: 0 / 1; Off / On) (MARCOS; ÁLVAREZ; FERNÁNDEZ, 2001).

- ✓ A abordagem deste trabalho é baseada na caracterização da dinâmica do sistema e orientada pela ocorrência de eventos que podem ser tratados como instantâneos e, portanto, podem ser tratados como SED (Sistema a Eventos Discretos) (MIYAGI, 2007).

- ✓ Para o diagnóstico de falhas, considera-se que está disponível de conhecimento prévio sobre o processo e/ou dados probabilísticos baseados no histórico de ocorrências passadas.

1.4.3 Definição do tipo de pesquisa

A pesquisa, quanto à sua finalidade, foi desenvolvida como pesquisa aplicada, pois o seu resultado fornece para os engenheiros de projetos de sistemas de

controle de segurança, uma sistemática para o desenvolvimento de algoritmos de controle para SIS, baseados em Controladores Programáveis (CP) e que utiliza métodos matemáticos previstos pelas normas IEC 61508 e IEC 61511.

A fonte de dados utilizada para esta pesquisa foi baseada em dados obtidos através de livros, artigos científicos e principalmente nas normas vigentes IEC 61508 e IEC 61511. Adicionalmente, a natureza dos dados obtidos foi qualitativa, onde o objetivo foi identificar as relações causa e efeito para o diagnóstico de falhas e suas consequências a partir de relatório de análise de riscos (HAZOP) e especificações de segurança.

Finalmente, quanto aos objetivos pretendidos, a pesquisa foi descritiva, ou seja, procurou-se definir o problema; descrever em detalhes as partes e suas relações; estudar e aplicar técnicas para solução do problema e produzir uma sistemática e aplicá-la a um estudo de caso real.

1.4.4 Método de investigação

O método de investigação adotado nesta metodologia foi o dedutivo. Foram pesquisadas técnicas de modelagem de sistemas de controle de segurança, no contexto de SED para tratamento de falhas onde foi adotada a rede de Petri. No caso de diagnóstico de falhas, a técnica de modelagem pesquisada baseada em probabilidades foi a rede Bayesiana.

Estas técnicas foram então aplicadas de forma sistemática, para o diagnóstico, coordenação e tratamento de falhas em um estudo de caso real e os resultados atingidos foram analisados e validados de acordo com as especificações técnicas.

1.4.5 Ciclo de vida do projeto de pesquisa

De acordo com Jensen (1992), detalham-se a seguir os aspectos associados às teorias, ferramentas e aplicações envolvidas no desenvolvimento do presente trabalho (Figura 1.2).

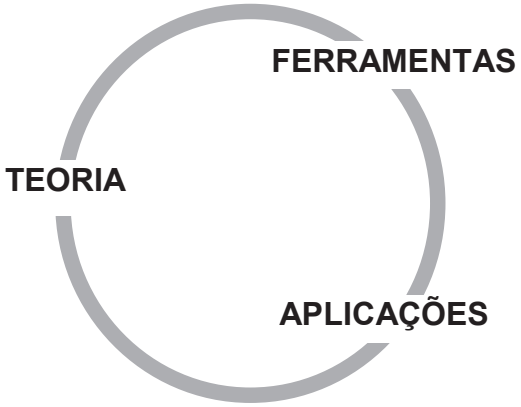


Figura 1.2 - Ciclo de vida para desenvolvimento da pesquisa (JENSEN, 1992).

É uma abordagem de engenharia que, no presente trabalho, considerou os aspectos formais associados à definição de modelos, os métodos de análise aplicáveis graças às ferramentas computacionais existentes e as aplicações em processos industriais como motor de desenvolvimento de novos paradigmas.

Os três aspectos identificados por (JENSEN, 1992) evoluíram simultaneamente, condicionando-se mutuamente. Os desenvolvimentos nas três áreas identificadas se beneficiaram das sinergias resultantes das atividades em cada uma das outras duas áreas.

A Figura 1.3 sintetiza as principais referências do presente trabalho em termos de trilogia apresentada.

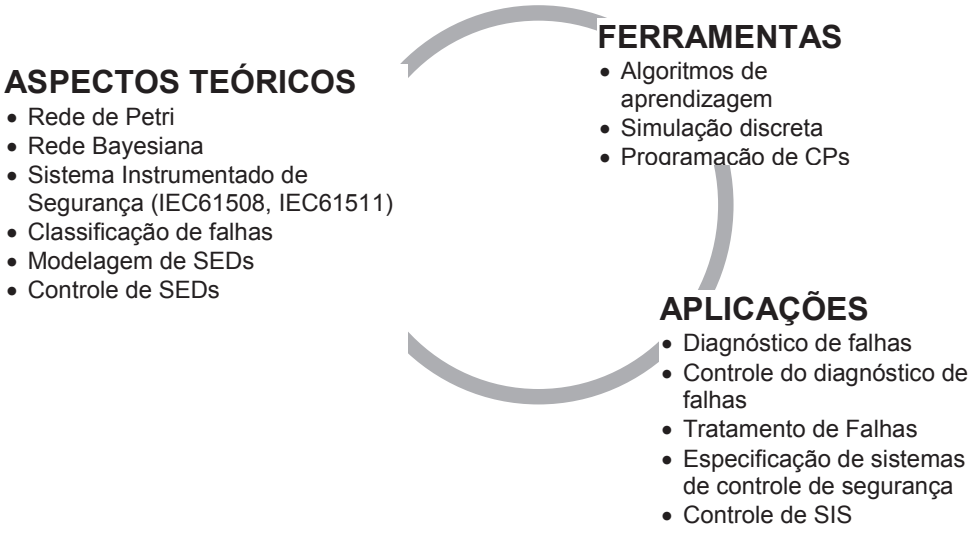


Figura 1.3 - Ciclo de desenvolvimento considerado nesta pesquisa.

1.5 ESTRUTURA DO TRABALHO

No Capítulo 1, apresenta-se inicialmente uma introdução, onde estão descritas as motivações, as justificativas, o objetivo e a metodologia de pesquisa utilizada para a elaboração deste trabalho.

No Capítulo 2, faz-se inicialmente uma discussão a respeito do conceito de falha e propõe-se uma classificação adequada para o contexto deste trabalho. Em seguida apresenta-se uma revisão bibliográfica sobre sistemas instrumentados de segurança (SIS), sobre as normas aplicadas à segurança funcional (ANSI / ISA SP 84.01; 1996; IEC 61508, 1998; IEC 61511, 2003) em indústrias de processo. Finalmente, são apresentados os requisitos para o desenvolvimento de algoritmos de controle de projetos de SIS.

No Capítulo 3, são abordadas as técnicas utilizadas para modelagem e validação de algoritmos de controle para projetos de SIS.

No Capítulo 4, é proposta uma sistemática para desenvolvimento e validação de algoritmos de controle para projetos de SIS, e que aborda a utilização de modelos matemáticos a partir da rede Bayesiana e rede de Petri. Os algoritmos de controle serão implementados em sistemas eletrônicos programáveis (PES) e abordam o diagnóstico, coordenação e tratamento de falhas críticas.

No Capítulo 5, é apresentado um exemplo de aplicação, de uma estação de compressão de gás natural (ECOMP); onde a sistemática proposta é aplicada para o desenvolvimento de algoritmos de controle de diagnóstico, coordenação e tratamento de falhas críticas.

No Capítulo 6 são descritas as principais conclusões e as sugestões que podem contribuir para a evolução deste trabalho. A referência bibliográfica encerra este trabalho.

Há também dois anexos com a seguinte finalidade:

- Anexo A - apresenta o algoritmo K2 utilizado para o exemplo de aplicação da ECOMP.
- Anexo B - apresenta a estrutura de programação e os algoritmos de controle para diagnóstico, coordenação e tratamento da falha crítica – SIF-01, identificada no estudo de caso da ECOMP.

2 SISTEMA INSTRUMENTADO DE SEGURANÇA

Do ponto de vista de segurança em um processo industrial, as falhas são usualmente binárias, isto é, apresentam somente dois estados (ex.: 0 / 1; Off / On) (MARCOS; ÁLVAREZ; FERNÁNDEZ, 2001). A abordagem deste trabalho considera que a dinâmica do sistema, do ponto de vista de segurança, é orientada pela ocorrência de eventos considerados críticos (falhas críticas) e, portanto, podem ser tratados como sistema a eventos discretos (SEDs) permitindo sua modelagem e análise com ferramentas formais, como a rede de Petri (MIYAGI, 2007). A seguir faz-se uma descrição sobre 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) envolvendo 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 (C^3I), etc. (HO, 1987). Neste sentido, CASSANDRAS (1993) apresenta uma classificação de sistemas, que considera os diferentes aspectos que os caracterizam.

A ocorrência de eventos no SED é em geral em intervalos de tempo irregulares e desconhecidos (RAMADGE; WONHAM, 1989) o que caracteriza no sistema um primeiro nível de indeterminismo com relação ao tempo (SANTOS FILHO, 2000). Estes eventos - como a chegada de material, início 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.

Embora a história do controle de SED seja tão antiga quanto ao do controle de SVC (MIYAGI, 2007), o estudo de SED é relativamente recente em relação ao conhecimento alcançado nos SVC. Nota-se que a modelagem matemática do SED ainda está longe de sua consolidação (HO, 1992), (CASSANDRAS; LaFORTUNE,

1999). O problema de controle em SED consiste em estabelecer um conjunto de regras e restrições que permitam ao sistema se comportar segundo uma lógica pré-estabelecida, atuando conforme uma sequência de procedimentos que atendam o objetivo da produção, no caso de sistemas produtivos industriais.

2.1 CONCEITO DE FALHA CRÍTICA

Segurança e confiabilidade são parâmetros essenciais para projetos de sistemas de controle (GOBLE, 1998). Os benefícios econômicos atingidos com projetos de sistemas de controle seguros e confiáveis incluem menor perda de produção, produtos de alta qualidade e redução de custos com riscos.

O parâmetro “confiabilidade” é a medida de sucesso. Confiabilidade geralmente é definida como “a probabilidade que um dispositivo ou componente irá realizar sua função quando for exigido para operar, dentro de limites específicos projetados” (GOBLE, 1998).

O parâmetro “segurança” é a medida da capacidade de um sistema falhar de modo seguro, promovendo um sistema livre de riscos não aceitáveis (GOBLE, 1998; IEC 61511, 2003).

O termo “risco” define uma métrica para quantificação do prejuízo, danos ambientais e perdas econômicas, de forma correlata, ou seja: probabilidade de ocorrência de uma falha e magnitude dos prejuízos ou perdas decorrentes desta falha (BELL, 2005). Assim, risco é medido em termos das consequências para a vida humana, danos ao meio-ambiente e perda de equipamentos. Ainda neste contexto, devemos esclarecer o conceito de falha. O termo “falha” segundo a (IEC 61511, 2003) é definido como uma condição anormal que pode causar uma redução ou perda da capacidade de uma unidade funcional. Neste trabalho, está sendo proposto o termo “falha crítica” como um sinônimo de evento perigoso ou desvio de uma variável controlada de sua faixa de operação segura e que conduz o processo industrial a um risco com magnitude *não aceitável* [8].

8 Por “risco não aceitável” entende-se por aquele que está em desacordo com os regulamentos internos de uma corporação, e/ou das leis regulamentadoras de âmbitos nacional e internacional e/ou das normas contratuais das instituições securitárias.

Neste contexto, é proposta neste trabalho uma classificação das falhas em dois grandes grupos:

- Falhas não críticas: são eventos associados a riscos de magnitude *aceitável*, ou seja, o comportamento especificado do sistema/processo pode ser recuperado de forma automática pelo sistema de controle de processo básico (BPCS), que pode envolver intervenção de operadores humanos, para que o processo industrial possa ser regenerado de forma controlada para um estado normal de operação.

- Falhas críticas: são eventos associados a riscos de magnitude *não aceitável* e que devem ser prevenidos ou mitigados, a fim de evitar um cenário catastrófico, podendo ocasionar fatalidades humanas e danos ao meio ambiente. Neste contexto, o processo industrial deverá ser degenerado de forma controlada, por ação de um sistema de controle específico, para um estado seguro.

As falhas consideradas criticas, do ponto de vista de segurança em um processo industrial, são usualmente binárias, isto é, apresentam somente dois estados (ex.: 0 / 1; Off / On) (MARCOS; ÁLVAREZ; FERNÁNDEZ, 2001). A abordagem deste trabalho considera que a dinâmica do sistema, do ponto de vista de segurança, é orientada pela ocorrência de eventos considerados críticos (falhas críticas) e, portanto, podem ser tratados como sistemas a eventos discretos (SEDs) permitindo sua modelagem e análise com ferramentas formais, como a rede de Petri (MIYAGI, 2007).

2.2 CAMADAS DE REDUÇÃO DE RISCOS

Existe sempre certo risco na operação de processos industriais. Algumas vezes este risco é inaceitável devido sua magnitude. Desta forma, a redução da magnitude dos riscos poderá ser exigida por regras corporativas, leis regulamentadoras e companhias de seguro. Isto faz surgir um conceito de risco aceitável. Quando um risco inerente é maior que o risco aceitável, então é exigida a redução deste risco (GOBLE, 1998).

Com o objetivo de reduzir os riscos em processos industriais, camadas individuais de redução de riscos podem ser empregadas dentro de uma estrutura

hierárquica de controle. Estas camadas de redução são dispositivos, sistemas ou ações capazes de prevenir um cenário de consequências indesejáveis. Elas são independentes do evento inicial e ação ou falha de qualquer outra camada de redução associada a este cenário (CRUZ-CAMPA et al.; 2009).

A Figura 2.1 mostra a redução do risco inicial de um processo industrial ao nível de risco aceitável. O objetivo de uma corporação é ajustar os seus processos industriais de tal forma que o risco inerente fique abaixo do risco aceitável, restando sempre um risco residual, uma vez que é impossível do ponto de vista prático, a situação de sistema infalível e de risco zero. Portanto, outras camadas podem ser empregadas para a redução do risco, como por exemplo, através do uso de outras tecnologias relacionadas à segurança (exemplo: válvulas de alívio, etc.) ou através de facilidades externas (ex: barreiras ou diques de contenção, invólucros ou compartimentos à prova de explosão, etc.). O foco do presente trabalho concentra-se na camada de redução de riscos associada à implantação de um sistema instrumentado de segurança (SIS).

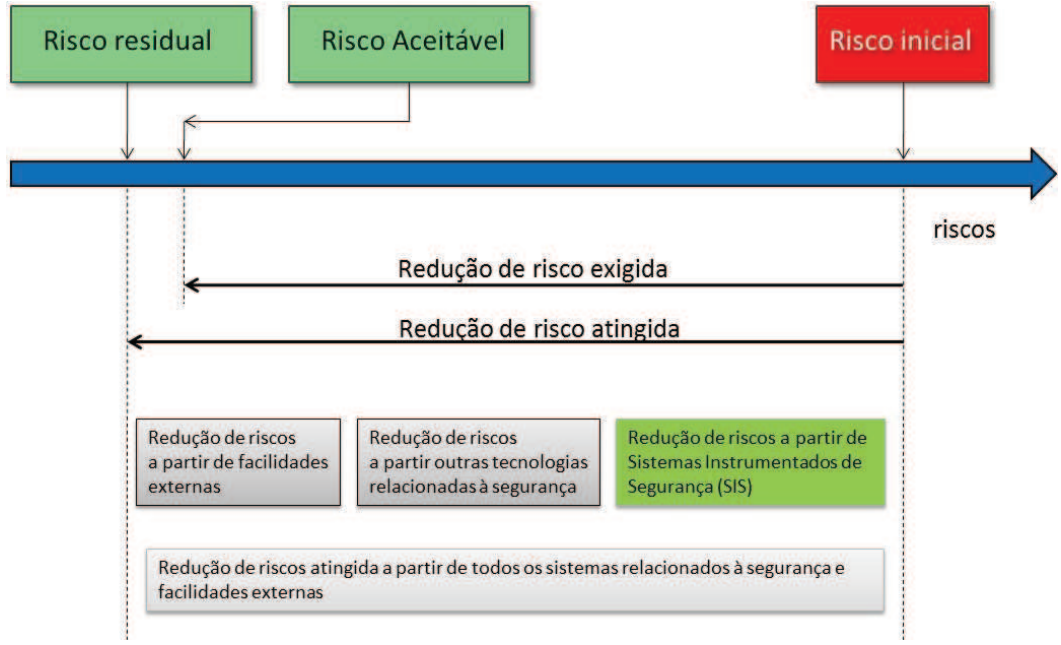


Figura 2.1 - Redução de riscos – conceitos gerais (baseada na Figura A.1 – IEC 61508-5;1998).

A estratégia de prevenção de acidentes começa no projeto da instalação que deve ser inerentemente segura. Entretanto, alguns processos industriais se tornam perigosos em determinadas situações que saem de controle por algum motivo como: elevadas temperaturas ou altas pressões. Além disso, quando se trata de

substâncias inflamáveis e/ou tóxicas, nem sempre uma instalação inerentemente segura justifica os elevados custos associados. Para estes casos, outras medidas de segurança foram desenvolvidas e as principais delas estão representadas na Figura 2.2.

Figura 2.2 - Camadas de redução de riscos (adaptado da norma IEC 61511-1).

No caso do SIS, as camadas de redução de riscos são projetadas para prevenção ou mitigação de riscos.

As camadas de prevenção impedem a ocorrência de falhas críticas, desde que o projeto destas camadas permita o diagnostico e tratamento adequados destas falhas. Estas camadas de prevenção envolvem:

- Concepção e projeto de procedimentos de controle para prevenir ou reduzir falhas críticas;
- Sistema de controle básico de processo (BPCS) que é capaz de atender a determinados requisitos de segurança de um projeto adequado de controle;
- Alarmes de alerta de situações críticas ao operador;
- Sistemas instrumentados de segurança (SIS); etc.

As camadas de mitigação são projetadas para reduzir as consequências geradas após a ocorrência de falhas críticas. Estas camadas envolvem:

- Proteção ativa: sistemas de alívio (válvulas de alívio, discos de ruptura, etc.);

- Proteção passiva: sistemas de contenção (diques);
- Planos de emergência para minimizar o impacto à planta e à comunidade;
- Alarmes de alerta de situações críticas ao operador;
- Sistemas instrumentados de segurança (SIS); etc.

2.3 CARACTERÍSTICAS DE UM SIS

Sistema instrumentado de segurança (SIS) constitui um sistema de controle de segurança que tem como objetivo, reduzir os riscos em processos industriais, quando é identificado pela corporação, que existem riscos não aceitáveis nestes processos durante sua operação. De uma forma geral, o SIS pode atuar de duas formas: (i) para prevenir a ocorrência de falhas críticas ou (ii) para mitigar as consequências geradas pela ocorrência de falhas críticas..

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

O SIS pode ser implementado a partir do uso de sistemas mecânicos, elétricos, eletrônicos e eletrônicos programáveis (E/E/EPs). Este trabalho aborda o projeto de SIS a partir do uso de sistemas eletrônicos programáveis (PESs) ou controladores programáveis (CPs) de segurança. A Figura 2.3 ilustra através de um diagrama de blocos, os componentes de hardware de um SIS a partir do uso de PES. O SIS é constituído por um ou mais sensores de segurança, um ou mais controladores programáveis de segurança (PESs) e um ou mais atuadores de segurança (LUNDTEIGEN; RAUSAND, 2009).

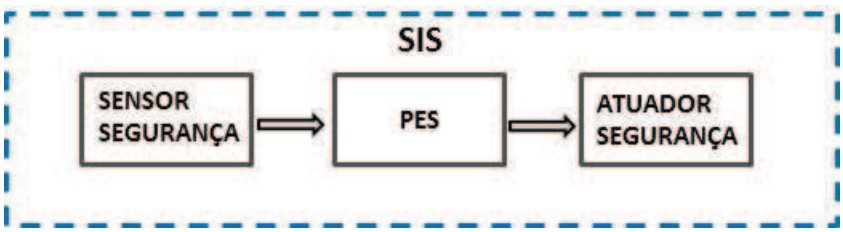


Figura 2.3 - Componentes de hardware de um SIS a partir do uso de PES.

De acordo com Lundteigen e Rausand (2009), um SIS é instalado para detectar eventos críticos (ex.: vazamento de gás, altas pressões) para evitar ou mitigar suas consequências aos seres humanos, meio-ambiente e equipamentos. Adicionalmente, segundo Rouvroyne e Bliek (2002), o SIS é usado para trazer o processo industrial a um estado seguro (ex.: desligamento de emergência quando pré-condições de variáveis de controle são violadas).

Neste contexto, a função de um SIS é monitorar através de sensores de segurança, eventos críticos no processo industrial e indicar alarmes ou executar ações pré-programadas, através de atuadores de segurança, para a prevenção de acidentes ou mitigação das consequências geradas pela ocorrência desses eventos (GOBLE, 1998). Adicionalmente, Goble (1998) define que um SIS:

- Não melhora o rendimento de um processo.
- Não aumenta a eficiência de um processo.
- Reduz gastos com perdas.
- Reduz custos de riscos.

Desta forma o SIS é um sistema desenvolvido para causar a redução de riscos e é responsável pela degeneração do processo industrial de forma controlada para um estado seguro, caso seja diagnosticada uma falha crítica.

2.3.1 Função instrumentada de segurança (SIF)

O SIS implementa uma ou mais funções instrumentadas de segurança (*safety instrumented function* ou SIF) (CRUZ-CAMPA et al., 2009). Cada SIF visa detectar uma condição perigosa e automaticamente tomar ações apropriadas para mover o processo para um estado seguro (CRUZ-CAMPA et al., 2009).

Do ponto de vista de hardware, um SIS implementa suas SIFs por meio de:

- um ou mais sensores (ex.: temperatura, pressão, nível, fogo, fumaça, concentração de gás, etc.);
- um ou mais dispositivos elétricos / eletrônicos / eletrônico programáveis (E/E/EPs) onde EP também denominado de PES é um controlador programável de segurança;
- um ou mais atuadores (ex.: válvulas de segurança, chaves elétricas, etc.).

2.3.2 Nível de integridade de segurança (SIL)

O nível de integridade de segurança (*safety integrated level* ou SIL) é a medida da segurança que se espera do SIS na realização de sua função quando solicitado (DUTUIT et al., 2008b), ou seja, o SIL reflete aquilo que os usuários finais podem esperar de um dispositivo ou sistema na sua função e, em caso de falha, que a falha ocorra de maneira segura. Falha segura é aquela que quando diagnosticada, faz com que o SIS degenere de forma controlada o processo industrial, levando este processo para um estado seguro (ex.: equipamento é desligado). SILs são medidas de segurança associadas a sistemas e seus componentes.

O SIL foi introduzido durante o desenvolvimento da norma IEC 61508. Esta norma trata de sistemas instrumentados de segurança e segurança funcional. O termo “segurança funcional” é a segurança que sistemas relacionados à segurança fornecem para o processo todo ou planta.

Neste contexto, a norma IEC 61508, considera que existem quatro classes de SIL. A Tabela 2.1 mostra cada classe de SIL de acordo com a IEC 61508.

Tabela 2.1 – Níveis de integridade de segurança (SIL) – (IEC 61508).

Nível de integridade de segurança (SIL)	Probabilidade de falha sob demanda (PFD)	Fator de redução de risco (FRR)
4	0,0001 – 0,00001	10000 - 100000
3	0,001 – 0,0001	1000 - 10000
2	0,01 – 0,001	100 - 1000
1	0,1 – 0,01	10 - 100

2.3.3 Probabilidade de falha sob demanda (PFD)

Considerando-se novamente a Tab. 2.1, observa-se que a probabilidade de falha sob demanda (PFD) é crucial para dimensionar o SIL, sendo um parâmetro importante para medir a capacidade de redução de risco de um SIS.

Segundo Rouvroye et al. (2002), a PFD é a probabilidade média de que uma SIF não estará apta para executar sua função sob demanda do processo que ela protege. Seguem abaixo, dois exemplos elucidativos para entender melhor este conceito:

- Exemplo 1: no caso da SIF determinar a desenergização das saídas em caso de falha crítica, PFD é a probabilidade do sistema falhar provocando saídas energizadas.
- Exemplo 2: no caso da SIF determinar a energização das saídas em caso de falha crítica, PFD é a probabilidade do sistema falhar provocando saídas desenergizadas.

A PFD de um sistema é obtida a partir de um relatório de análise de riscos deste sistema. Neste relatório, são identificadas as SIFs que compõem o sistema sob análise e para cada SIF são definidas as respectivas PFDs. Portanto, a PFD resultante de um sistema é obtida a partir da SIF mais crítica, ou seja, aquela que requer maior nível de segurança ou maior fator de redução de risco (FRR). A sintaxe para o cálculo da PFD do sistema é mostrada na equação (2.1).

$$PFD_{sist} = \text{MÍNIMO}\ (PFD_1 : PFD_2 : . \ . \ . \ . \ : PFD_{n-1} : PFD_n) \qquad (2.1)$$

2.3.4 Fator de redução de risco (FRR)

Outro parâmetro fundamental para dimensionar o SIL é o fator de redução de risco (FRR), conforme a Tab. 2.1. Goble (1998) define o fator de redução de risco (FRR) como sendo a relação entre o risco inerente e o risco aceitável, de acordo com a equação (2.2).

$$FRR = \frac{(\text{risco inerente})}{(\text{risco aceitável})} \qquad (2.2)$$

O “risco inerente” é o risco presente em um processo industrial quando em operação normal. Algumas vezes o risco inerente é maior que o risco admitido como aceitável. Neste caso, medidas de redução de risco devem ser empregadas. Daí a necessidade de se calcular o fator de redução de risco como métrica para a determinação do SIL de acordo com as PFDs associadas às SIFs presentes na especificação de projetos de SIS.

Ainda segundo Goble (1998), o fator de redução de risco é o inverso da PFD, de acordo com a equação (2.3).

$$FRR = \frac{1}{PFD} \qquad (2.3)$$

2.4 CONTROLADOR PROGRAMÁVEL DE SEGURANÇA

O sistema eletrônico programável (PES) definido pela IEC 61508 (1998) como um dos sistemas usados para a realização das funções de segurança em aplicações críticas é formado por um ou mais circuitos de entrada, um processador (CPU) e um ou mais circuitos de saída.

No contexto deste trabalho, o PES é baseado em um sistema microprocessado ou microcontrolado denominado de controlador programável (CP) de segurança. O CP de segurança é um controlador programável designado para uso em aplicações relacionadas com a segurança funcional (LIU et al., 2008).

Segundo a IEC 61508 (1998), o que difere um CP de segurança de um CP convencional é:

- ✓ a função de diagnóstico implementada em cada elemento do CP de segurança,
- ✓ arquiteturas de redundâncias para tratamento de sistemas tolerantes a falhas de hardware;
- ✓ a garantia de falha-segura, isto é, caso um elemento falhe, a falha não coloca o processo em um estado não seguro;
- ✓ a certificação diferenciada destes equipamentos. No caso dos CPs de segurança, a certificação é de acordo com a norma IEC 61508.

2.4.1 Arquiteturas do CP de segurança

As arquiteturas de CP de segurança aplicadas a SIS podem ser classificadas em (i) sem redundância ou (ii) com redundância.

As arquiteturas com redundância são utilizadas para aumentar a confiabilidade destes sistemas com relação à tolerância de falhas de hardware.

2.4.1.1 Arquitetura 1oo1D

A Figura 2.4 mostra uma arquitetura 1oo1D (lê-se 1 de 1 com diagnóstico) de um CP de segurança. Esta arquitetura adiciona à chave acionada pelo circuito de saída, uma chave em série acionada pelo circuito de diagnóstico. Se uma falha perigosa[9] for detectada pelo circuito de diagnóstico, esta chave pode desenergizar a saída convertendo falhas perigosas em falhas seguras[10].

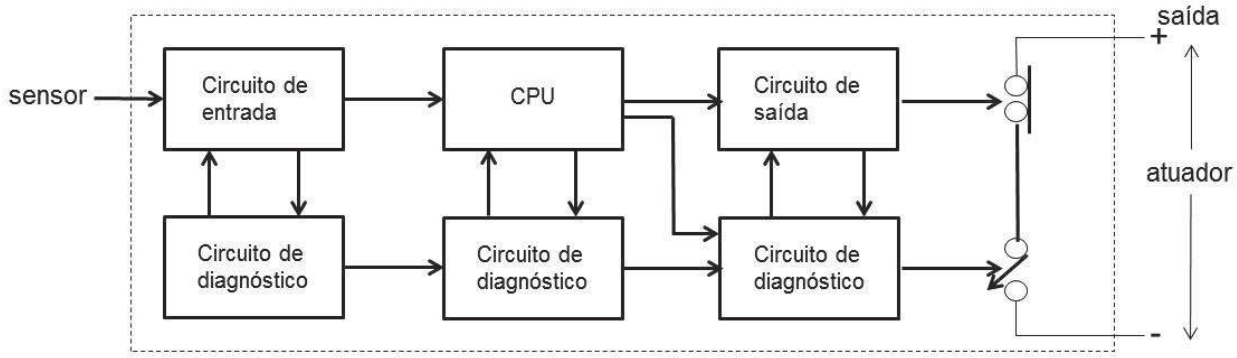


Figura 2.4 - Arquitetura 1oo1D de um CP de segurança.

2.4.1.2 Arquitetura 1oo2D

Na arquitetura 1oo2D (lê-se 1 de 2 com diagnóstico), dois CPs de segurança podem ser interligados para minimizar o efeito de falhas perigosas. Esta arquitetura utiliza dois processadores independentes (CPU) com seus respectivos circuitos de entrada, saída e circuitos de diagnóstico. As quatro saídas desta arquitetura estão interligadas em série. Caso ocorra uma falha em um dos CPs, a saída é desenergizada (falha-segura). Esta arquitetura oferece baixa probabilidade de falha sob demanda, porém aumenta a probabilidade de ocorrência de falha segura. A Figura 2.5 mostra uma arquitetura 1oo2D.

9 Por “falha perigosa” entende-se por uma falha no nível de hardware do circuito eletrônico e que impede o dispositivo de realizar sua função de segurança; exigido pelas normas aplicáveis e regras de certificação.

10 Por “falha segura” entende-se por aquela cujo risco apresenta uma magnitude aceitável, exigido por regras corporativas e normas aplicáveis.

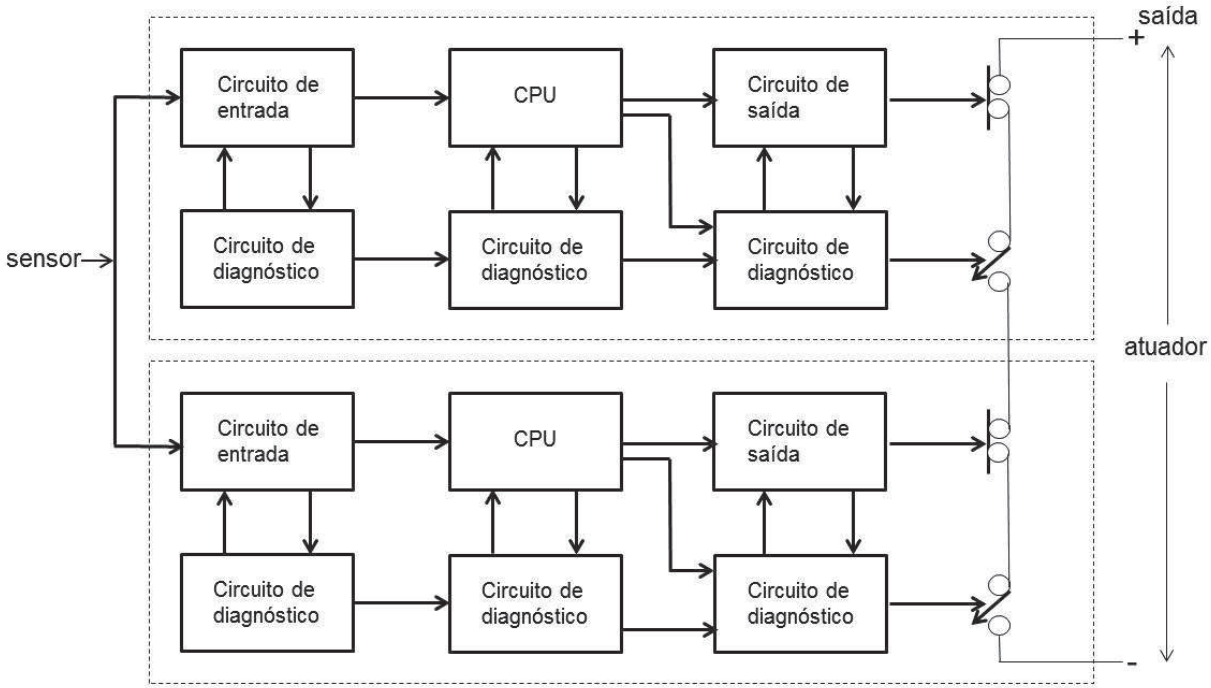


Figura 2.5 - Arquitetura 1oo2D de um CP de segurança.

2.4.1.3 Arquitetura 2oo2D

Outra arquitetura com dois CPs de segurança foi desenvolvida para situações onde falhas com saídas desenergizadas não são desejadas. Esta arquitetura é aplicada a sistemas de proteção do tipo “energização na falha”. As saídas dos dois CPs são interligadas em paralelo, conforme mostrado na Figura 2.6. Se um CP falhar com suas saídas desenergizadas, o outro CP ainda será capaz de manter a carga energizada.

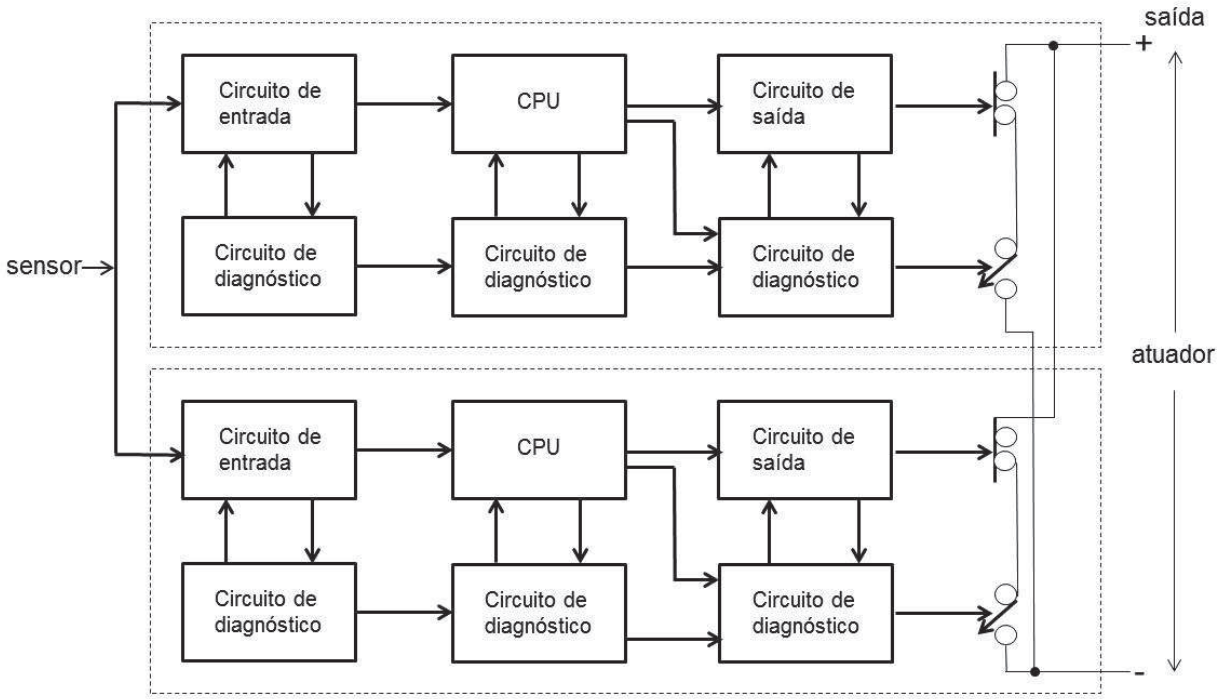


Figura 2.6 - Arquitetura 2oo2D de um CP de segurança.

2.4.1.4 Arquitetura 2oo3

A arquitetura 2oo3 (lê-se 2 de 3) é utilizada para tolerar ambos os tipos de falhas denominadas de “segura” (saída desenergizada) e “perigosa” (saída energizada). Esta arquitetura fornece segurança e alta disponibilidade com a utilização de três CPs.

Duas saídas de cada CP são necessárias para cada canal de saída. Estas duas saídas são interligadas em um circuito de “votação”, que determina o estado da saída, conforme mostrado na Figura 2.7. A saída atual é igual ao da “maioria”, ou seja, quando pelo menos duas saídas estiverem em “on”, a carga será energizada. Por outro lado, quando pelo menos duas saídas estiverem em “off”, a carga será desenergizada.

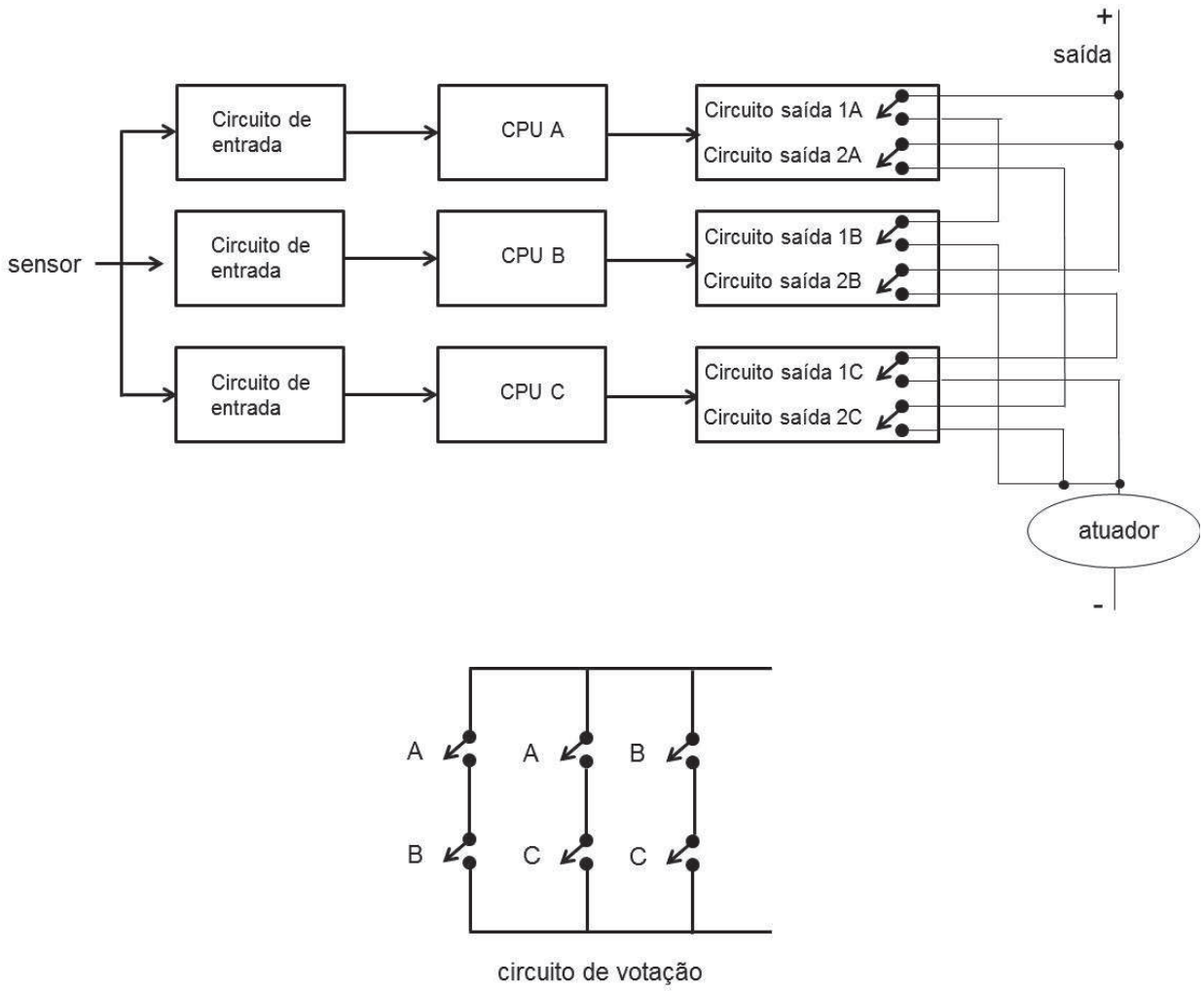


Figura 2.7 - Arquitetura 2oo3 de um CP de segurança.

2.5 NORMAS APLICADAS À SEGURANÇA FUNCIONAL

As normas aplicadas à segurança funcional e à integridade de SIS na área de processos industriais, são as normas IEC 61508 , IEC 61511 e ANSI/ISA SP 84.01.

De acordo com a IEC 61508-4 a segurança funcional é parte da segurança global do equipamento ou processo sob controle e que depende do correto funcionamento dos equipamentos E/E/EP relacionados à segurança ou outras tecnologias e facilidades externas de redução de riscos. Nesta seção serão discutidas as normas IEC 61508, IEC 61511 e ANSI/ISA SP 84.01.

2.5.1 IEC 61508

A IEC 61508 é uma norma internacional desenvolvida pela *International Electrotechnical Commission* (IEC) aplicável à segurança funcional de equipamentos elétricos, eletrônicos e eletrônicos programáveis (E/E/EP). Ela pode ser chamada de documento padrão, pois normas de segurança para diferentes segmentos industriais e aplicações derivam desta norma. Esta norma tem dois objetivos:

- orientar indústrias no desenvolvimento de normas suplementares que atendam os requisitos de segurança de suas aplicações;
- permitir o desenvolvimento de equipamentos E/E/EP relacionados à segurança, onde normas deste setor de aplicação não existem, sendo aplicada também para a certificação de hardwares e softwares destes equipamentos.

A Figura 2.8 mostra as principais normas de segurança vigentes para indústrias de diversos segmentos, entretanto, todas elas usam a IEC 61508 como referência.

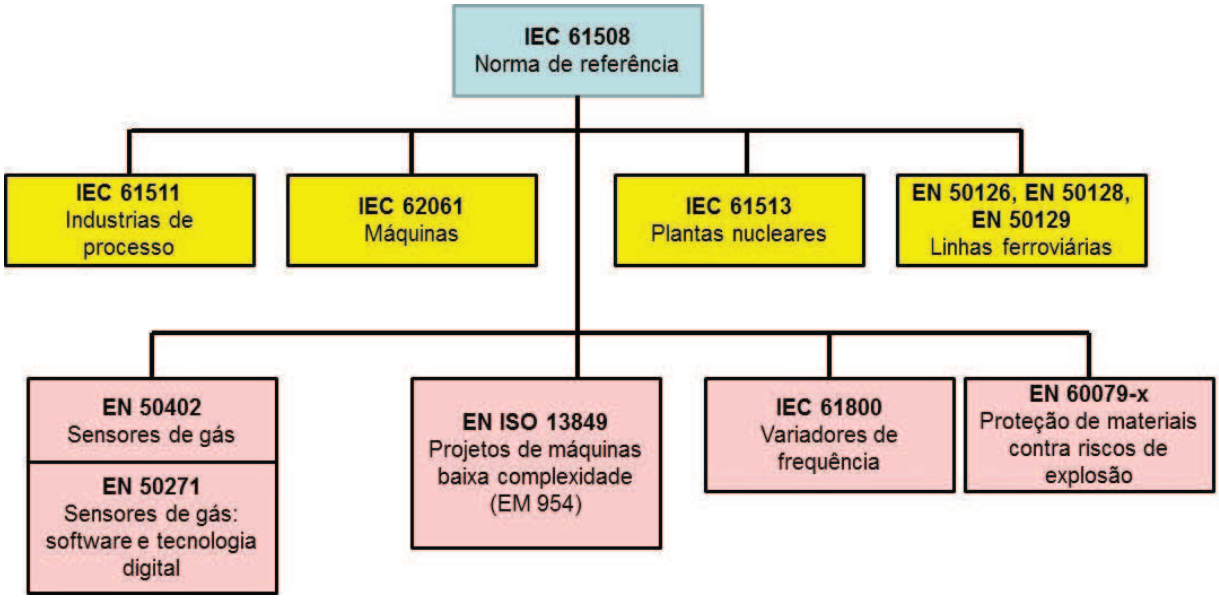


Figura 2.8 - Normas de segurança vigentes para diferentes segmentos industriais.

A norma IEC 61508 é baseada em dois conceitos fundamentais:

- Ciclo de vida de segurança.
- Níveis de integridade de segurança (SILs).

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. Segundo a IEC 61508, o ciclo de vida de segurança é definido como um conjunto de atividades necessárias envolvidas na implementação de SIFs, ocorrendo durante o período de tempo que começa na fase de concepção e finaliza quando todas as SIFs não são mais utilizadas. A Figura 2.9, mostra o diagrama de ciclo de vida de segurança segundo a IEC 61508. Nesta Figura são mostradas as atividades do projeto do SIS, começando a partir da concepção do projeto e finalizando quando todas as SIFs não são mais utilizadas, ou seja, quando o sistema não realiza mais sua função.

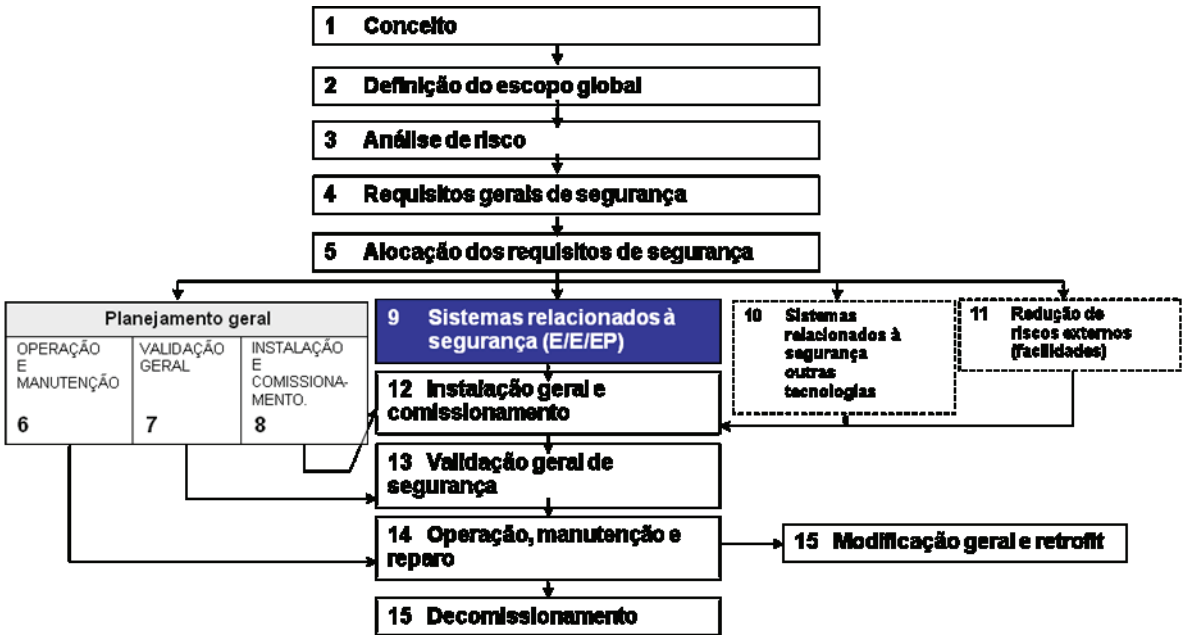


Figura 2.9 - Ciclo de vida de segurança. Adaptado de (IEC 61508; 1998).

É interessante comentar que cada fase deste ciclo de vida, está relacionada com uma ou várias partes da norma IEC 61508. A norma IEC 61508 é constituída por sete partes: IEC 61508-1 a IEC 61508-7, abaixo descritas:

- IEC 61508-1: requisitos gerais;
- IEC 61508-2: requisitos para sistemas E/E/EP relacionados à segurança;
- IEC 61508-3: requisitos de software;
- IEC 61508-4: definições e abreviações;
- IEC 61508-5: exemplos de métodos de determinação dos SILs;

- IEC 61508-6: orientações na aplicação da IEC61508-2 e -3;
- IEC 61508-7: visualização geral de técnicas e medidas.

2.5.2 IEC 61511 e ANSI / ISA SP 84.01

A IEC 61511 é a norma internacional aplicável à integridade de SIS em indústrias de processo (CRUZ-CAMP et al., 2009).

A IEC 61511 estabelece requisitos para o chamado ciclo de vida de segurança do SIS. Este ciclo de vida de segurança inclui requisitos para a especificação, projeto, implementação, operação, manutenção e modificação do SIS desde sua concepção até o seu decomissionamento[11] (CRUZ-CAMPA et al., 2009). A Figura 2.10 mostra esse ciclo de vida de segurança de acordo com a norma IEC 61511.

Pode-se observar que as atividades presentes no ciclo de vida de segurança previsto na IEC 61511, assemelham-se às atividades indicadas na norma IEC 61508, entretanto, ela estabelece uma atividade de gerenciamento e planejamento de todas as atividades do ciclo de vida de segurança, através de auditoria e avaliação destas atividades.

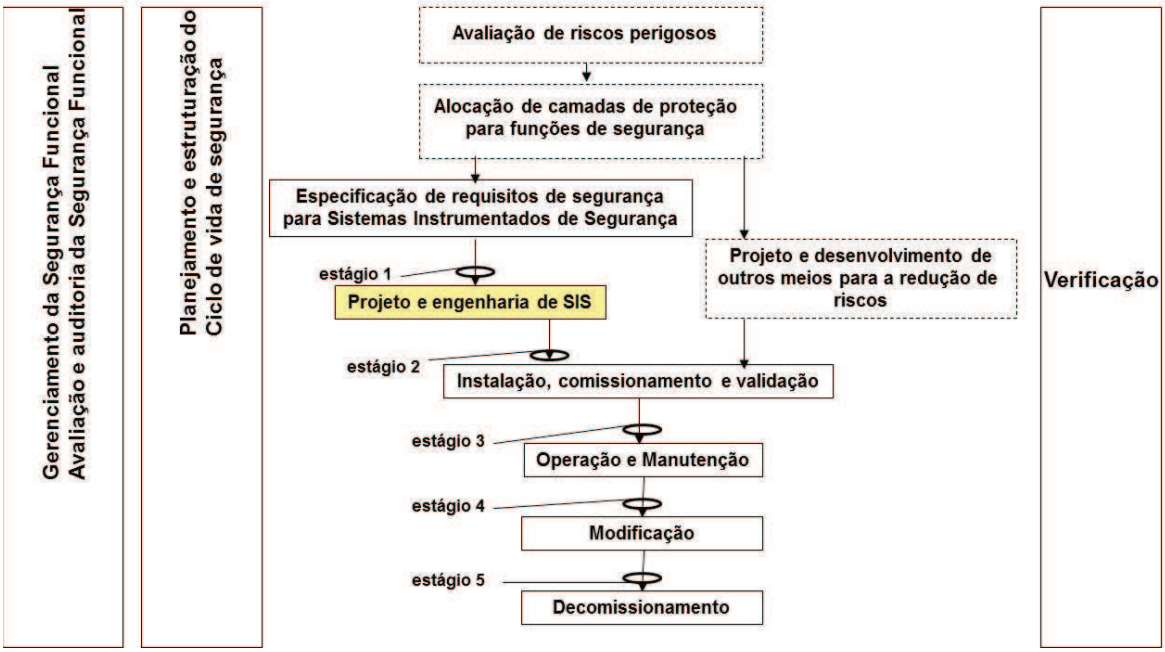


Figura 2.10 - Ciclo de vida de segurança. Adaptado de (IEC 61511; 2003).

11 "Decomissionamento" é considerado um processo formal para remover o sistema do seu estado ativo e para desativar o processo industrial; não comprometendo a saúde das pessoas, preservando o meio-ambiente e o estado dos equipamentos associados.

É interessante comentar que cada fase deste ciclo de vida, está relacionada com uma ou várias partes da norma IEC 61511. A norma IEC 61511 é constituída por três partes: IEC 61511-1 a IEC 61511-3, abaixo descritas:

- IEC 61511-1: estrutura, definições, sistema, requisitos de hardware e software;
- IEC 61511-2: orientações na aplicação da IEC 61151-1;
- IEC 61511-3: orientação para a determinação dos SILs exigidos.

No presente trabalho, consideram-se também as normas internacionais aplicáveis à segurança funcional de sistemas relacionados com a segurança do setor industrial de processos que são:

- IEC 61508 (1998) - Segurança funcional de sistemas elétrico / eletrônico / eletrônico programável relacionável à segurança.
- IEC 61511 (2003) - Segurança funcional – SIS para o setor de indústria de processos, também aceita pelo comitê formado pela ANSI (*American National Standards Institute*) juntamente com a ISA (*Instrumentation*, *Systems and Automation Society*) no projeto ISA 84 como ANSI/ISA SP 84.01 (2004).

A principal diferença entre a IEC 61511 e a ANSI/ISA SP 84.01 é que na norma ANSI/ISA foi adicionada uma cláusula aplicável a sistemas já comissionados e em operação antes da sua publicação. Esta cláusula permite que as companhias mantenham seus projetos de SISs existentes de acordo com as normas anteriores (ANSI/ISA SP 84.01, 1996) desde que todas as fases de projeto, manutenção, inspeção, testes e operação ocorram de “maneira segura” (CRUZ-CAMPA et al., 2009), isto é, executando procedimentos de validação e verificação previstos pela norma IEC 61511, de acordo com a Figura 2.10.

A Figura 2.11 mostra como as normas IEC 61508 e IEC 61511 vêm sendo aplicadas no setor industrial. Ambas são aplicáveis no setor de processos. A IEC 61508 é dirigida para fabricantes e fornecedores de tecnologias aplicadas à segurança funcional, enquanto que, a IEC 61511 é dirigida para empresas de projetos de SISs, integradores de sistemas e usuários finais de SISs, ou seja, a primeira suporta o desenvolvimento de dispositivos de hardware enquanto a segunda orienta o desenvolvimento de SISs que utilizam este hardware.

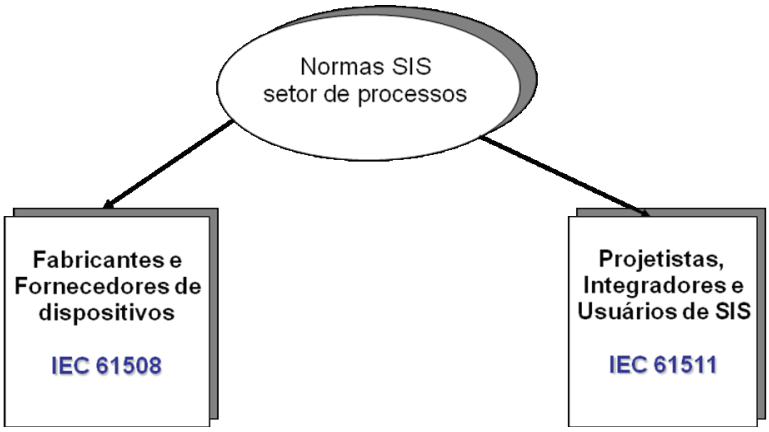


Figura 2.11 - Relação entre as normas IEC 61508 e IEC 61511. Adaptado de (IEC 61511; 2003).

2.5.3 Requisitos para o programa de controle de um SIS

No contexto deste trabalho, o programa de controle contempla o código usado para o diagnóstico e tratamento das falhas críticas de um processo industrial. Este código deve ser desenvolvimento e compilado[12] através de um software utilitário. O código compilado é então transferido para a memória de programa do PES ou controlador programável de segurança, a fim de executar o código e as funções de segurança especificadas no projeto do SISs. Nesta seção, será discutido os requisitos para o desenvolvimento do algoritmo de controle de um SIS, de acordo com a norma IEC 61511.

A norma IEC 61511, parte 1, cláusula 12, trata dos requisitos para o algoritmo de controle ou software de aplicação para SIS. A norma reconhece três tipos de softwares (Fig. 2.12) e três tipos de linguagens de programação (Fig. 2.13) utilizadas para o desenvolvimento destes softwares.

12 Conversão de um programa de linguagem de alto nível em um programa em código de máquina, o qual pode ser executado diretamente por um microprocessador ou microcontrolador.

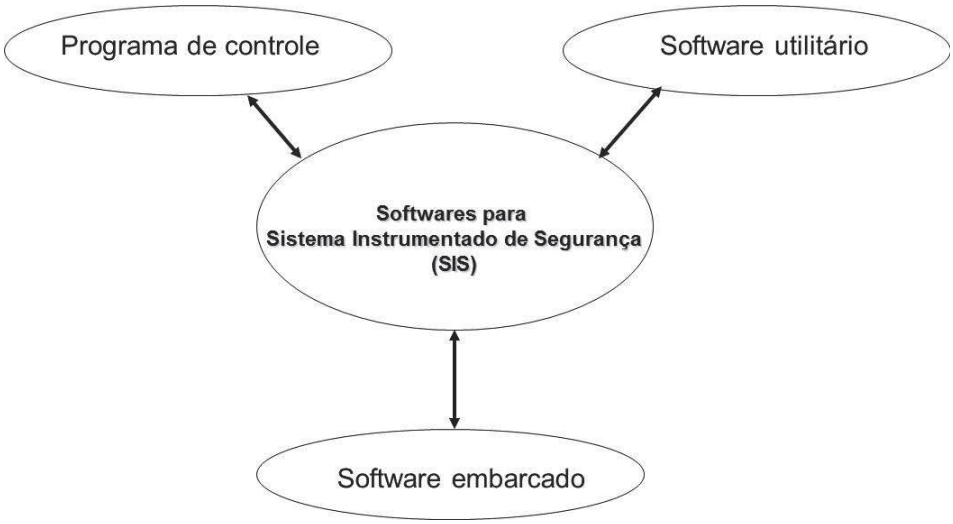


Figura 2.12 - Tipos de softwares para SIS. Adaptado de (IEC 61511; 2003).

O “programa de controle” é um código desenvolvido de acordo com a aplicação do usuário. No contexto deste trabalho, é o código que executa o diagnóstico e tratamento das falhas críticas do SIS. Em geral, ele contém sequências lógicas, permissividades, limites e expressões que coletam os sinais de entradas e acionam as saídas apropriadas, executam cálculos e tomam decisões necessários para atender aos requisitos funcionais do SIS.

O “software utilitário” é a ferramenta para o desenvolvimento, modificação e documentação dos algoritmos de controle.

O “software embarcado” faz parte do “pacote” fornecido pelo fabricante do equipamento / sistema e não é acessível para modificação. Este software também é referenciado como um *firmware* ou “software do sistema” (IEC 61511; 2003).

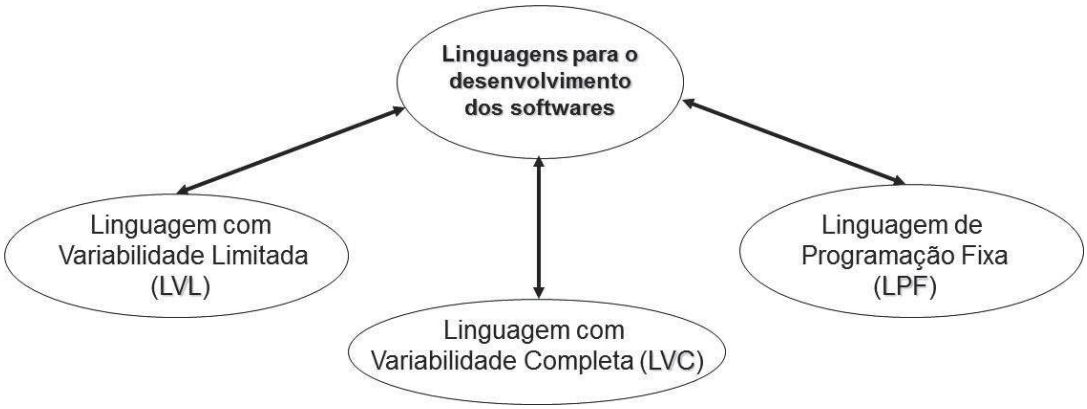


Figura 2.13 - Tipos de linguagens de programação para SIS. Adaptado de (IEC 61511; 2003).

O programa de controle é desenvolvido por meio de uma linguagem de programação que pode ser classificado de acordo com a estrutura na Figura 2.13.

A linguagem de programação fixa (LPF) é uma linguagem usada para ajustar parâmetros na conFiguração de operação de dispositivos de controle como a faixa de um transmissor de pressão, níveis de alarmes, endereços de redes, etc. (IEC 61511). Como exemplos de dispositivos programados com LPF, pode-se citar os sensores inteligentes, válvulas inteligentes, relés eletrônicos, etc.

A linguagem com variabilidade limitada (LVL) é uma linguagem de programação que pode combinar funções pré-definidas em bibliotecas a fim de implementar as especificações dos requisitos de segurança (IEC 61511; 2003). Exemplos típicos de linguagens de programação do tipo LVL são as descritas pela norma IEC 61131-3 (1992) - diagrama ladder (LD), diagrama de blocos de funções (FBD) e gráfico de sequenciamento das funções (SFC) -. Estas linguagens são de uso comum em controladores programáveis (CPs) que são considerados como equipamentos essenciais na implementação de sistemas de controle industriais.

A linguagem com variabilidade completa (LVC) é uma linguagem de programação com capacidade de implementar uma larga variedade de funções (IEC 61511; 2003). No setor industrial, este tipo de linguagem é encontrado frequentemente no desenvolvimento de softwares embarcados e raramente para a programação de algoritmos de controle. Como exemplo de LVC pode-se citar as linguagens Ada, C, Pascal, Instruction List, Java, etc.

De acordo com a norma IEC 61511 (2003), para aplicações com nível de integridade de segurança até SIL 3, o desenvolvimento e modificação do algoritmo de controle usando as linguagens LPF ou LVL é permitido. Para aplicações com SIL 4 e para aplicações usando a linguagem LVL, o desenvolvimento e a modificação do algoritmo de controle deverá obedecer a IEC 61508.

3 TÉCNICAS UTILIZADAS PARA MODELAGEM E VALIDAÇÃO DE ALGORÍTMOS DE CONTROLE

O sistema instrumentado de segurança (SIS) pode ser visto como um sistema dirigido por eventos e que apresenta funcionalmente características como reinicialização, assincronismo, paralelismo, concorrência entre eventos, etc., motivo pelo qual, podem ser tratados como SED. Além disso, tem-se a necessidade de desenvolver os modelos de diagnóstico e tratamento de falhas críticas associadas às SIFs de um SIS. Neste contexto, utiliza-se a técnica de redes de Petri interpretada para a descrição dos algoritmos de coordenação e tratamentos de falhas críticas; e uma combinação de rede Bayesiana e rede de Petri interpretada para modelagem dos algoritmos de diagnósticos de falhas críticas em SIS.

3.1 REDE DE PETRI (PN)

Rede de Petri (PN), como uma ferramenta gráfica e matemática, provê uma forma uniforme para modelagem, análise e projeto de SEDs (ADAM; ATLURI; HUANG, 1998; NASSAR et al., 2008; ZURAWSKI; ZHOU, 1994), sendo efetiva como técnica de descrição e especificação de processos (HAMADI; BENATALLAH, 2003; MORALES; MELO; MIYAGI, 2007; YOO; JEONG; CHO, 2010). Fornece uma representação que pode ser usada tanto como modelo conceitual quanto modelo funcional de um sistema em que se pode analisar e validar o funcionamento do sistema em cada fase de seu ciclo de desenvolvimento. A PN pode também ser utilizada como uma ferramenta de comunicação que garante o formalismo necessário para integrar equipes de projeto, permitindo uma fácil interpretação e identificação dos processos, do comportamento dinâmico dos processos e/ou dos sistemas que estão sendo modelados (NASSAR et al., 2008). Os modelos baseados em PN podem ser usados para avaliação qualitativa e quantitativa, envolvendo a análise das propriedades comportamentais e a medida de desempenho, respectivamente. Além disso, com o desenvolvimento de simuladores desde a década de 90 (ZURAWSKI; ZHOU, 1994), tem-se à disposição ferramentas para edição e análise destes modelos. Possibilita a representação da dinâmica do sistema e sua estrutura em diversos níveis de abstração, de acordo com a complexidade do sistema (NASSAR et al., 2008). É capaz de modelar a

sincronização de processos, a ocorrência de eventos assíncronos, de operações concorrentes e de conflitos, ou do compartilhamento de recursos (ADAM; ATLURI; HUANG, 1998; NASSAR et al., 2008; ZURAWSKI; ZHOU, 1994).

Desde sua apresentação por Carl Adam Petri (BRAUER; REISIG, 2006), a PN tem sido usada na modelagem e análise de diferentes tipos de sistemas e aplicações tais como: protocolos distribuídos (KANESHIRO et al., 2008), aplicações industriais (NASSAR et al., 2008; ZURAWSKI; ZHOU, 1994), diagnóstico e tratamento de falhas não críticas (MORALES; MELO; MIYAGI, 2007; RIASCOS; SIMÕES; MIYAGI, 2006; RU; HADJICOSTS, 2008), fluxo de processos (KIEPUSZEWSKI; HOFSTED; AALST, 2003), controle supervisório (LEE; ZHOU; HSU, 2005) entre outras. Este trabalho pretende estender sua aplicação para o diagnóstico e tratamento de falhas críticas em projeto de SIS.

3.1.1 Formalização

A PN é uma 4-tupla $N = (P, T, F, W)$ associada com uma descrição de estado indicada por M . Onde P e T são conjuntos finitos, não nulos e disjuntos. P é o conjunto finito de lugares e T é o conjunto finito de transições. F é o conjunto finito dos relacionamentos entre lugares e transições e é também chamado de conjunto de arcos orientados. W é um conjunto de números naturais não nulos que representam os pesos de cada arco orientado. M é um conjunto de números naturais que representa a quantidade de marcas nos lugares, que também é conhecido como marcação dos lugares. Mo indica assim uma marcação inicial, isto é, uma distribuição de marcas nos lugares que caracteriza o estado inicial da PN (HAN et al., 2008; MURATA, 1989; LI; ZHOU, 2008; XU et al., 2007; YOO; JEONG; CHO, 2010; ZURAWSKI; ZHOU, 1994). $M(p)$ indica o número de marcas no lugar P e muitas vezes é também indicado simplesmente por Mp.

Uma PN pode ser dita ordinária se $\forall f \in F, W(f) = 1$ (LI; ZHOU, 2008).

Em uma rede PN o pré-conjunto $x \in P \cup T$ é definido como ${}^{\bullet}x = y \in P \cup T | (y, x) \in F$. O pós-conjunto $x \in P \cup T$ é definido como $x^{\bullet} = y \in P \cup T | (x, y) \in F$. Os pré-conjuntos (pós-conjuntos) de um conjunto de elementos são definidos como a união dos pré-conjuntos (pós-conjuntos) desses elementos (MURATA, 1989).

Numa PN $t \in T$ está habilitada em M (simbolicamente $M[t >$) se, e somente se, $\forall p \in {}^{\bullet}t: M(p) > 0$. Uma transição $t \in T$ habilitada pode ser disparada. Como resultado de um disparo da transição t tem-se uma nova marcação M', que é denotado por $M[t > M'$, com $M'(p) = M(p) - 1$ se $p \in {}^{\bullet}t \backslash t^{\bullet}$; $M'(p) = M(p) + 1$ se $p \in t^{\bullet} \backslash {}^{\bullet}t$; e $M(p) = M'(p)$ nos demais casos, para todo $p \in P$ (ADAM; ATLURI; HUANG, 1998; LI; ZHOU, 2004).

Uma PN é limitada se, e somente se, $\exists k \in \mathbb{N}^{+}$, $\forall M \in R(N, M_0)$ e $\forall p \in P$, tal que $M(p) \leq k$, em que $R(N, M_0)$ é o conjunto das marcações na PN alcançáveis a partir de M_0. A PN é dita pura se, e somente se, não há loops, isto é, $\nexists (x, y) \in (P \times T) \cup (T \times P), (x, y) \in F \wedge (x, y) \in F$ (LI; ZHOU, 2008).

Outra representação de uma PN é por meio de matriz de incidência e equações de estados. A matriz de incidência numa PN é representada por $[N] = [\mathrm{c_{ij}}]$ indexada por P e T tal que $p_i \in P$, $t_j \in T$ e $f_{ij} \subseteq (P \times T) \cup (T \times P)$ com f_{ij} o arco orientado ligando o lugar p_i à transição t_j ou a transição t_j ao lugar p_i, $c_{ij} = W(f_{ij})$ (MURATA, 1989).

No caso de uma PN pura, a matriz $N = [c_{ij}]$ é tal que $c_{ij} = 1$ se $t_j \in {}^{\bullet}p_i \backslash p_i^{\bullet}$, $c_{ij} = -1$ se $t_j \in p_i^{\bullet} \backslash {}^{\bullet}p_i$ e c=0 nos demais casos (DAVID; ALLA, 1994; ZURAWSKI; ZHOU, 1994).

A dinâmica de uma PN indica a mudança de estados da mesma e as regras de mudança de estados da PN são à base do sucesso dessa ferramenta na modelagem de sistemas dinâmicos (MURATA, 1989).

3.1.2 Representação gráfica

De acordo com a definição da PN, existe uma representação gráfica de seus elementos, de acordo com a Figura 3.1.

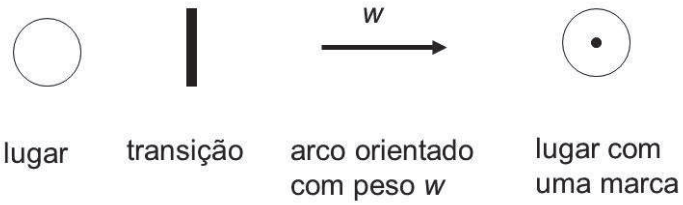


Figura 3.1 - Representação gráfica dos elementos de uma PN.

Graficamente a evolução da marcação M para M' de uma PN, conforme descrito na seção 3.1.1, pode ser vista na Figura 3.2.

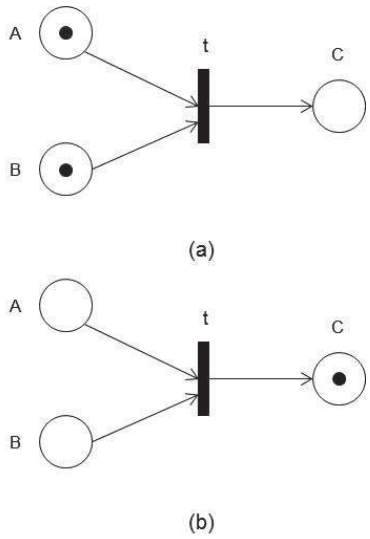


Figura 3.2 - Representação da dinâmica da PN, em que (a) é a PN antes do disparo de t e (b) é a PN depois do disparo de t.

3.1.3 Propriedades

A PN possui propriedades que permitem ao desenvolvedor do modelo identificar a presença ou ausência de comportamentos e funcionalidades específicas do domínio da aplicação do sistema em estudo. As propriedades podem ser distinguidas em comportamentais e estruturais (ZURAWSKI; ZHOU, 1994).

De acordo com Zurawski e Zhou (1994), as propriedades estruturais não dependem do conjunto de marcas iniciais da PN, mas sim de sua topologia e as propriedades comportamentais dependem do estado inicial da PN, ou seja, da marcação inicial M_0 e do conjunto de marcações acessíveis a partir da marcação inicial M_0. Ainda segundo Cardoso e Valette (1997), as propriedades comportamentais são reagrupadas sob o nome genérico de “boas propriedades”. Os métodos de análise destas propriedades podem basear-se no grafo de alcançabilidade. Neste contexto, as “boas propriedades” são: limitabilidade e segurança, vivacidade e reiniciabilidade.

As propriedades de interesse nesse trabalho são as “boas propriedades” a seguir descritas:

3.1.3.1 Limitabilidade e Segurança

Na área de comunicação e sistemas de informação, os lugares da PN são frequentemente usados para representar áreas de armazenamento de informação e em sistemas de manufatura são usados em geral para representar armazenamento de produtos e ferramentas. É preciso garantir que as áreas de armazenamento não excedam sua capacidade (ZURAWSKI; ZHOU, 1994).

Em PN, a propriedade que verifica a capacidade de um lugar é a limitação. Uma rede é dita k-limitada se o número de marcas em qualquer lugar p, em que $p \in P$, é sempre menor ou igual à k (com $k \in \mathbb{N}$) para toda marcação M alcançável a partir do estado inicial M_0 (ZURAWSKI; ZHOU, 1994). Ou então, em uma PN com, $p \in P$, se $\exists B > 0$ (com $B \in \mathbb{N}$) tal que $\forall M \in R(N, M_0)$ e $M(p) \leq B$, então p é limitado. Define-se que o limite B de uma PN é $max\{B\}$, $\forall p \in P$. A Figura 3.3 ilustra uma PN não limitada, pois o lugar p_4 pode receber infinitas marcas.

Uma PN é dita segura se ela é 1-limitada, ou seja, $B = 1$ para todos p lugares da PN (HAN et al., 2008) (ZURAWSKI; ZHOU, 1994). A Figura 3.4 ilustra uma rede segura.

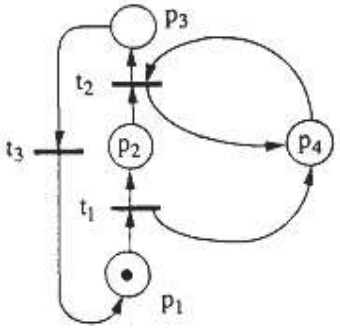


Figura 3.3 - Exemplo de rede de Petri não limitada (ZURAWSKI; ZHOU, 1994).

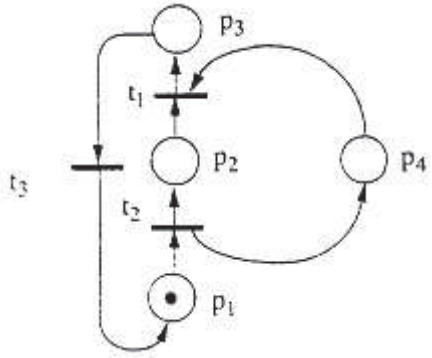


Figura 3.4 - Exemplo de rede de Petri segura (ZURAWSKI; ZHOU, 1994).

3.1.3.2 Vivacidade e Reiniciabilidade

O conceito de vivacidade é fortemente relacionado à situação de *deadlock* (estado em que a PN não pode disparar nenhuma de suas transições).

Uma rede é considerada viva se $\forall M$, $M_0[> M$, isto é, ela pode progredir por meio de alguma sequência de disparo. A partir de uma M_0, a rede pode não estar imediatamente em *deadlock*, mas pode existir uma limitação quanto a sequência de disparos que pode levar a PN a um estado de *deadlock* (ZURAWSKI; ZHOU, 1994) (HAN et al., 2008). Por isso existem diferentes níveis de vivacidade para uma transição t e uma marcação M_0, esses diferentes níveis podem ser analisados segundo o conjunto de todas possíveis sequências de disparos a partir de M_0 representada por $L(M_0)$. Uma transição t em uma PN é dita:

- $L0$-viva (ou morta) se não houver sequência de disparos em $L(M_0)$ em que t possa disparar;
- $L1$-viva (potencialmente disparável) se t pode ser disparada pelo menos uma vez em alguma sequência de disparos em $L(M_0)$;
- $L2$-viva se t pode ser disparada pelo menos *k* vezes em alguma sequência de disparos em $L(M_0)$, dado qualquer $k > 1$ inteiro positivo;
- $L3$-viva se t pode ser disparada infinitamente, em alguma sequência de disparos em $L(M_0)$;
- $L4$-viva (ou viva) se t é $L1$-viva em todas as marcações em $R(N, M_0)$.

Um caso de rede de Petri viva pode ser visto na Figura 3.5 e todas suas transições são $L4$-vivas. Já na Figura 3.6 a transição t_0 é $L0$-viva, para a marcação inicial M_0, a transição t_1 é $L1$-viva, a transição t_2 é $L2$-viva e a transição t_3 é $L3$-viva.

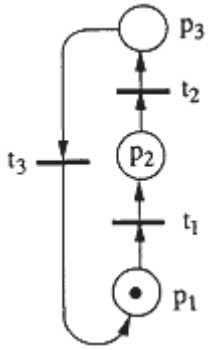


Figura 3.5 - Exemplo de rede de Petri reinicializável e viva (ZURAWSKI; ZHOU, 1994).

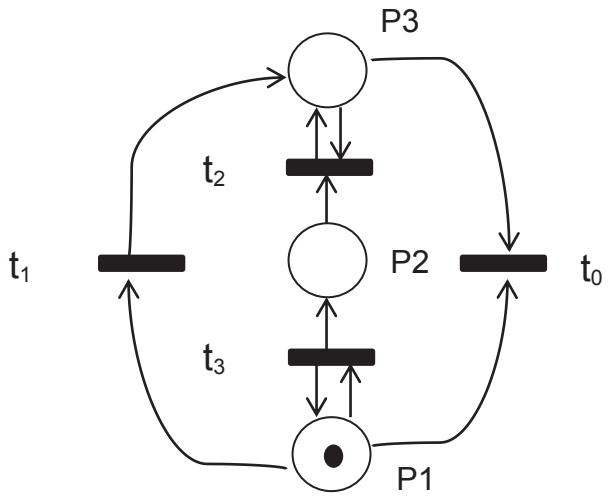


Figura 3.6 - Exemplo de PN com transições com diferentes níveis de vivacidade (ZURAWSKI; ZHOU, 1994).

Uma rede é considerada reinicializável se M é alcançável de $R(N, M_0)$ e M_0 é alcançável de $R(N, M)$ (ZURAWSKI; ZHOU, 1994). A Figura 3.5 ilustra uma rede reinicializável e a Figura 3.7 ilustra uma rede não reinicializável.

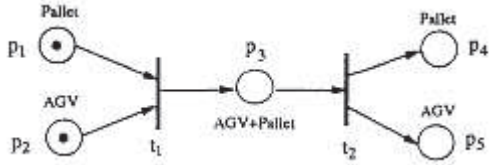


Figura 3.7 - Exemplo de rede de Petri não reinicializável (ZURAWSKI; ZHOU, 1994).

Neste trabalho, para atender aos requisitos das normas IEC 61508 e IEC 61511, as “boas propriedades” serão analisadas para cada etapa de construção dos modelos de diagnóstico, coordenação e tratamento das falhas de um SIS. A

propriedade de reiniciabilidade será analisada a partir da simulação dos modelos construídos com o uso da ferramenta HPSim (ANSCHUETZ, 2010) e as propriedades de vivacidade e segurança (1-limitada) serão analisadas com o uso da ferramenta PIPE2 (BONET et al., 2007).

Para a modelagem do comportamento de um SIS, será utilizada a rede de Petri interpretada que segundo Peterson (1977) é a rede à qual se associa uma interpretação, ou significado, aos seus lugares e transições, passando por isso a corresponder a algo real que se pretende modelar. No caso da rede de Petri interpretada, são associadas variáveis às transições da rede – representando condições e ações existentes no sistema. Tais variáveis podem indicar o estado dos atuadores, sensores, etc., permitindo assim, modelar a interação com o ambiente externo (CARDOSO; VALETTE, 1997).

Para a rede de Petri interpretada, definem-se dois novos tipos de elementos, denominados de arco habilitador e arco inibidor, conforme mostra a Figura 3.8.

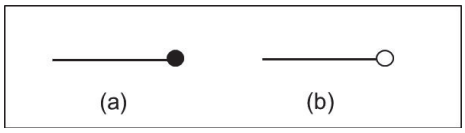
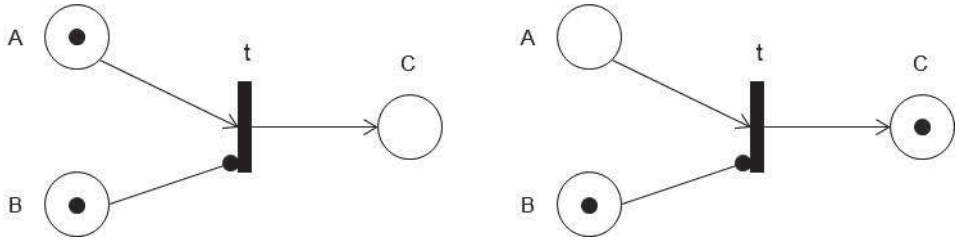


Figura 3.8 - (a) arco habilitador (b) arco inibidor.

Quando o lugar associado ao arco habilitador tem marca, a transição associada ao arco habilitador é habilitada para disparar, conforme mostra a Figura 3.9. Caso contrário, se o lugar associado ao arco habilitador não tem marca, a transição associada ao arco habilitador é desabilitada para disparar.

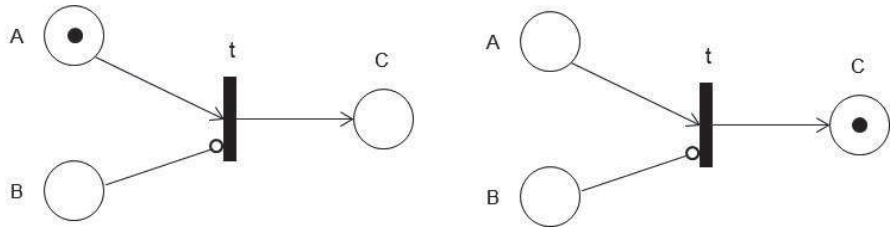


(a) (b)

Figura 3.9 - (a) PN antes do disparo de t (b) PN depois do disparo de t.

Por sua vez, quando o lugar associado ao arco inibidor não tem marca, a transição associada ao arco inibidor é habilitada para disparar, conforme mostra a

Figura 3.10. Caso contrário, se o lugar associado ao arco inibidor tem marca, a transição associada ao arco inibidor é desabilitada para disparar.



(a) (b)

Figura 3.10 - (a) PN antes do disparo de t (b) PN depois do disparo de t.

3.2 REDE BAYESIANA (BN)

De acordo com Pearl (2000), o ser humano tem certa dificuldade em associar números (informações estatísticas) à sua crença em determinado fato. É mais fácil observar se um fato específico depende de outro ou se um determinado fato, afeta ou não afeta outro fato. Assim, a representação gráfica, com seus relacionamentos de dependência mais explícitos, possibilita uma maior aproximação do raciocínio humano.

A rede Bayesiana (BN) fornece um método de raciocínio usado para representar graficamente crenças parciais sob condições de incerteza (PEARL, 2000). Adicionalmente, a BN é uma estrutura que graficamente modela as relações de probabilidades de dependência “causa – efeito” para um grupo de variáveis dentro de um domínio. A BN tem sido extensivamente aplicada para diagnóstico de falhas (CHIEN; CHEN; LIN, 2002; COZMAN, 2001; LERNER et al., 2002; MURPHY, 2007).

A BN é um grafo que permite representar a combinação de conhecimento especialista humano de um processo e da teoria de probabilidade para a construção da estrutura de diagnóstico; sendo que ambas, são recomendadas para a construção de uma “boa” rede Bayesiana (RIASCOS et al., 2007).

3.2.1 Formalização

Uma rede Bayesiana (BN) é um grafo acíclico orientado onde os nós representam variáveis aleatórias e os arcos direcionados representam

relacionamentos causais diretos entre os nós que conectam. Em uma BN, cada nó X_i, representado através de um círculo, é condicionalmente dependente de qualquer subconjunto de nós que são conhecidos como os nós pais de X_i (representados por $pa(X_i)$). A associação entre as variáveis e os seus pais é feita através de arcos e representa as relações de causa – efeito, descritas por $P(X_i \mid pa(X_i))$. Normalmente, tais relações são fornecidas em formato de Tabela, as quais são chamadas de Tabelas de probabilidade condicional (COOPER; HERSKOVITS, 1992). A probabilidade condicional (P_rC) numericamente quantifica a relação causa-efeito (MURPHY, 2007).

Assim, considerando-se $X_1, X_2, ..., X_n$ como os nós de uma rede Bayesiana e tomando-se da estrutura desta rede as situações onde se tem dependência condicional, através da equação (3.1), permite-se determinar a probabilidade conjunta de todos os nós (NILSSON, 1998; RUSSELL; NORVIG, 1995).

$$P(X_1, X_2, \ldots, X_n) = \prod_{i=1}^{n} P(X_i \mid pa(X_i)) \qquad (3.1)$$

Uma BN é uma tripla $BN = (V, F, P)$ onde:

- ✓ $V = \{X_1, ..., X_n\}$ corresponde a um conjunto finito de nós da rede, representados por círculos;
- ✓ F corresponde a um conjunto finito de arcos orientados. Pode-se dizer que $G(V,F)$ é uma estrutura que representa um grafo acíclico orientado;
- ✓ P é a distribuição de probabilidade, determinada com o emprego da equação (3.1).

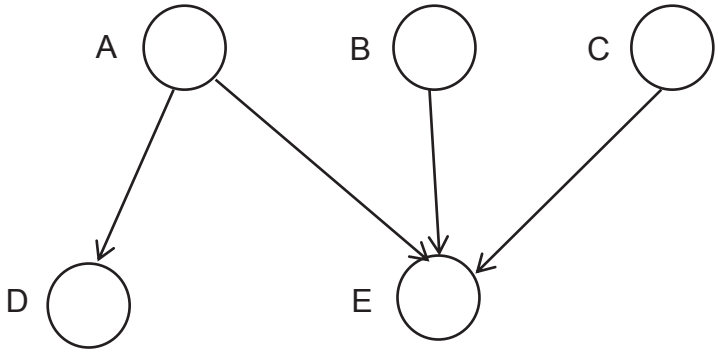


Figura 3.11 - Estrutura de uma BN.

A Figura 3.11 mostra um exemplo de uma rede Bayesiana. Neste exemplo, a estrutura da BN estabelece a influência causal das variáveis *A*, *B* e *C* sobre as variáveis *D* e *E*. O conjunto *V = {A, B, C, D, E}* é o conjunto de variáveis do sistema.

3.2.2 Construção da rede Bayesiana

No processo de construção da BN é necessário calcular as probabilidades condicionais (parâmetros numéricos) e identificar a estrutura da rede, ou seja, identificar variáveis e as relações de dependência causa – efeito, dadas pelos arcos (HRUSCHKA, 2003).

O processo de construção é dividido em duas partes: aprendizagem da estrutura (relações entre as variáveis); e a aprendizagem dos parâmetros numéricos (probabilidade condicional). Ambas as partes, estrutura e parâmetros podem ser aprendidas por meio de um especialista e indutivamente.

Por aprendizagem com especialista entende-se que o conhecimento será transmitido por meio de um especialista, que é responsável por definir e/ou supervisionar a construção da rede baseando-se em seu conhecimento ou conhecimento de outros. Já a aprendizagem indutiva, utiliza-se de um banco de dados obtido através de operações passadas, e partindo deste a rede é construída automaticamente.

Em Darwiche (2010) é citado que existem alguns métodos para a construção da rede Bayesiana a partir da aprendizagem da estrutura da rede e a partir da aprendizagem numérica ou das probabilidades condicionais entre as variáveis. Um método largamente subjetivo e que reflete o conhecimento humano é usado para

capturar as relações causais entre as varáveis e representá-las graficamente através da BN. Outro método para a construção da BN é baseada em aprendizagem a partir de um banco de dados. (DARWICHE, 2010). No contexto deste trabalho, utiliza-se o método de aprendizagem da estrutura da BN, pois se está interessado nas relações causa – efeito entre as variáveis num determinado domínio de interesse.

3.2.3 Aprendizagem da estrutura da rede Bayesiana

Segundo Hruschka (2003), para a aprendizagem da estrutura existem várias metodologias na literatura, sendo que cada uma é melhor em um tipo de aplicação. Adicionalmente, Cheng et al. (1998) citam que nas últimas décadas, muitos algoritmos de aprendizagem de estrutura de BN têm sido desenvolvidos. Estes algoritmos geralmente são divididos em dois grupos: pesquisa e pontuação (*search & scoring*) e análises de dependência. Um resumo destes algoritmos, assim como, suas vantagens e desvantagens podem ser encontrados em (CHENG; BELL; LIU, 1998). Dentre o grupo de algoritmos de aprendizagem de estrutura baseados em pesquisa e pontuação, destaca-se o algoritmo *Bayesian-score* (*K2*) desenvolvido por Cooper e Herskovitz (1992).

3.2.3.1 K2

O algoritmo *K2* requer uma ordenação das variáveis e faz uso de um método de pontuação Bayesiana para alcançar seu objetivo, que é encontrar a estrutura da rede Bayesiana (G) mais provável, dado um conjunto de dados D. Logo, o que este algoritmo pesquisa é o maior valor possível de probabilidade condicional.

Admitindo que uma BN que tem uma estrutura gráfica G e probabilidades condicionais (associadas à estrutura), Cooper e Herskovits (1992), determinaram uma fórmula para calcular a probabilidade P(G|D), supondo que nenhum conjunto de probabilidades condicionais é preferido para uma estrutura G antes de se analisar a base de dados.

A idéia do algoritmo é representar um problema com *n* variáveis através da existência de $2^{n(n-1)/2}$ possíveis estruturas, podendo escolher aquela estrutura que melhor representa o problema por meio da seguinte equação (3.2) (MURPHY, 2007).

$$P(G|D)= c\prod_{i=1}^{n}\prod_{j=1}^{qi}\frac{(ri-1)!}{(Nij+ri-1)!}\prod_{k=1}^{ri} Nijk\ ! \qquad (3.2)$$

Na equação (3.2), *n* é o número de variáveis, r_i é a quantidade total de possíveis valores que a variável X_i *(i = 1, ... , n)* pode assumir, *D* é uma base de dados com *m* observações (casos). O conjunto de pais da *i-ésima* variável X_i é representado por π_i. A *j-ésima* conFiguração dos pais de X_i é representada por w_{ij} e o número total de possíveis conFigurações dos pais π_i é representado por q_i. O valor de N_{ijk} representa a quantidade total de observações em *D* onde a variável X_i está no *k-ésimo* estado e os seus pais apresentam a *j-ésima* conFiguração. A constante *c* é chamada de constante de probabilidade *a priori* isto é, P(G), para cada *G*. Já N_{ij} é o número total de observações em *D* onde se tem X_i com qualquer um de seus possíveis valores e π_i com a *j-ésima* conFiguração; conforme equação (3.3):

$$Nij= \sum_{k=1}^{n} Nijk \qquad (3.3)$$

A melhor estrutura é aquela que maximiza o valor da equação (3.2)

Segundo Hruschka (2003), o algoritmo *K2* para construção da estrutura da BN, deve ser iniciado admitindo que um nó não possua pais, para então serem adicionados à rede os pais que maximizam a probabilidade da estrutura como um todo. A partir do momento em que a adição de qualquer nó não aumentar mais a probabilidade da rede, deve-se parar de inserir pais para o nó atual. Para saber quando tal probabilidade não está mais sofrendo aumento, deve-se utilizar a seguinte equação (3.4):

$$g(i,\pi_i) = \prod_{j=1}^{q_i}\frac{(r_i-1)!}{(N_{ij}+r_i-1)!}\prod_{k=1}^{r_i} N_{ijk}! \qquad (3.4)$$

De acordo com (CHENG; BELL; LIU, 1998), a grande repercussão deste algoritmo, está relacionada aos resultados precisos obtidos quando ele foi aplicado ao conjunto de dados da rede *ALARM*. Esta rede é uma referência amplamente utilizada para testes de algoritmos de aprendizado de estrutura. Partindo de um conjunto de 10.000 casos, o *K2* gerou a estrutura da rede *ALARM* com apenas um

arco a mais e, um arco faltando em aproximadamente 17 minutos, utilizando-se um computador *Macintosh II*.

O algoritmo *K2* representa um método exato de inferência, sendo relativamente simples de ser aplicado para a geração automática da BN; e também este algoritmo já está implementado no software MatLab denominado de BNToolbox (MURPHY, 2007). Desta forma, optou-se por utilizá-lo no contexto deste trabalho, conforme apresentado no Anexo A.

4 SISTEMÁTICA PROPOSTA

Apresenta-se aqui o conjunto de procedimentos sistematizados para desenvolvimento e validação de algoritmos de controle, a partir de modelagem e análise de diagnóstico e tratamento de falhas críticas em um processo industrial, em que se concebe uma camada de redução de riscos (SIS) baseada em sistemas eletrônicos programáveis (PES). Esta sistemática contempla a especificação das funções instrumentadas de segurança (SIFs), que representam falhas críticas a serem detectadas e diagnosticadas via sensores e tratadas pelo SIS via atuadores, com a finalidade de mitigar ou prevenir riscos com acidentes potencialmente altos.

Inicialmente um modelo para diagnóstico de “falhas críticas” é construído das causas → efeitos (ex.: tendo-se certeza sobre a causa de um problema, podem-se identificar quais efeitos são produzidos por esta causa). Entretanto, no raciocínio de diagnóstico, as causas são diagnosticadas baseadas nos efeitos monitorados (ex.: qual a causa mais provável baseada nos efeitos observados).

Para a modelagem de diagnósticos de falhas, são utilizados modelos gráficos, baseados na abordagem de representação de conhecimento e de raciocínio diagnóstico (LUO et al., 2005). Existem vários métodos de modelagem para capturar o comportamento do sistema sob condições de falha (ex.: rede de Petri (PN) e rede Bayesiana (BN)) (LUO et al., 2005).

No contexto de diagnóstico de falhas críticas a sistemática utiliza duas técnicas de modelagem gráficas: rede Bayesiana (BN) e rede de Petri (PN) interpretada. Adicionalmente para a coordenação e tratamento de falhas críticas, utiliza-se também a rede de Petri (PN) interpretada.

4.1 APRESENTAÇÃO DA SISTEMÁTICA

A sistemática em questão é apresentada na Figura 4.1, cujo conceito foi apresentado inicialmente em (SQUILLANTE et al., 2010a).

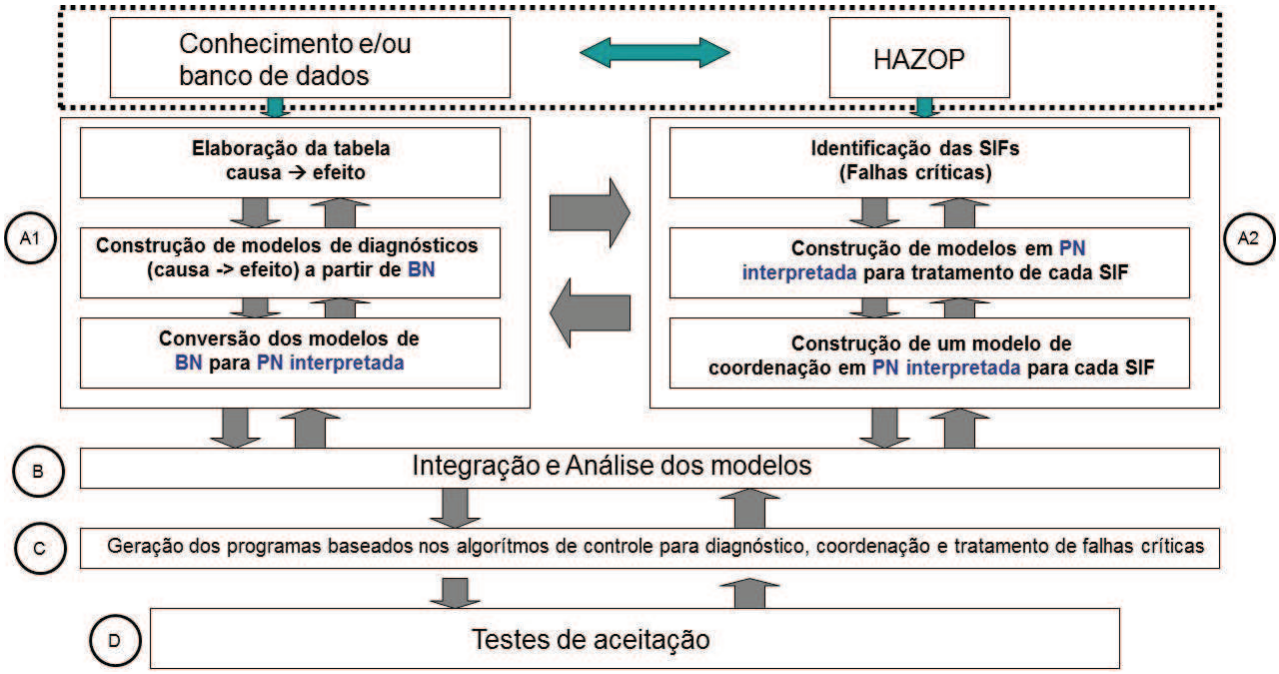


Figura 4.1 - Sistemática para o diagnóstico e tratamento de falhas críticas em SIS.

A abordagem caracteriza-se pela construção e análise de modelos de diagnóstico, coordenação e tratamento de falhas críticas considerando quatro etapas:

Etapa (A) – modelagem.

Etapa (B) – análise.

Etapa (C) - geração dos programas de controle baseados nos algoritmos de controle para diagnóstico, coordenação e tratamento de falhas críticas.

Etapa (D) - testes finais de aceitação.

A etapa de modelagem (A) é subdividida em dois estágios complementares: (A1) modelagem do diagnóstico de falhas críticas e (A2) modelagem do tratamento e coordenação de falhas críticas.

A sistemática proposta utiliza como fonte de dados de entrada: (i) relatório de análise de riscos (HAZOP), (ii) conhecimento das relações causa → efeito por um especialista ou equipe de especialistas e/ou banco de dados, conforme mostrado na Figura 4.1.

Para atender aos critérios de validação de requisitos de cada etapa durante todo o ciclo de desenvolvimento de um SIS, de acordo com a norma IEC 61511, a cada

passo de modelagem deve ser realizada uma análise das “boas” propriedades do modelo gerado. Caso seja necessário, volta-se para o passo anterior para que os devidos ajustes sejam realizados, otimizando-se assim o retrabalho durante o ciclo de desenvolvimento. A atividade de análise das propriedades e validação dos modelos para cada etapa compreende as seguintes atividades:

- Edição do modelo em PN interpretada a partir de ferramenta computacional HPSim (ANSCHUETZ, 2010). Simulação do modelo a fim de validar se o mesmo atende aos requisitos técnicos especificados e a análise da propriedade de reiniciabilidade. Para a simulação do modelo, são considerados os modelos dos dispositivos de sensoriamento e dispositivos de atuação para fechar a malha de controle.
- Edição do modelo em PN interpretada a partir de ferramenta computacional PIPE2 (BONET et al., 2007), a fim de analisar as propriedades de vivacidade e segurança (1-limitada).

A etapa de análise (B) investiga a interação entre os modelos de diagnóstico, coordenação e tratamento de falhas críticas. Novamente utilizam-se as ferramentas computacionais citadas anteriormente para análise do modelo integrado.

Na etapa (C), tem-se a geração dos programas de controle baseados nos algoritmos de controle a partir dos modelos integrados de diagnóstico, coordenação e tratamento para cada SIF, gerados na etapa (B), de acordo com a norma IEC 61131-3.

Finalmente, na etapa (D), têm-se os testes finais de aceitação que são executados a fim de validar se as SIFs e SIS atendem às especificações técnicas de acordo com a norma IEC 61511.

As etapas para a modelagem e análise do algoritmo de controle para sistemas eletrônicos programáveis (PES) de sistemas instrumentados de segurança (SIS); que considera o diagnóstico, a coordenação e o tratamento de falhas críticas utilizando a sistemática proposta, são descritas a seguir.

4.2 ETAPA A1: MODELAGEM DO DIAGNÓSTICO DE FALHAS CRÍTICAS

Passo 1: *Elaboração de Tabela de relação causa → efeito*.

Neste passo, constrói-se uma Tabela que relaciona as causas (*falhas críticas*) definidas para cada SIF; e os efeitos (sinais de *sensores*) observados quando estas causas ocorrem. O critério para construção desta Tabela pode ser:

- baseado em conhecimento extraído do sistema, onde as relações entre as variáveis são estabelecidas por um especialista ou grupo de pessoas especialistas;
- baseado em especificações técnicas do projeto de SIS, como por exemplo: memorial descritivo, diagrama de processo e instrumentação (P&ID), relatório de análise de riscos e matriz de causa x efeito ou;
- baseado em um banco de dados com registros de falhas obtidos a partir de um histórico de operações ou experimentos em campo.

A Tabela de relação causa → efeito é construída da seguinte forma: (i) a primeira coluna representa o número do caso do relacionamento causa – efeito, (ii) as colunas a seguir representam as causas ou falhas críticas (considerar uma coluna para cada falha crítica); (iii) as demais colunas representam os estados binários dos sinais dos sensores e que representam os efeitos que foram observados quando da ocorrência das falhas críticas (considerar uma coluna para cada efeito). Os valores binários associados aos sensores são baseados nos limiares máximos e mínimos permitidos dentro de uma faixa de operação segura: o valor 0 significa operação segura e o valor 1 significa “desvios” de processo que colocam o mesmo em um estado de operação não seguro.

Passo 2: *Construção de modelos de relacionamento causa -> efeito baseados em BN*.

Neste passo, utiliza-se a Tabela causa → efeito obtida no passo 1, para a construção da estrutura inicial do modelo de relacionamento (causa → efeito) em rede Bayesiana (BN).

A construção deste modelo de relacionamento (causa →efeito) é realizada através do conhecimento ou da aplicação de algoritmos de aprendizagem de estrutura da BN.

Uma vez obtida a estrutura inicial da BN por meio de um algoritmo de aprendizagem, são consideradas restrições baseadas no conhecimento de relacionamento entre as variáveis. As restrições que devem ser consideradas são:

- Eliminação de arcos de relacionamento entre as causas. Considerando que o sistema que é o objeto de controle deve ser degenerado imediatamente mediante a ocorrência de qualquer uma das falhas criticas previstas, então não é pertinente haver o relacionamento entre estas falhas na BN, pois uma vez degenerado, o comportamento dinâmico do sistema que foi considerado para a geração da BN deixa de ser válido;
- Eliminação e inserção de novos arcos de relacionamento, caso as relações na BN não estejam de acordo com as especificações técnicas e/ou conhecimento sobre estas relações.

Passo 3: *Conversão dos modelos em BN para PN interpretada.*

Embora os modelos em BN representem uma estrutura que relaciona as causas como sendo as *falhas críticas*, com os efeitos monitorados através dos sinais de sensores, as causas devem ser diagnosticadas baseadas nos efeitos monitorados, ou seja, uma relação (efeito → causa) deve ser estabelecida (exemplo: qual a causa mais provável baseada nos efeitos observados). Por outro lado, a fim de implementar o algoritmo de controle de diagnóstico das falhas críticas em um PES de um SIS, os modelos em BN devem ser convertidos para modelos gráficos com formalismo das rede de Petri (PN). Neste contexto, esta sistemática adota a execução da seguinte atividade:

- ✓ Conversão dos modelos de diagnósticos em rede Bayesiana (BN) para modelos de descrição do diagnóstico em rede de Petri (PN) interpretada.

O objetivo desta atividade é converter um modelo de diagnóstico em BN para um modelo de descrição do diagnóstico que tenha o formalismo da rede de Petri e que possa ser implementado em um algoritmo de controle para diagnóstico, afim de:

- fornecer uma interpretação aos lugares e transições da PN com relação às variáveis internas e variáveis externas (sinais de sensores); facilitando a conversão desta rede para um algoritmo de controle.
- fornecer uma relação lógica entre as variáveis externas (sinais de sensores) por meio de transições da rede de Petri
- analisar as "boas propriedades" da PN a partir de simulação por meio de ferramenta computacional;
- validar o modelo com base na especificação técnica, a partir de simulação por meio de ferramenta computacional.

Esta atividade é executada, observando-se as seguintes situações:

a) obtenção das relações causais de dependência a partir da rede Bayesiana derivada para cada SIF.
b) obtenção das relações lógicas entre as variáveis externas (sinais de sensores) a partir da relação causal.
c) construção do modelo em PN interpretada obtendo-se uma estrutura efeito → causa, a fim de representar um modelo de diagnóstico a partir do raciocínio abductivo.
d) durante a construção da PN interpretada, considerar que o modelo deve permitir sua reinicialização a fim de atender a propriedade de reiniciabilidade exigida para esta rede e considerar também a possibilidade da falha ser espúria, ou seja, a possibilidade de o diagnóstico não ser efetivado.
e) representação no modelo, dos eventos associados às transições, indicando em particular, os eventos que exigem uma interação com o ambiente externo (ex.: sinais de sensores e atuadores).

No final desta sub etapa A1; têm-se modelos de diagnósticos construídos em PN interpretada, que podem ser editados e simulados usando, por exemplo, a ferramenta computacional HPSim (ANSCHUETZ, 2010), com o propósito de validação se os mesmos atendem aos requisitos técnicos especificados e a análise da propriedade de reiniciabilidade de cada modelo. Para a simulação do modelo de diagnóstico, são considerados os modelos dos dispositivos de sensoriamento para representar o controle de malha fechada que deve ser executado. Finalmente, a fim

de se analisar as propriedades de vivacidade e segurança, pode-se utilizar, por exemplo, a ferramenta computacional PIPE2 (BONET et al., 2007).

4.3 ETAPA A2: MODELAGEM DO TRATAMENTO E COORDENAÇÃO DE FALHAS CRÍTICAS

Passo 1: *Identificação das SIFs*.

A partir de um estudo de análise de riscos (ex.: HAZOP), previsto no início do ciclo de vida de segurança (IEC 61508, 1998; IEC 61511, 2003), um relatório é gerado. Neste relatório, encontram-se os seguintes dados:

- ✓ Identificação da SIF;
- ✓ Descrição da SIF;
- ✓ Consequências devidas à falha;
- ✓ SIL;
- ✓ eventos inicializadores (sinais de sensores);
- ✓ ações a serem executadas pelo SIS (sinais para os atuadores), a fim de prevenir ou mitigar riscos.

Neste passo, é elaborada uma Tabela baseada nos dados obtidos do relatório. A Tabela deverá conter os seguintes campos: identificação das SIFs, descrição das "falhas críticas", consequências devidas à falha, SIL, eventos inicializadores e ação a ser executada pelo SIS. A partir desta Tabela, identificam-se informações importantes para a construção dos modelos de tratamento:

- as "falhas críticas" que estão associadas a cada SIF;
- as ações a serem executadas pelo SIS para cada SIF que são definidas a partir das regras de tratamento de cada SIF e consequentemente de cada "falha crítica".

Passo 2: *Construção do modelo de tratamento para cada SIF em PN interpretada*.

Neste passo, três atividades são executadas:

- ✓ construção dos modelos de tratamento, em rede de Petri interpretada, para cada “falha crítica”, conforme as regras de tratamento obtidas no passo anterior.
- ✓ Edição e simulação do modelo de tratamento, usando, por exemplo, a ferramenta computacional HPSim, com o propósito de validação e análise da propriedade de reiniciabilidade. Para a simulação do modelo de tratamento, são considerados os modelos dos dispositivos de sensoriamento e dos dispositivos de atuação.
- ✓ Edição do modelo de tratamento, usando, por exemplo a ferramenta computacional PIPE2, a fim de analisar as propriedades de vivacidade e segurança (1-limitada).

Passo 3: *Construção do modelo de coordenação em PN interpretada para cada SIF*.

A função do modelo de coordenação é determinar qual algoritmo de tratamento de falha crítica deve ser executado em função do diagnóstico inferido. Neste contexto, não há prioridade para o tratamento das falhas e o processamento ocorre de forma independente de acordo com o resultado do algoritmo de diagnóstico.

Este modelo é construído de tal forma que sua implementação seja robusta quanto à ocorrência de falhas espúrias. As falhas espúrias, neste contexto, estão relacionadas com possíveis informações “falsas” provenientes de sensores mal calibrados. (ex.: um sensor indica que uma variável está fora da faixa de operação segura por um intervalo de tempo pequeno e retorna para uma faixa segura de operação). Se o modelo de coordenação não for robusto à ocorrência de falhas espúrias, o modelo de tratamento será executado indevidamente, ocasionando uma degeneração indevida do processo industrial e consequentemente uma parada de produção. Uma das soluções empregadas para a implementação de um modelo robusto à ocorrência de falhas espúrias e que é aplicada neste trabalho, é por meio de transições temporizadas da PN.

As atividades a seguir são executadas:

- ✓ Construção de um modelo de coordenação para cada SIF usando a técnica de rede de Petri interpretada. Uma vez que uma causa de um problema é

diagnosticada pelo modelo de diagnóstico, o modelo de coordenação é responsável pela chamada do modelo de tratamento respectivo, a fim de prevenir ou mitigar um acidente.

- ✓ Edição e simulação de cada modelo de coordenação, usando, por exemplo, a ferramenta computacional HPSim (ANSCHUETZ, 2010) a fim de validar se o modelo atende aos requisitos técnicos especificados, e a análise da propriedade de reiniciabilidade é atendida.
- ✓ Edição de cada modelo de coordenação, usando, por exemplo, a ferramenta computacional PIPE2 (BONET et al., 2007) e análise das propriedades de vivacidade e segurança.

4.4 ETAPA B: INTEGRAÇÃO E ANÁLISE DOS MODELOS EM PN

Neste passo, os modelos em PN interpretada para diagnóstico, coordenação e tratamento de falhas críticas são integrados para compor o modelo geral de uma SIF. A integração entre os modelos de diagnóstico, coordenação e tratamento é feita a partir de conexões lógicas, uma vez que não deve haver fluxo de marcas da PN entre os modelos.

Uma vez que os modelos são integrados executam-se as seguintes atividades:

- ✓ Edição e simulação de cada modelo de SIF obtido, usando, por exemplo, a ferramenta computacional HPSim (ANSCHUETZ, 2010) a fim de validar se o modelo atende aos requisitos técnicos especificados, e se a propriedade de reiniciabilidade é atendida. Para a simulação dos modelos, são considerados os modelos dos dispositivos de sensoriamento e dos dispositivos de atuação para fechar a malha de controle.
- ✓ Edição de cada modelo de SIF obtido, usando, por exemplo, a ferramenta computacional PIPE2 (BONET et al., 2007) e análise das propriedades de vivacidade e segurança.

4.5 ETAPA C: GERAÇÃO DOS PROGRAMAS BASEADOS NOS ALGORITMOS DE CONTROLE

O controlador programável (CP) é um equipamento essencial na implementação de sistemas de controle industriais e normas têm sido estabelecidas (IEC 61131, 2003) para uso deste equipamento. Estas normas representam um passo relevante para o desenvolvimento do sistema de controle, entretanto, elas são insuficientes para a análise e validação das estratégias de controle (FREY; LITZ, 2000). Esta observação pode ser expandida para sistemas de controle de segurança, pois, a norma IEC 61508 identifica o CP também como sistema eletrônico programável (PES) (SQUILLANTE et al., 2010b). Neste contexto, em Frey e Litz (2000), são apresentadas várias razões para a aplicação de métodos adequados para o desenvolvimento de algoritmos de controle de CPs, tais como:

- a crescente complexidade do problema de controle;
- a demanda pela redução do tempo de desenvolvimento;
- a demanda pela possibilidade de reutilização de módulos de software existentes;
- a demanda por soluções de alta qualidade, especialmente para condições de segurança que necessitam de procedimentos de análise e validação.

Assim, nesta etapa, tem-se a conversão dos modelos integrados de diagnóstico, coordenação e tratamento de falhas criticas para cada SIF, gerados na etapa anterior, para programas de controle que implementam os algoritmos de controle em linguagens de programação definidas na IEC 61131-3 (2003) destacando-se: diagrama ladder (LD), diagrama de blocos de função (FBD) e gráfico de sequenciamento das funções (SFC).

A conversão é feita de forma sistemática e isomórfica. Muitos trabalhos de pesquisa têm sido publicados sobre metodologias para a conversão de modelos em PN para programas em linguagens de programação definidas na IEC 61131-3 (LEE et al., 2004; MUSIC et al., 2005; THAPA et al., 2005; WIGHTKIN et al., 2010).

Não faz parte do escopo deste trabalho, comparar as metodologias existentes, porém destaca-se que para a execução desta etapa, de maneira formal, deve-se

seguir uma determinada metodologia para a geração dos programas de controle baseados nos algoritmos de controle.

4.6 ETAPA D: TESTES DE ACEITAÇÃO

De acordo com as normas IEC 61508 (1998) e IEC 61511 (2003), uma das atividades do ciclo de vida de segurança de projeto de SIS, está relacionada com os testes finais de aceitação executados via *comissionamento* e *start-up*. As seguintes condições devem ser verificadas "*a priori"* para que esta etapa seja executada:

- ✓ O sistema eletrônico programável (PES), suas interfaces de entradas e saídas e demais componentes e acessórios devem estar devidamente instalados na sala de controle;
- ✓ Os sensores de segurança devem estar conectados às interfaces de entrada do PES;
- ✓ Os atuadores de segurança devem estar conectados às interfaces de saída do PES;
- ✓ Os programas de controle baseados nos algoritmos de controle para diagnóstico, coordenação e tratamento de falhas críticas, gerados na etapa anterior, devem ser transferidos para a memória de programa do PES;

A atividade de *comissionamento* deve ser executada com o objetivo de:

- ✓ testar o estado de funcionamento dos sensores de segurança;
- ✓ testar o estado de funcionamento dos atuadores de segurança;
- ✓ testar a instalação destes sensores e atuadores nas interfaces de entradas e saídas do PES;
- ✓ testar o estado de funcionamento das interfaces de entradas e saídas;
- ✓ testar o estado de funcionamento do PES;
- ✓ analisar se o programa de controle baseado no algoritmo de controle atende a especificação técnica para diagnóstico e tratamento das SIFs. Esta análise é

feita para cada SIF, a partir de simulações das entradas (sensores), por combinações conhecidas, e observação dos respectivos atuadores.

A atividade de *start-up* deve ser executada com o objetivo de:

- ✓ colocar o BPCS e o sistema instrumentado de segurança (SIS) do processo industrial em operação;
- ✓ acompanhar a partida inicial de cada equipamento e/ou sistema; conforme planejamento pré-definido por equipe de engenharia e operação.

Na abordagem deste trabalho, esta etapa é realizada de acordo com a recomendação das normas IEC 61508 (1998) e IEC 61511 (2003), embora se observe que não existe um método formal para a execução da mesma.

5 APLICAÇÃO DA SISTEMÁTICA PROPOSTA

Neste capítulo é apresentado um exemplo de aplicação que considera SIFs provenientes de um relatório de análise de riscos (HAZOP) de um projeto de uma estação de compressão (ECOMP) de gás natural - Figura 5.1. Este caso foi utilizado para a avaliação da sistemática proposta neste trabalho. O gás natural é uma mistura de hidrocarbonetos leves e altamente inflamáveis. Neste contexto, este processo envolve diversos riscos com magnitude *inaceitável*. Daí a necessidade de se projetar uma camada de redução destes riscos (SIS).

Figura 5.1 - Estação de Compressão de Gás – ECOMP.
Fonte: http://www.bonatti.it/Projects/Mellitah-Gas-Compression-Station, acessada em 15/02/2011.

5.1 DESCRIÇÃO DO PROCESSO

A ECOMP possui várias linhas de alimentação de gás, denominadas de *linhas de sucção*, provenientes de um gasoduto de transporte deste gás. O gás na entrada da estação de compressão passa por filtros, antes de ser comprimido por meio de equipamentos denominados de turbos compressores. Uma parte deste gás é

desviada para uma unidade denominada *utilidades*. A unidade *utilidades* é responsável pelo controle de temperatura e pressão do gás a ser utilizado por outros equipamentos essenciais à operação deste processo, tais como: gás de partida e gás combustível para os turbos compressores e aquecedores e, adicionalmente, gás combustível para a geração de energia elétrica no processo. Após o gás ser comprimido pelos turbos compressores, ele é retornado para o gasoduto por meio de uma *linha de descarga*. A Figura 5.2 mostra um Diagrama de Processo e Instrumentação (P& ID)[13] da linha de entrada de gás na ECOMP (*linha de sucção 1)*, a Figura 5.3 mostra o P&ID de outra linha de entrada de gás na ECOMP (linha de sucção 2) e a Figura 5.4 mostra o P&ID da *linha de descarga* na saída da ECOMP.

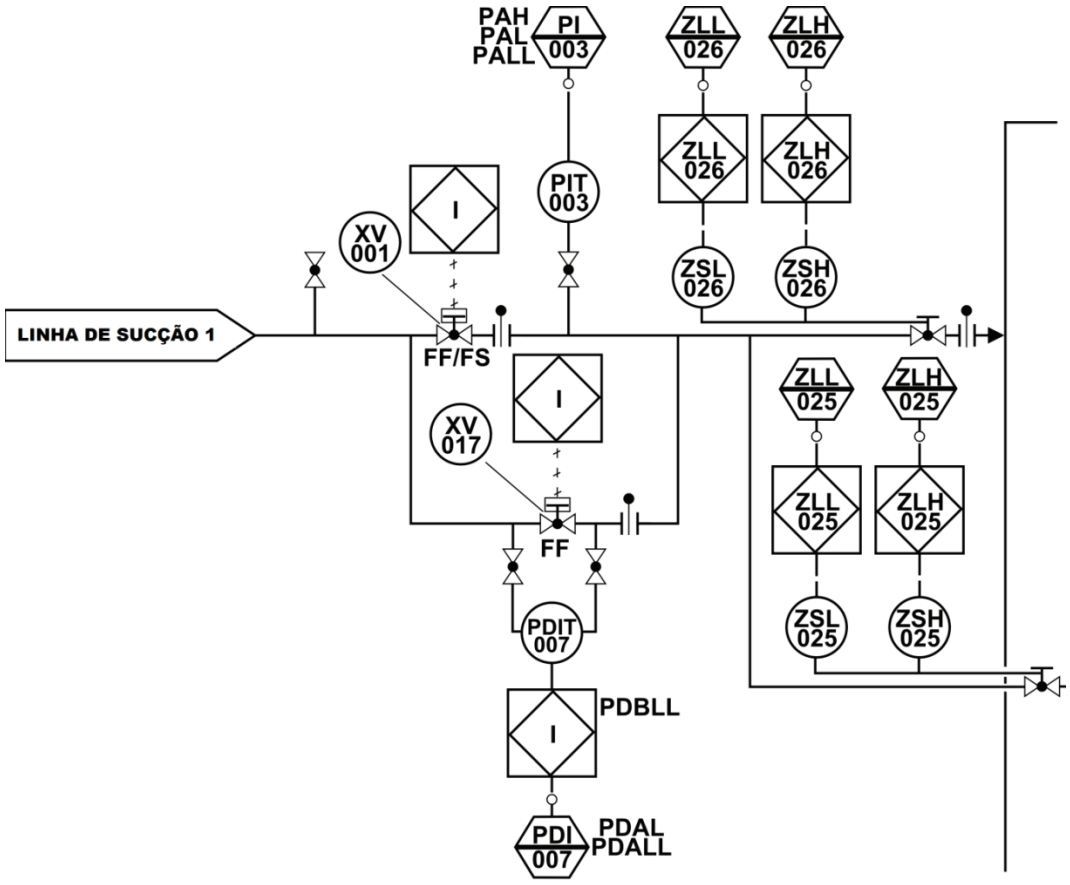


Figura 5.2 - P&ID da linha de sucção 1 na entrada da ECOMP.

13 A simbologia dos instrumentos de processo das Figuras 5.2, 5.3 e 5.4, estão de acordo com a norma ANSI/ISA-S5.1-1984 (R1992) – *Instrumentation Symbols and Identification.* Esta norma foi concebida para ser uma padronização de simbologia e identificação de instrumentos e equipamentos de processo; sendo atualmente sua abrangência a nível mundial. Esta norma é utilizada na elaboração dos seguintes documentos: (i) Fluxogramas de Processo e Mecânico, (ii) Diagramas de Processo e Instrumentação, (iii) Especificações e Listas de instrumentos e (iv) Identificação de Instrumentação e Funções de controle.

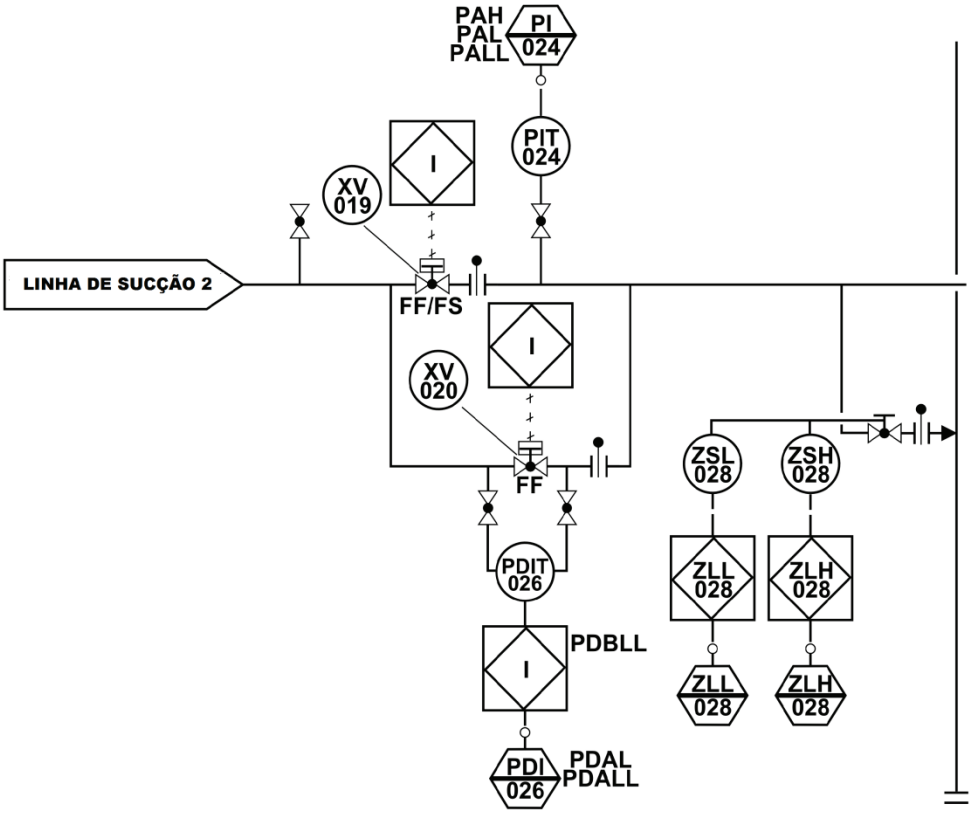


Figura 5.3 - P&ID da linha de sucção 2 na entrada da ECOMP.

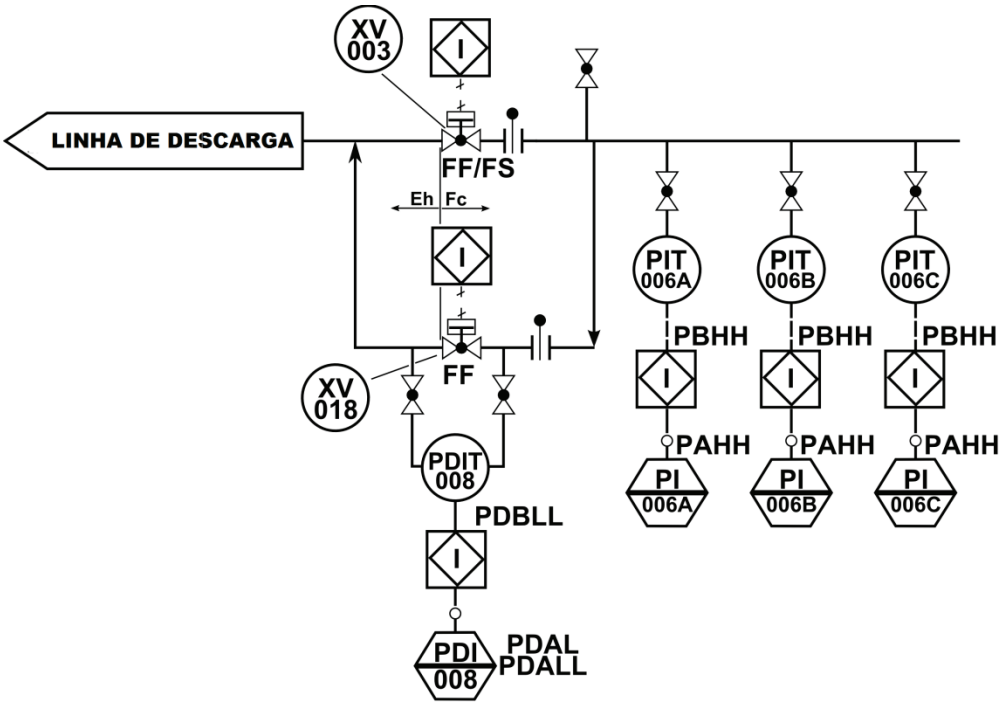


Figura 5.4 - P&ID da linha de descarga na saída da ECOMP.

5.2 ARQUITETURA DO SISTEMA DE CONTROLE

A arquitetura do sistema de controle da ECOMP é mostrada via diagrama de blocos na Figura 5.5. O CP ESC corresponde ao BPCS, que é o sistema de controle básico do processo, e que faz parte da unidade *utilidade* descrita anteriormente. Todos os sensores, atuadores e equipamentos relacionados com a unidade *utilidade* do processo, estão integrados com o BPCS. Adicionalmente, cada turbo compressor tem um controlador programável (CP) local. Como existem na ECOMP quatro turbos compressores, os CPs são denominados :

- CP-TC_A : Controlador Programável do turbo compressor A
- CP-TC_B : Controlador Programável do turbo compressor B
- CP-TC_C : Controlador Programável do turbo compressor C
- CP-TC_D : Controlador Programável do turbo compressor D

Finalmente, um controlador programável de segurança (CP segurança), compõe o sistema de controle responsável pela camada de redução de riscos (SIS) da ECOMP. Os sensores e atuadores de segurança da ECOMP estão integrados com o SIS, cuja função é garantir a *segurança funcional* neste processo. Para monitoração das variáveis de processo e indicação de alarmes, foram definidas duas Interfaces Homem Máquina (IHM). Adicionalmente, foi instalada uma Estação de Engenharia com ferramentas de modificação e implementação de telas gráficas nas IHMs.

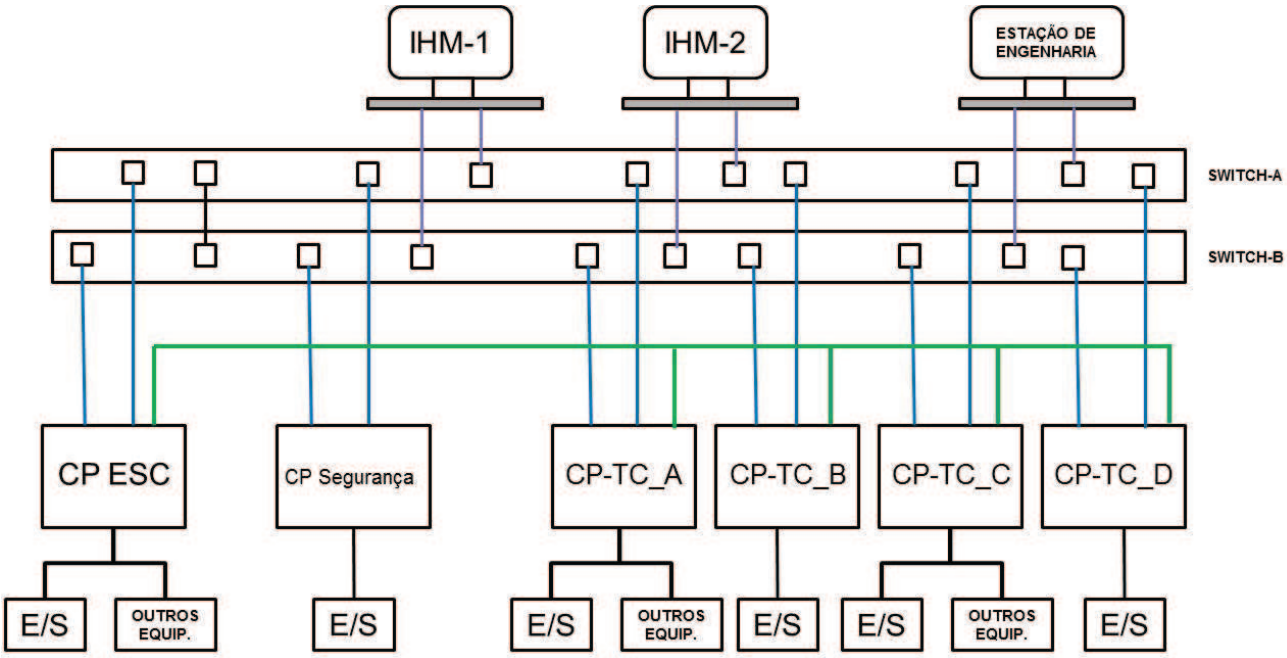


Figura 5.5 - Arquitetura do Sistema de Controle da ECOMP.

5.3 APLICAÇÃO DA SISTEMÁTICA PROPOSTA

5.3.1 Etapa A1: Modelagem do diagnóstico de falhas críticas

5.3.1.1 Passo 1: Elaboração de Tabela de relação causa → efeito

O passo 1 foi executado com base em conhecimento extraído do sistema; onde as relações entre as variáveis foram estabelecidas por grupos de pessoas especialistas; formados pelas equipes de operação, engenharia e manutenção. A Tabela 5.1 mostra a relação causa → efeito e a Tabela 5.2 mostra a descrição dos eventos associados às colunas apresentadas na Tabela 5.1.

Tabela 5.1 - Relação causa → efeito.

Causa	Falha 1	Falha 2	Falha 3	Falha 4	PSHH-006A	PSHH-006B	PSHH-006C	LSHH-006	LSHH-007	PDSHH-005	LSHH-013	LSHH-014	PDSHH-025	PSHH-207A	PSHH-207B	PSHH-207C	PSHH-207D	TSHH-209A	TSHH-209B	TSHH-209C	TSHH-209D
1	1	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	1	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	1	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	1	0	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	0	1	0	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	0	0
6	0	1	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0
7	0	1	0	0	0	0	0	1	1	0	1	1	0	0	0	0	0	0	0	0	0
8	0	1	0	0	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	0
9	0	1	0	0	0	0	0	0	1	1	0	1	1	0	0	0	0	0	0	0	0
10	0	1	0	0	0	0	0	1	0	1	1	0	1	0	0	0	0	0	0	0	0
11	0	1	0	0	0	0	0	1	1	1	1	1	1	0	0	0	0	0	0	0	0
12	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0
13	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0
14	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0
15	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0
16	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0
17	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0
18	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	0	0	0
19	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0
20	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	1	0	0	0	0
21	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0
22	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	1	1	0	0	0	0
23	0	0	1	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0
24	0	0	1	0	0	0	0	0	0	0	0	0	0	1	1	0	1	0	0	0	0
25	0	0	1	0	0	0	0	0	0	0	0	0	0	1	1	1	0	0	0	0	0
26	0	0	1	0	0	0	0	0	0	0	0	0	0	1	1	1	1	0	0	0	0
27	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
28	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
29	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1
30	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
31	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1
32	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0
33	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1
34	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0
35	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1
36	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0
37	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	1
38	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0
39	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	1
40	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0
41	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1

Tabela 5.2 - Descrição das colunas apresentadas na Tabela 5.1.

Coluna	Descrição
Falha 1	Pressão muito alta na descarga da ECOMP
Falha 2	Nível de condensado muito alto nos filtros da ECOMP
Falha 3	Pressão muito alta na descarga dos turbos compressores A / B / C e D
Falha 4	Temperatura muito alta na descarga dos turbos compressores A / B / C e D
PSHH-006A	Desvio de pressão muito alta proveniente do sensor PIT-006A
PSHH-006B	Desvio de pressão muito alta proveniente do sensor PIT-006B
PSHH-006C	Desvio de pressão muito alta proveniente do sensor PIT-006C
LSHH-006	Desvio de nível muito alto de condensado no filtro A, proveniente do sensor LIT-006
LSHH-007	Desvio de nível muito alto de condensado no filtro A, proveniente do sensor LIT-007
PDSHH-005	Desvio de pressão diferencial muito alta no filtro A, proveniente do sensor PDIT-005
LSHH-013	Desvio de nível muito alto de condensado no filtro B, proveniente do sensor LIT-013
LSHH-014	Desvio de nível muito alto de condensado no filtro B, proveniente do sensor LIT-014
PDSHH-025	Desvio de pressão diferencial muito alta no filtro B, proveniente do sensor PDIT-025
PSHH-207A	Desvio de pressão muito alta na descarga do turbo compressor A, proveniente do sensor PIT-207A
PSHH-207B	Desvio de pressão muito alta na descarga do turbo compressor B, proveniente do sensor PIT-207B
PSHH-207C	Desvio de pressão muito alta na descarga do turbo compressor C, proveniente do sensor PIT-207C
PSHH-207D	Desvio de pressão muito alta na descarga do turbo compressor D, proveniente do sensor PIT-207D
TSHH-209A	Desvio de temperatura muito alta na descarga do turbo compressor A, proveniente do sensor TIT-209A
TSHH-209B	Desvio de temperatura muito alta na descarga do turbo compressor B, proveniente do sensor TIT-209B
TSHH-209C	Desvio de temperatura muito alta na descarga do turbo compressor C, proveniente do sensor TIT-209C
TSHH-209D	Desvio de temperatura muito alta na descarga do turbo compressor D, proveniente do sensor TIT-209D

Na Tabela 5.1, as colunas denominadas de Falha 1, Falha 2, Falha 3 e Falha 4, são consideradas as causas e as demais colunas representam os estados binários de sensores, que foram observados na ocorrência das referidas falhas, representando, portanto, os efeitos. Na Tabela 5.1, todos os valores são binários (ex:

0 = Off, 1 = On), com exceção da primeira coluna, onde os números representam o número de casos obtidos para as falhas críticas que estão sendo consideradas. As colunas 2, 3, 4 e 5 definem as falhas críticas denominadas de Falha 1, Falha 2, Falha 3 e Falha 4 a serem diagnosticadas. As colunas restantes, representam os valores binários dos estados dos sensores quando uma falha crítica ocorre.

Para a elaboração da Tabela 5.1, foram considerados os seguintes documentos que fazem parte da especificação técnica do sistema de controle e da camada de redução de risco:

- Diagrama do processo e instrumentação (P&ID);
- Memorial descritivo do processo;
- Relatório final de análise de riscos (HAZOP);
- Matriz Causa x Efeito.

5.3.1.2 Passo 2: Construção de modelos de relacionamento causa → efeito baseados em rede Bayesiana (BN)

O passo 2 foi executado baseado na utilização de um algoritmo de aprendizagem de rede Bayesiana (BN) e a partir da Tabela 5.1 de relacionamento causa → efeito obtida no passo 1. O algoritmo utilizado para a aprendizagem da BN foi o K2 (busca e pontuação), citado na seção 3.2.3. O programa computacional baseado no algoritmo K2 utilizado para a construção da BN é apresentado no Anexo A e a Figura 5.6 mostra a estrutura inicial da BN construída a partir do algoritmo K2.

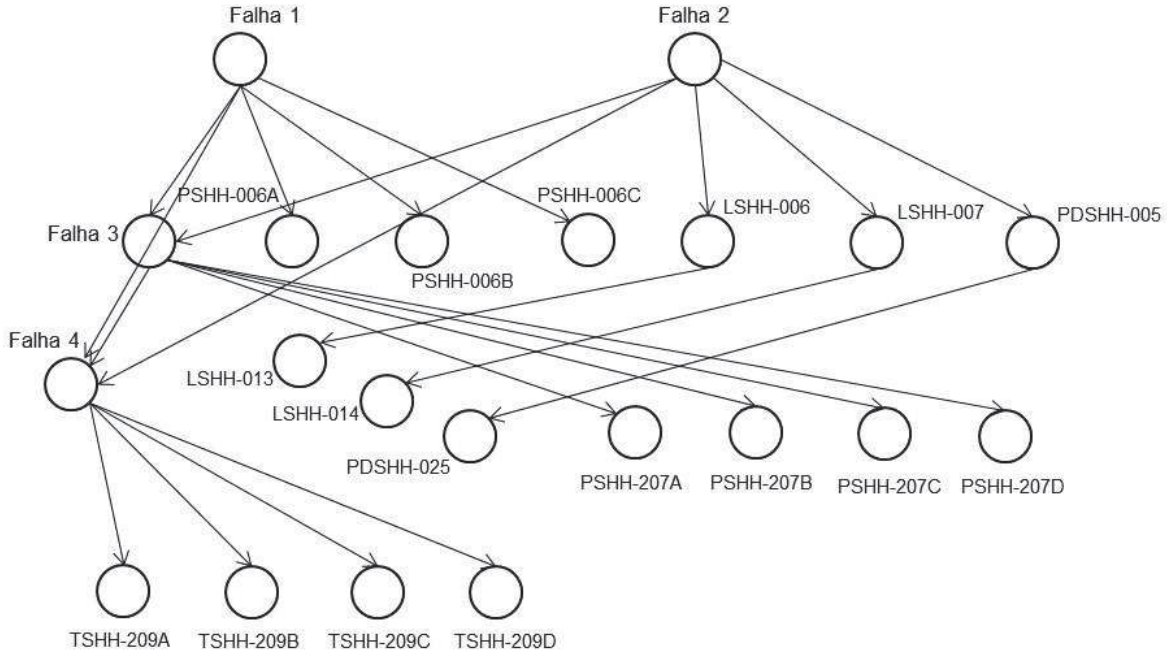


Figura 5.6 - Estrutura inicial da BN construída a partir do algoritmo K2.

Uma vez obtida a estrutura inicial da BN através do algoritmo de aprendizagem K2, foram consideradas as restrições baseadas no conhecimento de relacionamento entre as variáveis. As restrições consideradas neste exemplo foram:

- Eliminação de arcos de relacionamento entre as causas, uma vez que as causas constituem um conjunto de nós pais da rede Bayesiana, tal que, a independência condicional entre os nós pais deve ser satisfeita.
- Eliminação e inserção de novos arcos de relacionamento, na estrutura de relacionamento entre a variável (Falha 1) e seus descendentes: (PSHH-006A, PSHH-006B e PSHH-006C). Esta modificação deve-se ao fato de que está sendo adotado um sistema de votação “2oo3” entre os sensores PIT-006A, PIT-006B e PIT-006C para a confirmação da Falha 1, de acordo com os requisitos especificados a partir do estudo de HAZOP.

Portanto, a estrutura de relacionamento baseada em um sistema de votação “2oo3” entre os sensores relacionados com a Falha 1 é mostrada na Tabela 5.3.

Tabela 5.3 - Sistema de votação “2oo3”.

Falha 1	PSHH-006A	PSHH-006B	PSHH-006C
1	1	1	0
1	1	0	1
1	0	1	1
1	1	1	1

Desta forma, aplicadas as regras acima, a BN resultante é mostrada na Figura 5.7.

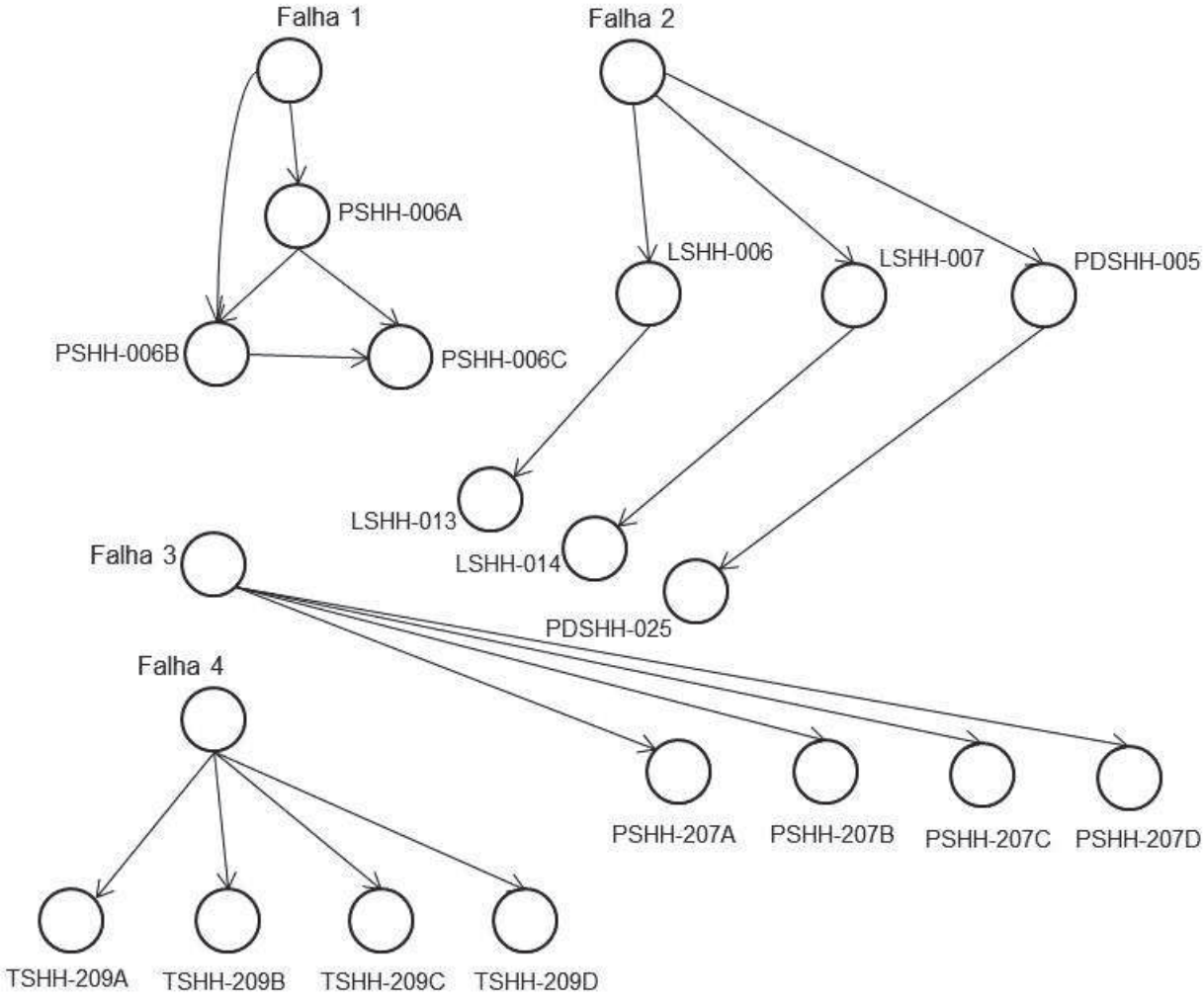


Figura 5.7 - BN resultante.

5.3.1.3 Passo 3: Conversão dos modelos em BN para PN interpretada

Os modelos resultantes de diagnósticos em BN, obtidos no passo anterior foram convertidos para modelos de diagnóstico em PN interpretada. Desta forma:

a) obteve-se as relações causais de dependência a partir da BN.

b) obteve-se as relações lógicas entre as variáveis externas (sensores) a partir da relação causal.

c) cada modelo em PN interpretada foi construído obtendo-se uma estrutura efeito → causa, a fim de representar um modelo de diagnóstico baseado em raciocínio abductivo.

d) durante a construção da PN interpretada, considerou-se que o modelo deve permitir sua reinicialização a fim de atender a propriedade de reiniciabilidade exigida para esta rede.

e) os eventos associados às transições da PN, em particular os eventos que exigem uma interação com o ambiente externo (ex.: sinais de sensores e atuadores), foram representados em cada modelo.

O modelo de diagnóstico da Falha crítica 1 em PN interpretada foi desenvolvido de acordo com o seguinte procedimento:

a) A partir da rede Bayesiana (BN) para a Falha 1 (Figura 5.7), obteve-se as seguintes relações causais de dependência:

$$\text{Falha 1} \dashrightarrow \text{PSHH-006A} \qquad (5.1)$$

$$\text{Falha 1} \dashrightarrow \text{PSHH-006B} \qquad (5.2)$$

$$\text{PSHH-006A} \dashrightarrow \text{PSHH-006C} \qquad (5.3)$$

$$\text{PSHH-006A} \dashrightarrow \text{PSHH-006B} \qquad (5.4)$$

$$\text{PSHH-006B} \dashrightarrow \text{PSHH-006C} \qquad (5.5)$$

b) A partir das relações causais de 5.1 a 5.5, obtiveram-se as relações lógicas entre as variáveis externas (sinais de sensores)

$$\text{Falha 1} \dashrightarrow (\text{PSHH-006A} \wedge \text{PSHH-006B}) \vee (\text{PSHH-006A} \wedge \text{PSHH-006C}) \qquad (5.6)$$

$$\text{Falha 1} \dashrightarrow (\text{PSHH-006B} \wedge \text{PSHH-006C}) \qquad (5.7)$$

De (5.6) e (5.7) obtêm-se:

$$\text{Falha 1} \dashrightarrow (\text{PSHH-006A} \wedge \text{PSHH-006B}) \vee (\text{PSHH-006A} \wedge \text{PSHH-006C}) \vee (\text{PSHH-006B} \wedge \text{PSHH-006C}) \qquad (5.8)$$

c) As relações lógicas foram representadas graficamente através de rede de Petri (PN), construindo-se uma estrutura efeito → causa.

A Figura 5.8 abaixo mostra a PN interpretada resultante.

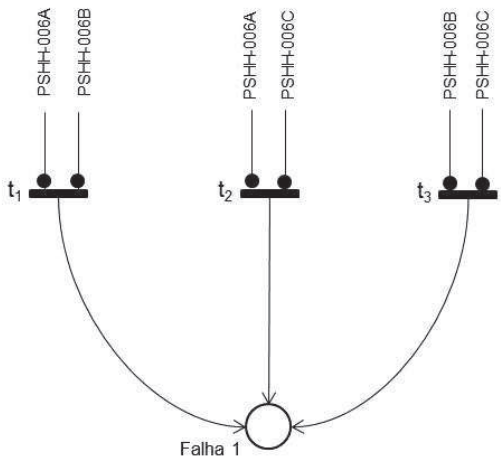


Figura 5.8 - Modelo em PN interpretada – estrutura efeito → causa.

d) Por fim, o modelo da Fig. 5.9 é construído incluindo a representação dos elementos adicionais necessários para reinicializar o modelo após não haver mais detecção de falhas e considera também a possibilidade da falha ser espúria, ou seja, a possibilidade de o diagnóstico não ser efetivado. Os lugares F_{AB}, F_{AC} e F_{BC} representam estados transitórios que podem corresponder às falhas espúrias. Se as transições t_4 ou t_5 ou t_6 são habilitadas para o disparo, significa que o sinal do(s) sensor(es) deixou(aram) de ser ativo(s) e portanto, o diagnóstico de falha deve ser abortado; voltando o sistema para o estado inicial (PRONTO_D1 com marca). Adicionalmente a Tabela 5.4 descreve as interpretações dadas aos elementos do modelo.

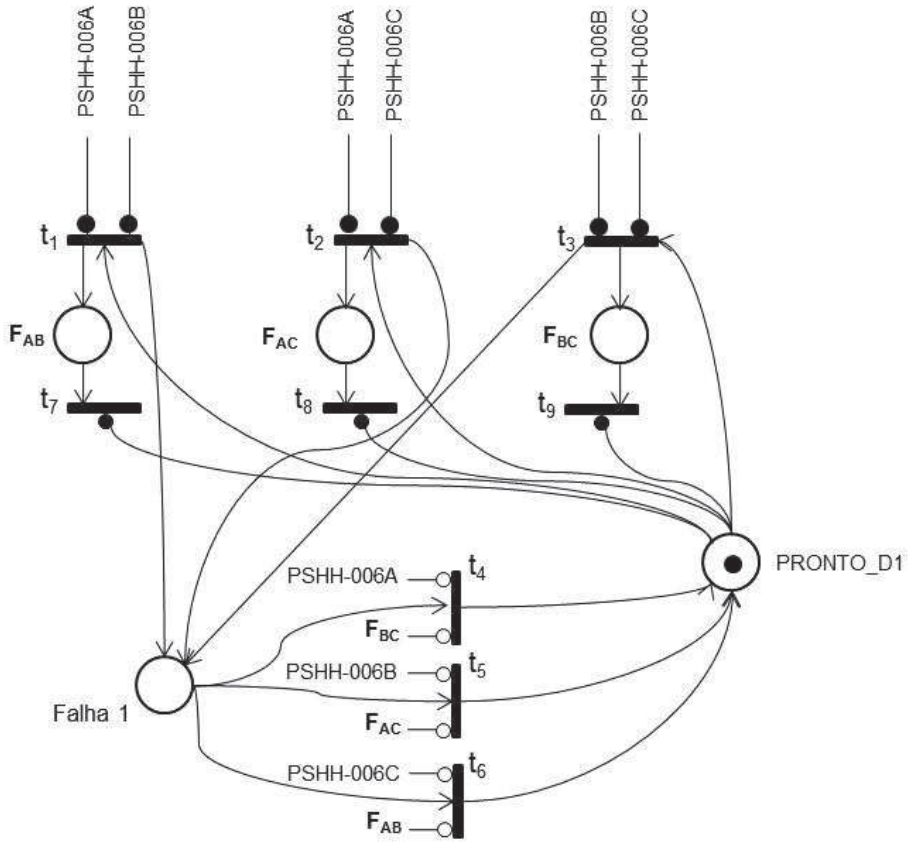


Figura 5.9 - Modelo em PN interpretada – diagnóstico da Falha crítica 1.

Tabela 5.4 – Elementos do modelo em PN interpretada para Falha 1.

ELEMENTO	DESCRIÇÃO
Arco habilitador associado "PSHH-006A"	Desvio de pressão muito alta na descarga da ECOMP, detectado a partir do sensor PIT-006A
Arco habilitador associado "PSHH-006B"	Desvio de pressão muito alta na descarga da ECOMP, detectado a partir do sensor PIT-006B
Arco habilitador associado "PSHH-006C"	Desvio de pressão muito alta na descarga da ECOMP, detectado a partir do sensor PIT-006C
Lugar "F_{AB}"	Memória auxiliar que sinaliza que a transição t1 foi disparada
Lugar "F_{AC}"	Memória auxiliar que sinaliza que a transição t2 foi disparada
Lugar "F_{BC}"	Memória auxiliar que sinaliza que a transição t3 foi disparada
Lugar "PRONTO_D1"	Modelo pronto para reinicializar em caso de desvio de pressão na descarga da ECOMP
Lugar "Falha 1"	Diagnóstico de Falha devido à Pressão muito alta na descarga da ECOMP.

Da mesma forma, os demais modelos para diagnóstico das "falhas críticas" em PN interpretada, são mostrados nas Figuras 5.10, 5.11 e 5.12. Adicionalmente, as

Tabelas 5.5 a 5.7 descrevem as interpretações dadas aos elementos dos modelos gerados.

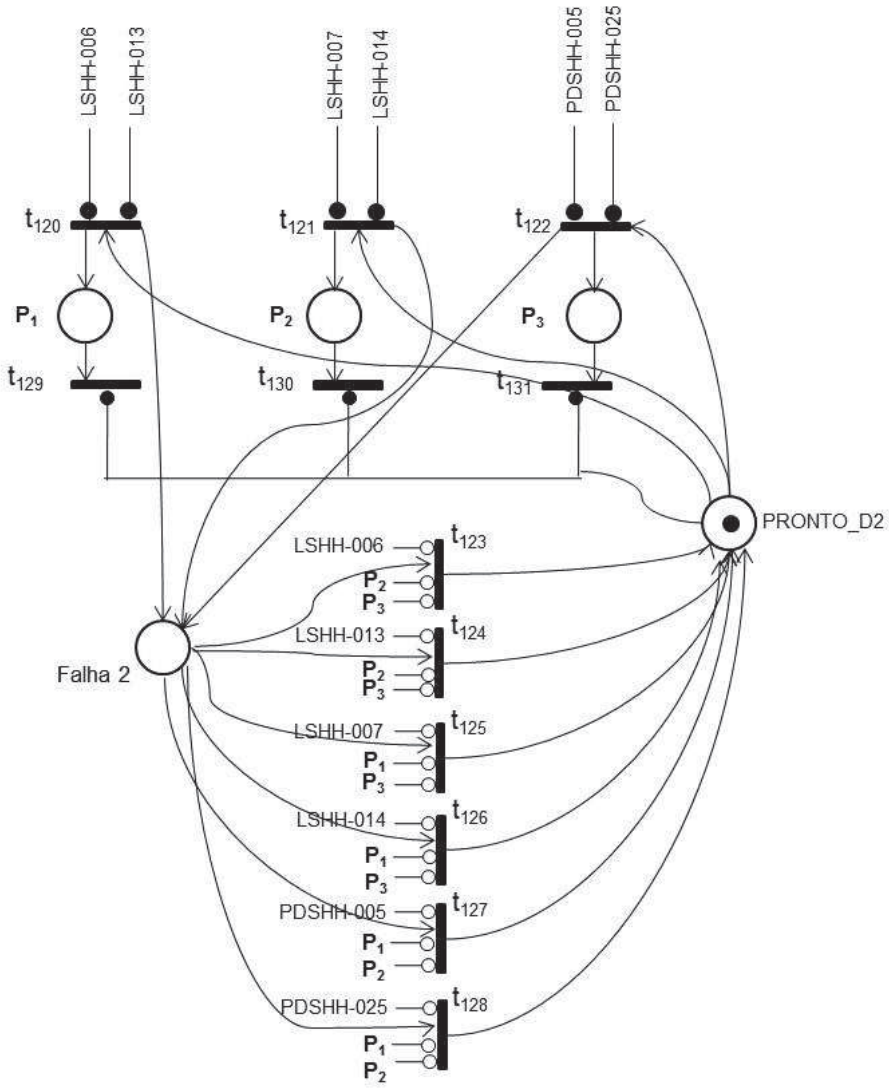


Figura 5.10 - Modelo em PN interpretada – diagnóstico da Falha crítica 2.

Tabela 5.5 – Elementos do modelo em PN interpretada para Falha 2.

ELEMENTO	DESCRIÇÃO
Arco habilitador associado "LSHH-006"	Desvio de nível de condensado muito alto no Filtro A na entrada da ECOMP, detectado a partir do sensor LIT-006
Arco habilitador associado "LSHH-013"	Desvio de nível de condensado muito alto no Filtro B na entrada da ECOMP, detectado a partir do sensor LIT-013
Arco habilitador associado "LSHH-007"	Desvio de nível de condensado muito alto no Filtro A na entrada da ECOMP, detectado a partir do sensor LIT-007
Arco habilitador associado "LSHH-014"	Desvio de nível de condensado muito alto no Filtro B na entrada da ECOMP, detectado a partir do sensor LIT-014

ELEMENTO	DESCRIÇÃO
Arco habilitador associado “PDSHH-005”	Desvio de pressão diferencial muito alta no Filtro A na entrada da ECOMP, detectado a partir do sensor PDIT-005
Arco habilitador associado “PDSHH-025”	Desvio de pressão diferencial muito alta no Filtro B na entrada da ECOMP, detectado a partir do sensor PDIT-025
Lugar “P1”	Memória auxiliar que sinaliza que a transição t121 foi disparada
Lugar “P2”	Memória auxiliar que sinaliza que a transição t122 foi disparada
Lugar “P3”	Memória auxiliar que sinaliza que a transição t123 foi disparada
Lugar “PRONTO_D2”	Modelo pronto para reinicializar em caso de desvio de pressão diferencial nos Filtros A ou B na entrada da ECOMP
Lugar “Falha 2”	Diagnóstico de Falha devido à Pressão diferencial muito alta nos Filtros A ou B na entrada da ECOMP.

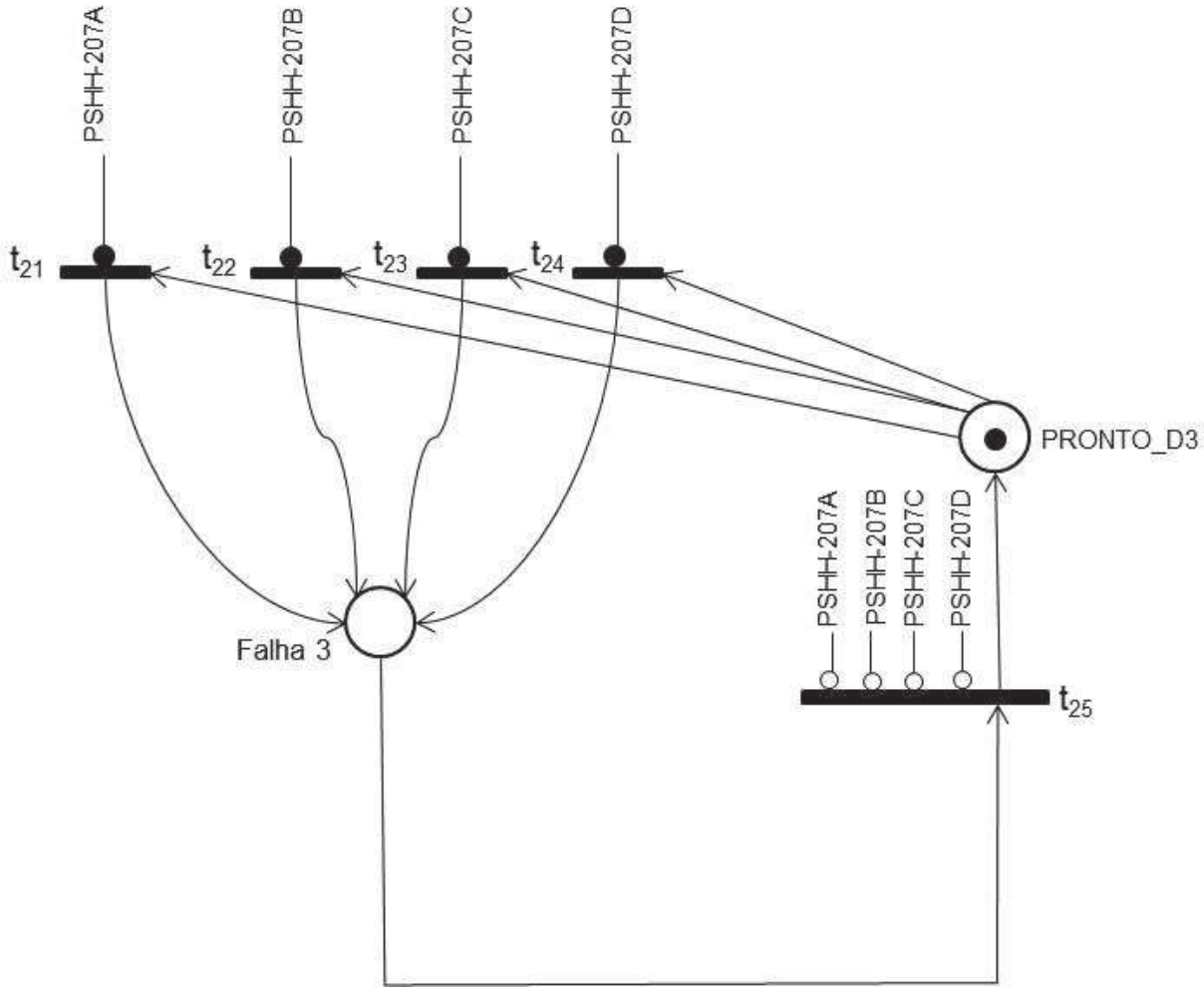


Figura 5.11 - Modelo em PN interpretada – diagnóstico da Falha crítica 3.

Tabela 5.6 – Elementos do modelo em PN interpretada para Falha 3.

ELEMENTO	DESCRIÇÃO
Arco habilitador associado "PSHH-207A"	Desvio de pressão muito alta na descarga do turbo compressor A, detectado a partir do sensor PIT-207A
Arco habilitador associado "PSHH-207B"	Desvio de pressão muito alta na descarga do turbo compressor B, detectado a partir do sensor PIT-207B
Arco habilitador associado "PSHH-207C"	Desvio de pressão muito alta na descarga do turbo compressor C, detectado a partir do sensor PIT-207C
Arco habilitador associado "PSHH-207D"	Desvio de pressão muito alta na descarga do turbo compressor D, detectado a partir do sensor PIT-207D
Lugar "PRONTO_D3"	Modelo pronto para reinicializar em caso de desvio de pressão muito alta na descarga dos turbos compressores A, B, C ou D
Lugar "Falha 3"	Diagnóstico de Falha devido à Pressão muito alta em um dos turbo compressores A, B, C ou D.

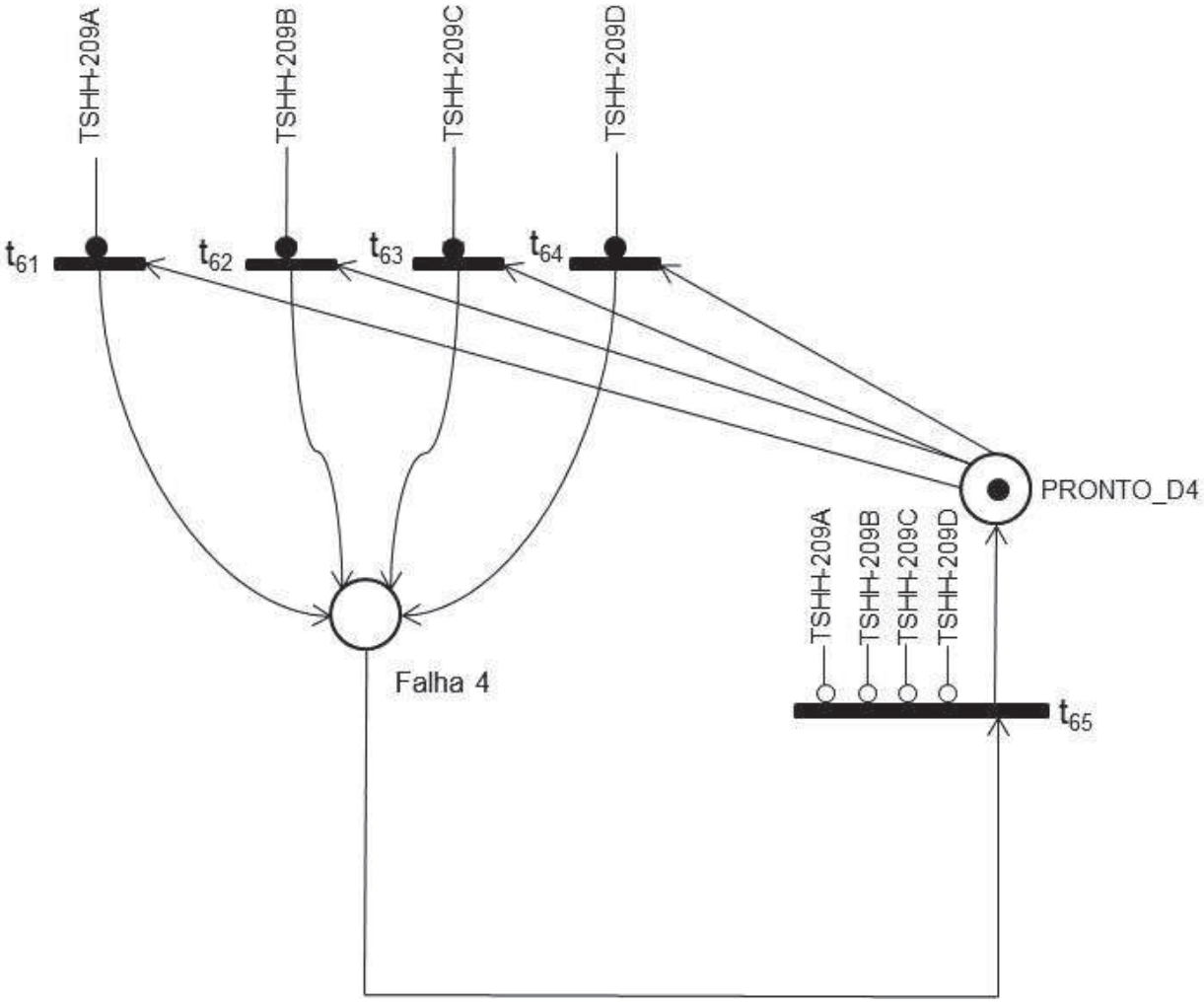


Figura 5.12 - Modelo em PN interpretada – diagnóstico da Falha crítica 4.

Tabela 5.7 – Elementos do modelo em PN interpretada para Falha 4.

ELEMENTO	DESCRIÇÃO
Arco habilitador associado "TSHH-209A"	Desvio de temperatura muito alta na descarga do turbo compressor A, detectado a partir do sensor TIT-209A
Arco habilitador associado "TSHH-209B"	Desvio de temperatura muito alta na descarga do turbo compressor B, detectado a partir do sensor TIT-209B
Arco habilitador associado "TSHH-209C"	Desvio de temperatura muito alta na descarga do turbo compressor C, detectado a partir do sensor TIT-209C
Arco habilitador associado "TSHH-209D"	Desvio de temperatura muito alta na descarga do turbo compressor D, detectado a partir do sensor TIT-209D
Lugar "PRONTO_D4"	Modelo pronto para reinicializar em caso de desvio de temperatura muito alta na descarga dos turbos compressores A, B, C ou D
Lugar "Falha 4"	Diagnóstico de Falha devido à temperatura muito alta em um dos turbo compressores A, B, C ou D.

Construídos os modelos de diagnóstico das falhas críticas em PN interpretada; procedeu-se a sua análise e validação de requisitos por meio de simulação com a ferramenta HPSim (ANSCHUETZ, 2010).

Para análise dos modelos de diagnósticos de falhas críticas, deve-se considerar o comportamento dos dispositivos de sensoriamento e dos dispositivos de atuação. As Figuras 5.13 a 5.16 mostram os modelos resultantes que foram assim construídos a fim de se fazer a simulação dos mesmos.

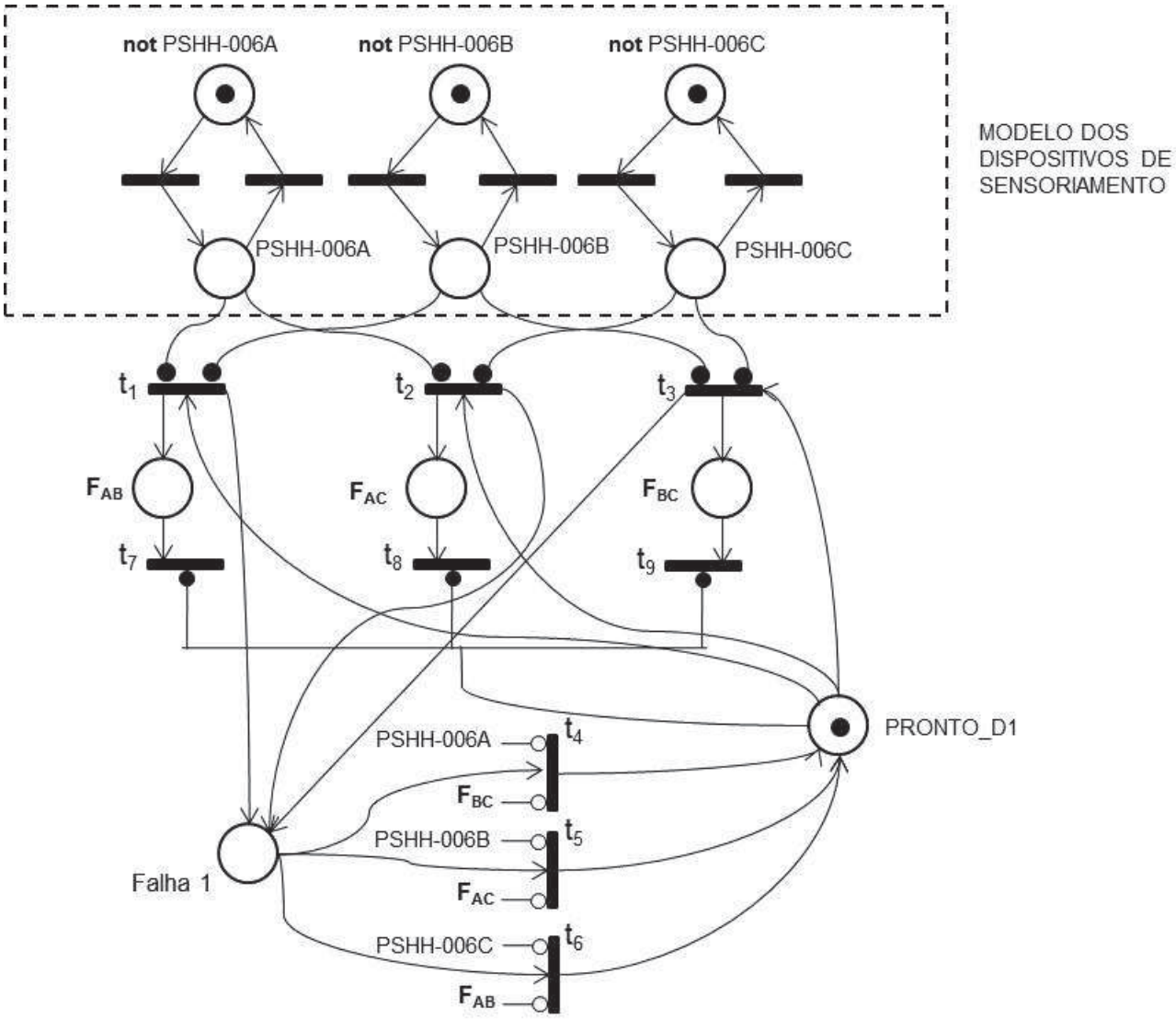


Figura 5.13 - Modelo em PN interpretada para simulação – diagnóstico da Falha crítica 1.

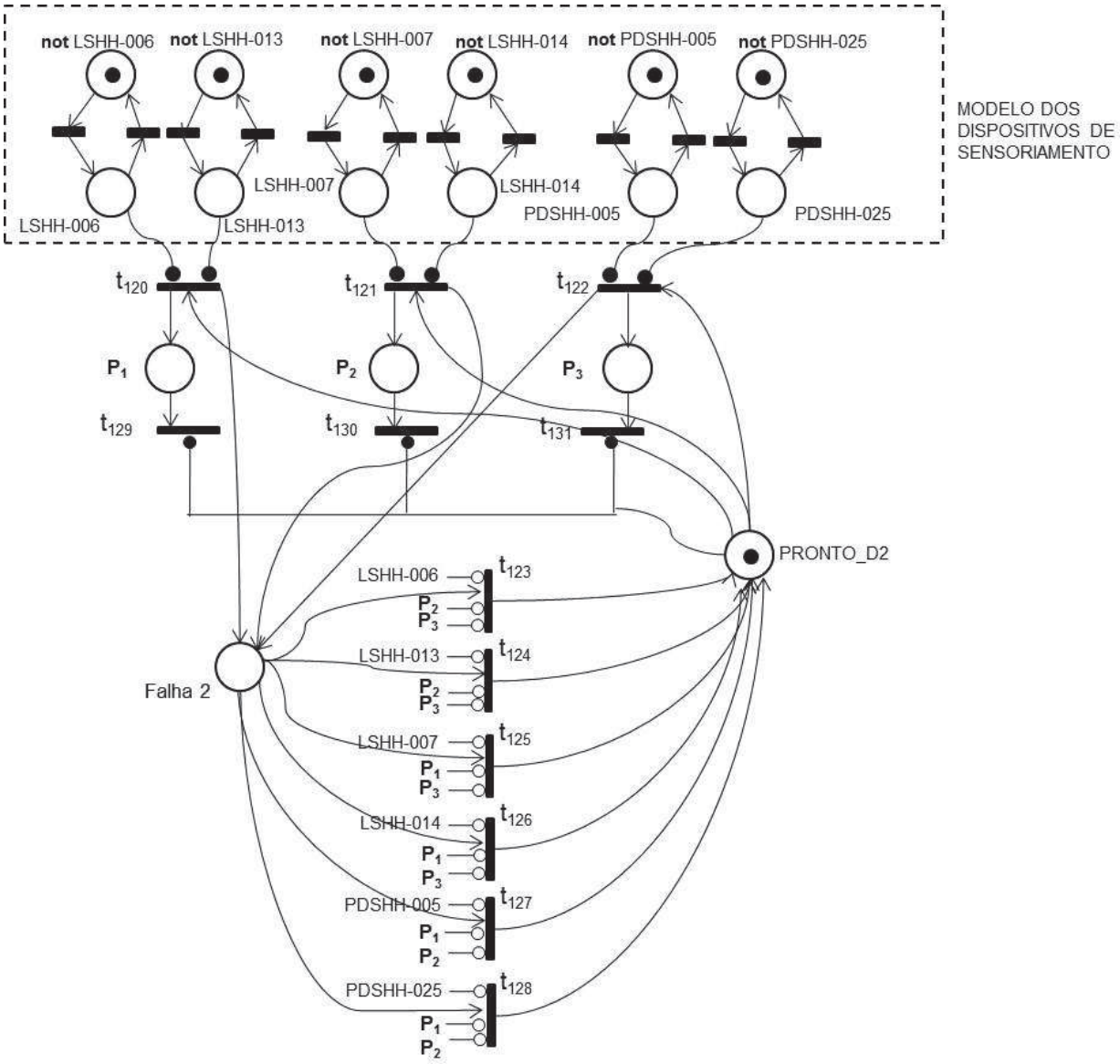


Figura 5.14 - Modelo em PN interpretada para simulação – diagnóstico da Falha crítica 2.

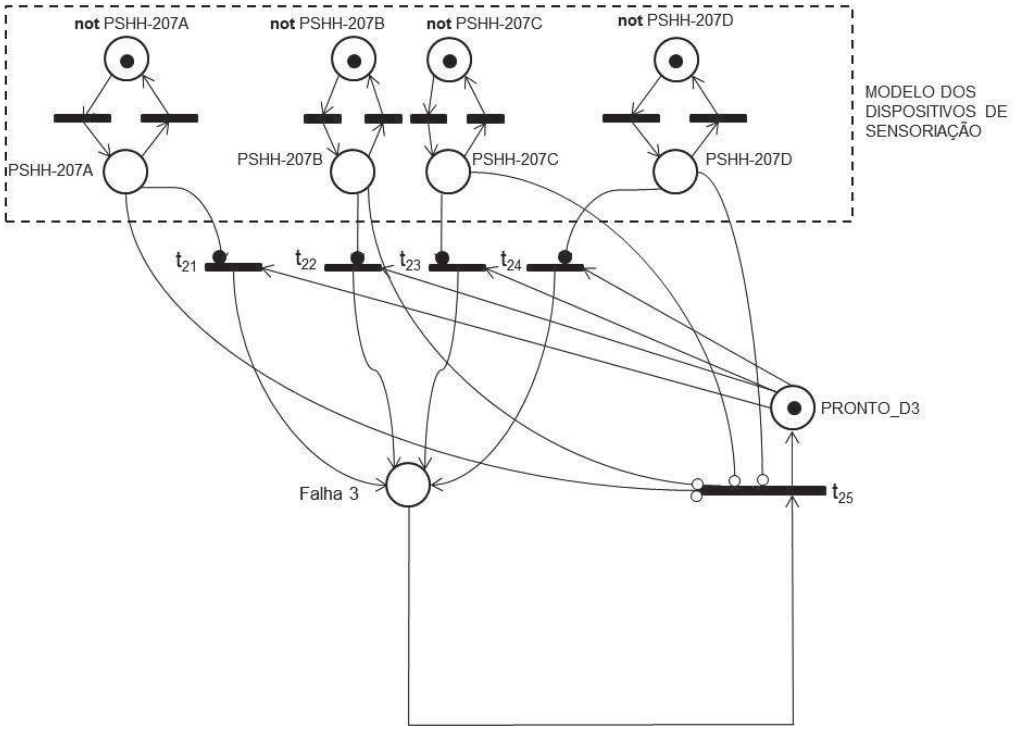


Figura 5.15 - Modelo em PN interpretada para simulação – diagnóstico da Falha crítica 3.

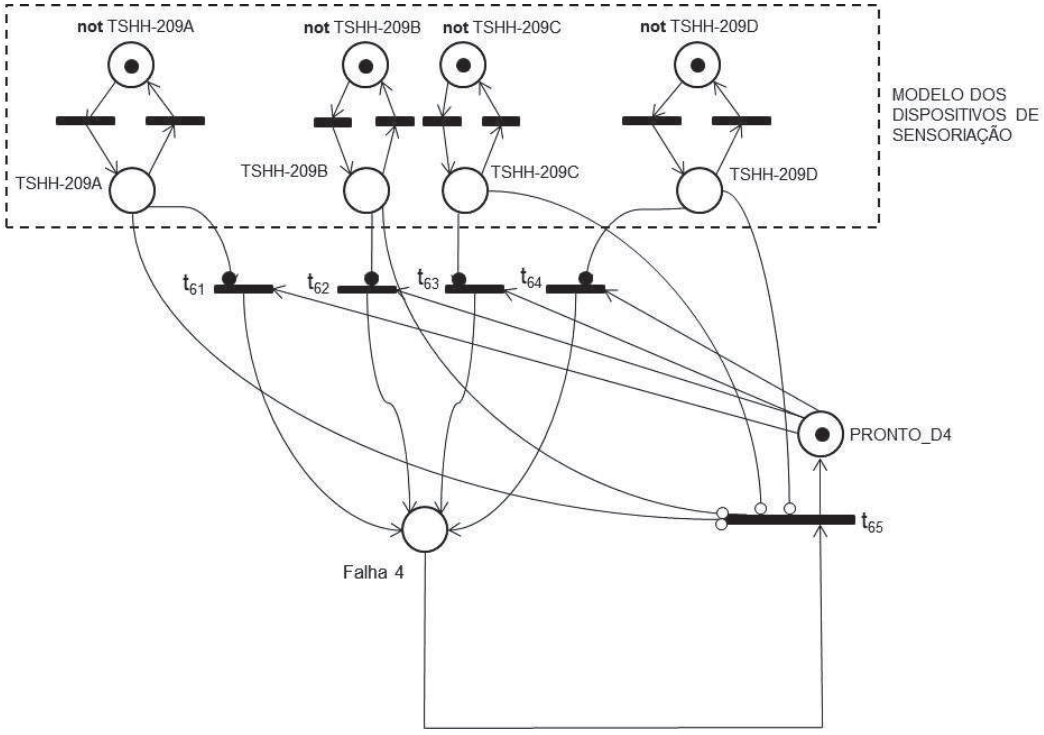


Figura 5.16 - Modelo em PN interpretada para simulação – diagnóstico da Falha crítica 4.

Finalmente, a fim de concluir a etapa A1, as “boas propriedades” foram analisadas para os modelos de diagnósticos de falhas críticas construídos. A

propriedade de reiniciabilidade foi analisada por meio de simulação dos modelos com o uso da ferramenta HPSim (ANSCHUETZ, 2010) e as propriedades de vivacidade e segurança foram analisadas com o uso da ferramenta PIPE2 (BONET et al., 2007). Um resumo da análise das “boas propriedades” para os modelos construídos é indicado na Tabela 5.8.

Tabela 5.8 – Resumo das “boas propriedades” das PN interpretadas.

Modelo em PN interpretada	Propriedade dinâmica	Resultado
Diagnóstico da falha crítica 1	Vivacidade	Verificado com sucesso
	Segurança	Verificado com sucesso
	Reiniciabilidade	Verificado com sucesso
Diagnóstico da falha crítica 2	Vivacidade	Verificado com sucesso
	Segurança	Verificado com sucesso
	Reiniciabilidade	Verificado com sucesso
Diagnóstico da falha crítica 3	Vivacidade	Verificado com sucesso
	Segurança	Verificado com sucesso
	Reiniciabilidade	Verificado com sucesso
Diagnóstico da falha crítica 4	Vivacidade	Verificado com sucesso
	Segurança	Verificado com sucesso
	Reiniciabilidade	Verificado com sucesso

5.3.2 Etapa A2: Modelagem de tratamento e coordenação de falhas críticas

5.3.2.1 Passo 1: Identificação das SIFs

O passo 1 foi executado, construindo-se uma Tabela que mostra a identificação das SIFs, as “falhas críticas” associadas a cada SIF, os níveis de segurança SIL definidos para cada SIF, os eventos inicializadores e por fim as ações a serem executadas pelo SIS; com base no relatório gerado a partir de um estudo de análise de riscos (HAZOP) no processo. Este estudo de caso considerou apenas quatro SIFs, embora o relatório de análise de riscos completo para a ECOMP, seja constituído por oito SIFs. A Tabela 5.9 mostra a identificação das SIFs baseadas neste relatório. A partir desta Tabela, identificaram-se informações importantes para a construção dos modelos de tratamento:

- as “falhas críticas” que estão associadas a cada SIF;

- as ações a serem executadas pelo SIS e que caberia a cada SIF para o tratamento das correspondentes falhas críticas.

5.3.2.2 Passo 2: Construção do modelo de tratamento para cada SIF em PN interpretada

O passo 2 foi executado conforme o procedimento proposto:

A. Construção dos modelos de tratamento em rede de Petri interpretada para cada "falha crítica". As regras para tratamento foram obtidas da Tabela 5.9 construída no passo 1.
B. Edição e simulação do modelo de tratamento em ferramenta computacional HPSim, com o propósito de validação e análise da propriedade de reiniciabilidade. Para a simulação do modelo de tratamento, foram integrados os modelos dos dispositivos de sensoriamento e dos dispositivos de atuação.
C. Edição do modelo de tratamento em ferramenta computacional PIPE2, a fim de analisar as propriedades de vivacidade e segurança (1-limitada).

Desta forma, os modelos para tratamento das "falhas críticas" em PN interpretada, são mostrados nas Figuras 5.17, 5.18, 5.19 e 5.20. Adicionalmente, as Tabelas 5.10 a 5.13 descrevem as interpretações dadas aos elementos dos modelos gerados.

Tabela 5.9 – Identificação das SIFs.

SIF-ID	Descrição	Consequências de falha na demanda	SIL	Eventos inicializadores	Ação
1	Pressão muito alta na descarga da ECOMP (**Falha 1**)	• Possíveis danos na linha de descarga; • Vazamento incontrolado de gás podendo ocasionar explosão; • Vibração excessiva e ruído alto.	3	• PIT-006A • PIT-006B • PIT-006C votação 2oo3	• Fechar válvulas: XV-001 / XV-017; XV-019 / XV-020; XV-003 / XV-018. • Parada de emergência dos turbos compressores TC-12001A/B/C/D.
2	Nível de condensado muito alto nos Filtros A e B na entrada da ECOMP (**Falha 2**)	• Arraste de condensado para os turbos compressores A, B, C e D com possibilidade de dano aos mesmos.	1	• LIT-006 • LIT-007 • LIT-013 • LIT-014 • PDSHH-005 • PDSHH-025	• Fechar válvulas: XV-001 / XV-017; XV-019 / XV-020; XV-003 / XV-018. XV-005 / XV-022 • Parada de emergência dos turbos compressores TC-12001A/B/C/D.
3	Pressão muito alta na descarga dos turbos compressores A, B, C e D (**Falha 3**)	• Possíveis danos na linha de descarga; • Possível fluxo reverso; • Danificação dos turbos compressores.	1	• PIT-207A • PIT-207B • PIT207C • PIT207D	Parada de emergência dos turbos compressores: TC-12001A/B/C/D.
4	Temperatura muito alta na descarga dos turbos compressores A, B, C e D (**Falha 4**)	• Possíveis danos na linha de descarga.	1	• TIT-209A • TIT-209B • TIT-209C • TIT-209D	Parada de emergência dos turbos compressores: TC-12001A/B/C/D.

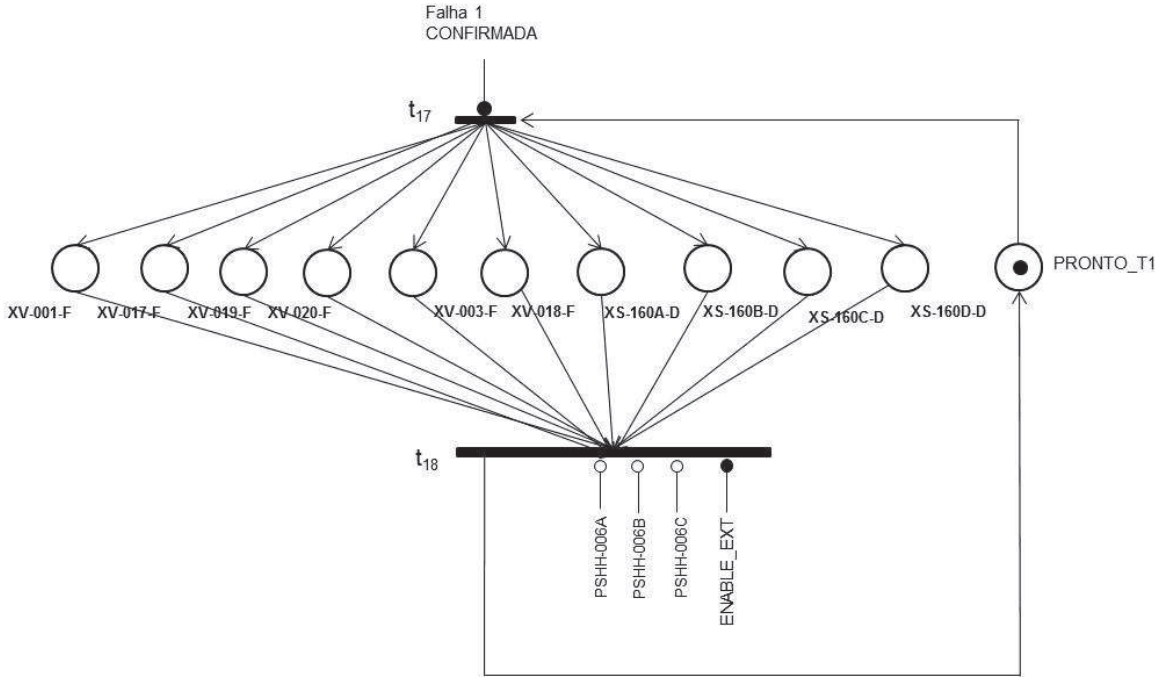


Figura 5.17 - Modelo em PN interpretada – tratamento da Falha crítica 1.

Tabela 5.10 - Elementos do modelo em PN interpretada da Figura 5.19.

ELEMENTO	DESCRIÇÃO
Arco habilitador associado "Falha 1 – Confirmada"	Confirmação do diagnóstico de falha crítica 1, proveniente do modelo de coordenação da falha crítica 1
Lugar "XV-001-F"	Comando "Fecha" no atuador da válvula XV-001 na linha de sucção 1 da ECOMP
Lugar "XV-017-F"	Comando "Fecha" no atuador da válvula XV-017 no "by-pass" da linha de sucção 1 da ECOMP
Lugar "XV-019-F"	Comando "Fecha" no atuador da válvula XV-019 na linha de sucção 2 da ECOMP
Lugar "XV-020-F"	Comando "Fecha" no atuador da válvula XV-020 no "by-pass" da linha de sucção 2 da ECOMP
Lugar "XV-003-F"	Comando "Fecha" no atuador da válvula XV-003 na linha de descarga da ECOMP
Lugar "XV-018-F"	Comando "Fecha" no atuador da válvula XV-018 no "by-pass" da linha de descarga da ECOMP
Lugar "XS-160A-D"	Comando de "Parada de Emergência" do turbo compressor A
Lugar "XS-160B-D"	Comando de "Parada de Emergência" do turbo compressor B
Lugar "XS-160C-D"	Comando de "Parada de Emergência" do turbo compressor C
Lugar "XS-160D-D"	Comando de "Parada de Emergência" do turbo compressor D

ELEMENTO	DESCRIÇÃO
Arco habilitador associado “ENABLE_EXT”	Sinal de controle externo utilizado para reiniciar o modelo de tratamento.
Lugar “PRONTO_T1”	Modelo pronto para reinicializar em caso de nova confirmação de diagnóstico de falha crítica 1

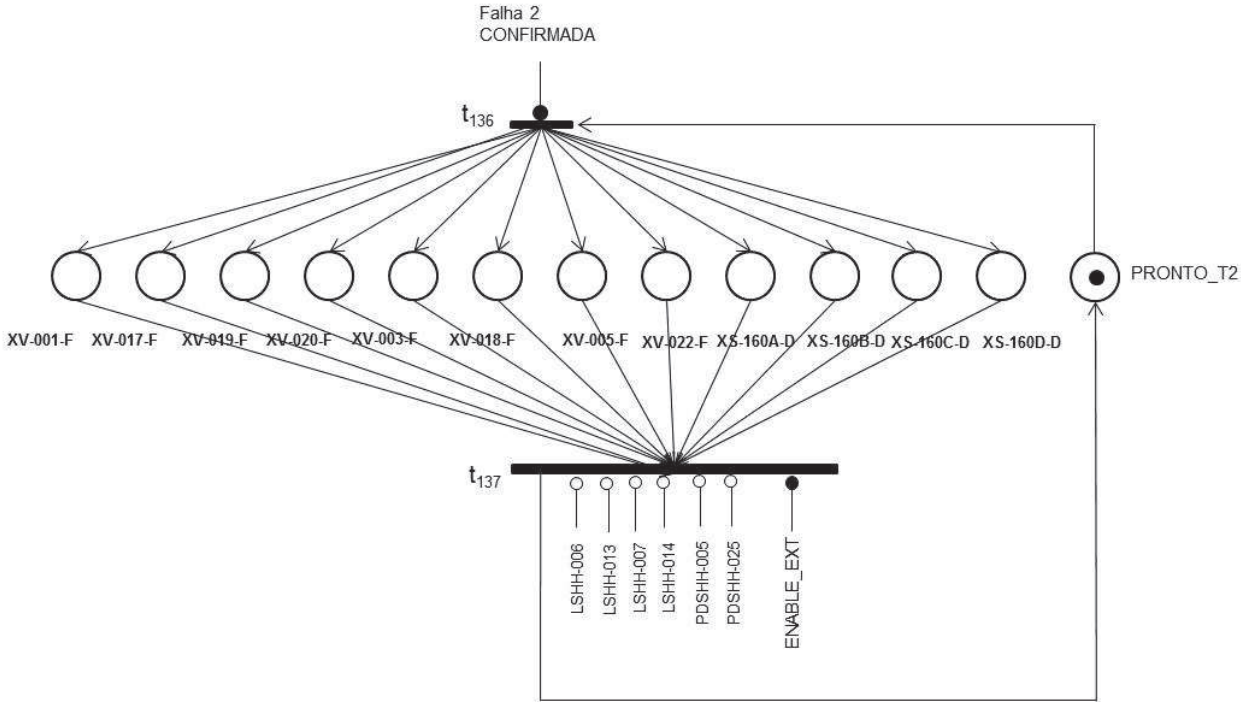


Figura 5.18 - Modelo em PN interpretada – tratamento da Falha crítica 2.

Tabela 5.11 - Elementos do modelo em PN interpretada da Figura 5.20.

ELEMENTO	DESCRIÇÃO
Arco habilitador associado “Falha 2 – Confirmada”	Confirmação do diagnóstico de falha crítica 2, proveniente do modelo de coordenação da falha crítica 2
Lugar “XV-001-F”	Comando “Fecha” no atuador da válvula XV-001 na linha de sucção 1 da ECOMP
Lugar “XV-017-F”	Comando “Fecha” no atuador da válvula XV-017 no “by-pass” da linha de sucção 1 da ECOMP
Lugar “XV-019-F”	Comando “Fecha” no atuador da válvula XV-019 na linha de sucção 2 da ECOMP
Lugar “XV-020-F”	Comando “Fecha” no atuador da válvula XV-020 no “by-pass” da linha de sucção 2 da ECOMP
Lugar “XV-003-F”	Comando “Fecha” no atuador da válvula XV-003 na linha de descarga da ECOMP
Lugar “XV-018-F”	Comando “Fecha” no atuador da válvula XV-018 no “by-pass” da linha de descarga da ECOMP

ELEMENTO	DESCRIÇÃO
Lugar “XV-005-F”	Comando “Fecha” no atuador da válvula XV-005 na saída do filtro A
Lugar “XV-022-F”	Comando “Fecha” no atuador da válvula XV-022 na saída do filtro B
Lugar “XS-160A-D”	Comando de “Parada de Emergência” do turbo compressor A
Lugar “XS-160B-D”	Comando de “Parada de Emergência” do turbo compressor B
Lugar “XS-160C-D”	Comando de “Parada de Emergência” do turbo compressor C
Lugar “XS-160D-D”	Comando de “Parada de Emergência” do turbo compressor D
Arco habilitador associado “ENABLE_EXT”	Sinal de controle externo utilizado para reiniciar o modelo de tratamento.
Lugar “PRONTO_T2”	Modelo pronto para reinicializar em caso de nova confirmação de diagnóstico de falha crítica 2

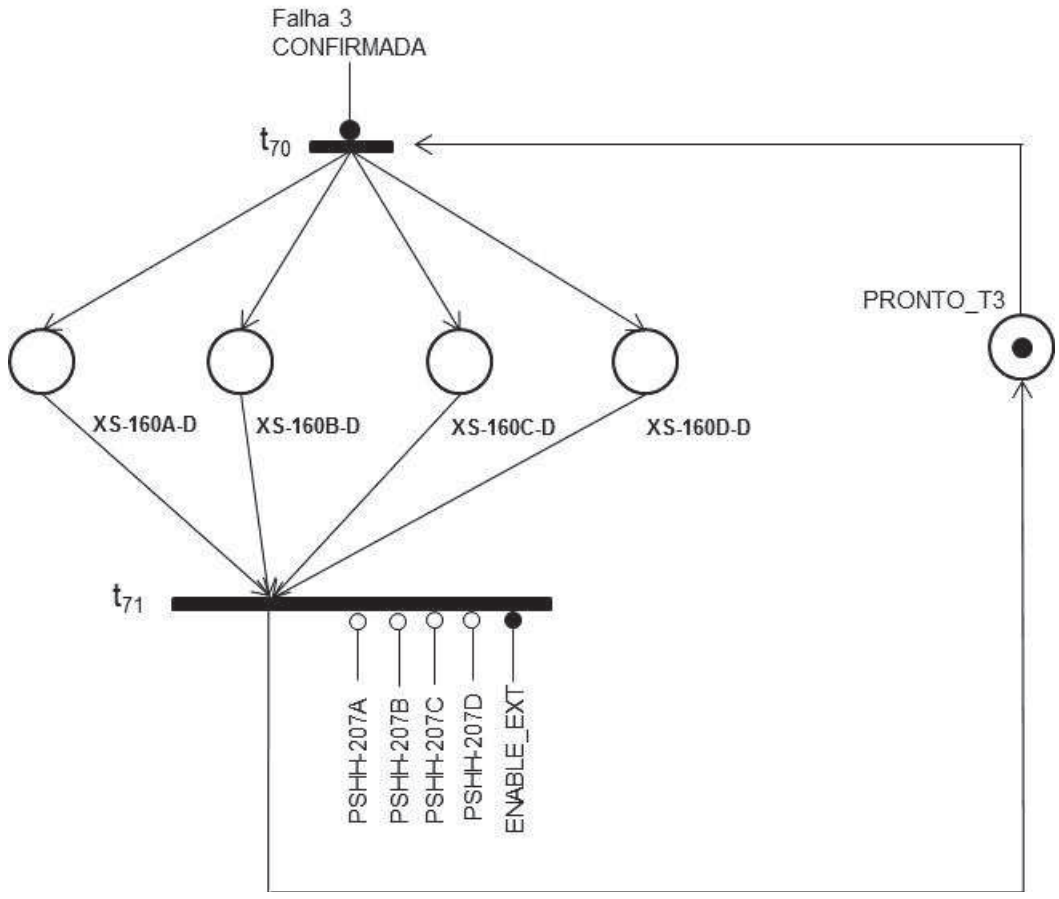


Figura 5.19 - Modelo em PN interpretada – tratamento da Falha crítica 3.

Tabela 5.12 - Elementos do modelo em PN interpretada da Figura 5.21.

ELEMENTO	DESCRIÇÃO
Arco habilitador associado "Falha 3 – Confirmada"	Confirmação do diagnóstico de falha crítica 3, proveniente do modelo de coordenação da falha crítica 3
Lugar "XS-160A-D"	Comando de "Parada de Emergência" do turbo compressor A
Lugar "XS-160B-D"	Comando de "Parada de Emergência" do turbo compressor B
Lugar "XS-160C-D"	Comando de "Parada de Emergência" do turbo compressor C
Lugar "XS-160D-D"	Comando de "Parada de Emergência" do turbo compressor D
Arco habilitador associado "ENABLE_EXT"	Sinal de controle externo utilizado para reiniciar o modelo de tratamento.
Lugar "PRONTO_T3"	Modelo pronto para reinicializar em caso de nova confirmação de diagnóstico de falha crítica 3

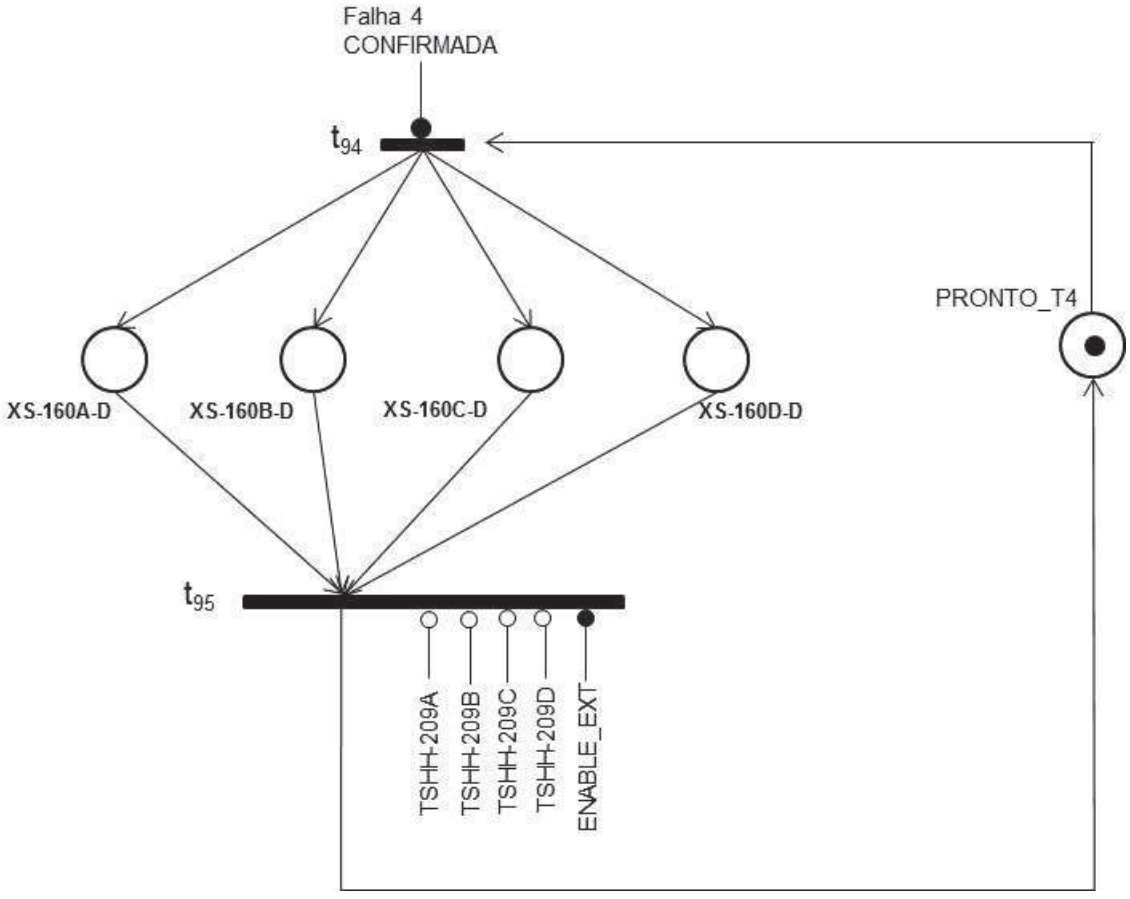


Figura 5.20 - Modelo em PN interpretada – tratamento da Falha crítica 4.

Tabela 5.13 - Elementos do modelo em PN interpretada da Figura 5.22.

ELEMENTO	DESCRIÇÃO
Arco habilitador associado "Falha 4 – Confirmada"	Confirmação do diagnóstico de falha crítica 4, proveniente do modelo de coordenação da falha crítica 4
Lugar "XS-160A-D"	Comando de "Parada de Emergência" do turbo compressor A
Lugar "XS-160B-D"	Comando de "Parada de Emergência" do turbo compressor B
Lugar "XS-160C-D"	Comando de "Parada de Emergência" do turbo compressor C
Lugar "XS-160D-D"	Comando de "Parada de Emergência" do turbo compressor D
Arco habilitador associado "ENABLE_EXT"	Sinal de controle externo utilizado para reiniciar o modelo de tratamento.
Lugar "PRONTO_T3"	Modelo pronto para reinicializar em caso de nova confirmação de diagnóstico de falha crítica 4

Construídos os modelos de tratamento das falhas críticas em PN interpretada; procedeu-se sua análise e validação de requisitos através de simulação com o uso da ferramenta computacional HPSim (ANSCHUETZ, 2010).

Os modelos de tratamento de falhas críticas construídos para simulação contêm os modelos dos dispositivos de sensoriamento e modelos dos dispositivos de atuação. As Figuras 5.21 a 5.24 mostram os modelos resultantes a fim de se fazer a simulação dos mesmos.

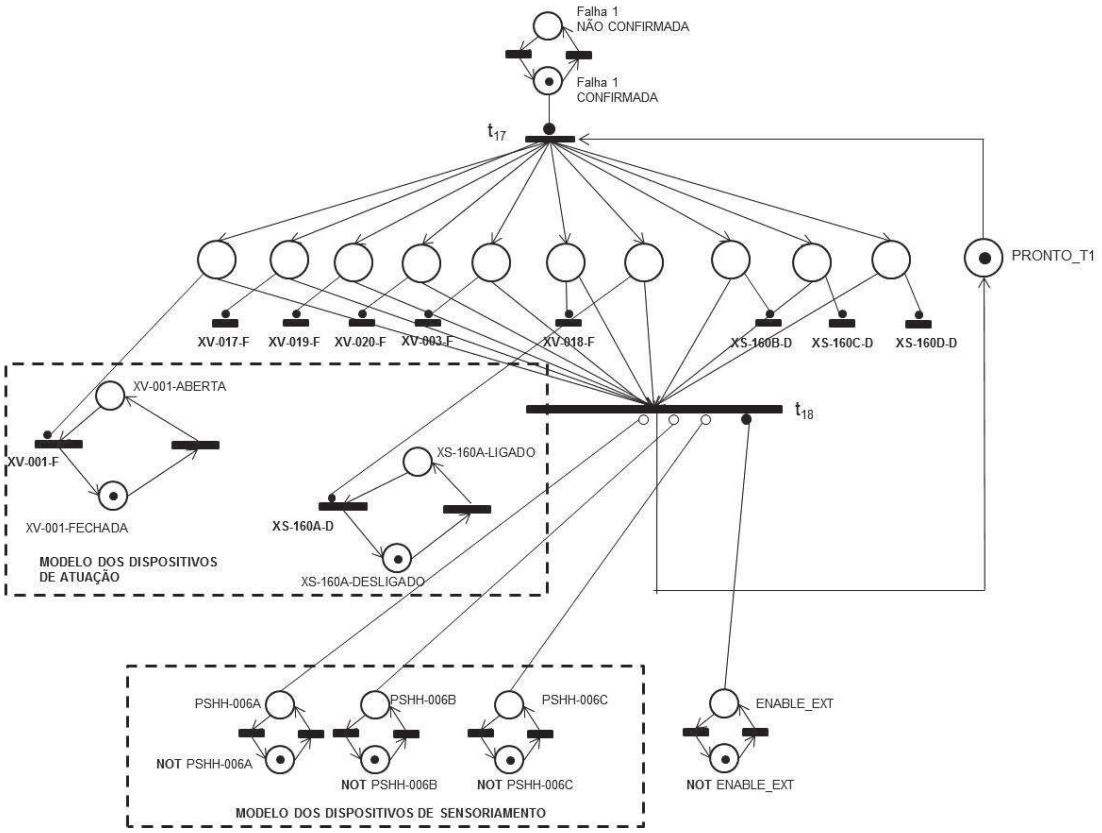


Figura 5.21 - Modelo em PN interpretada para simulação – tratamento da Falha crítica 1.

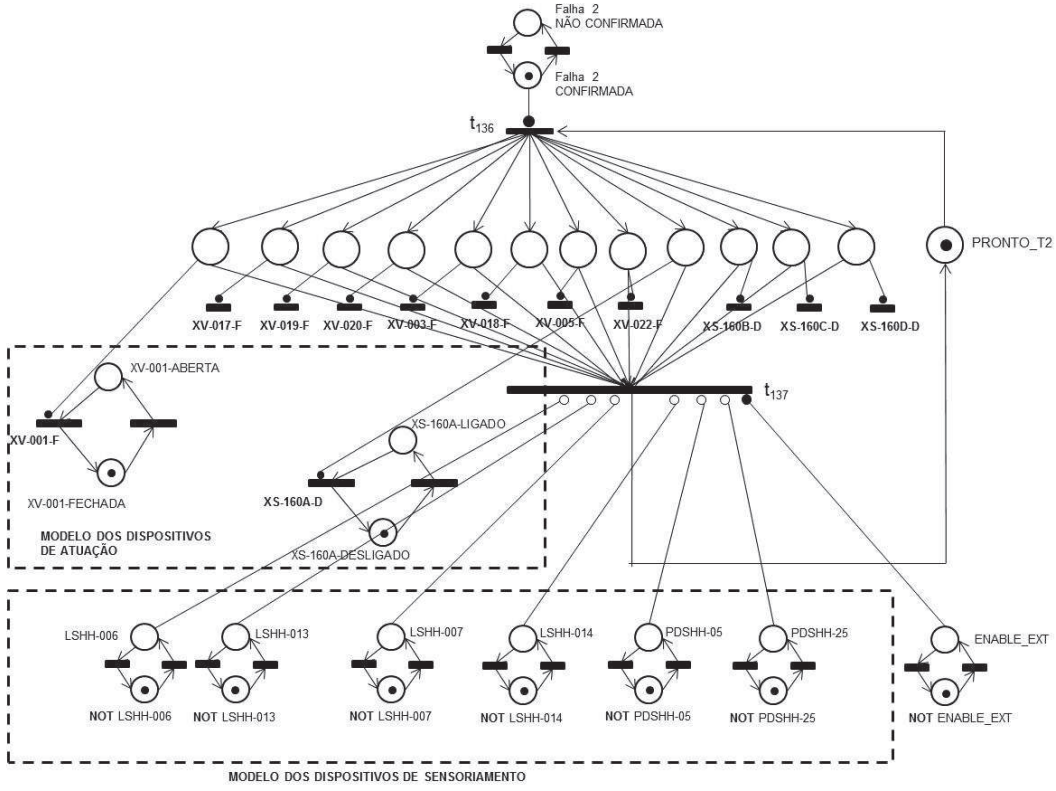


Figura 5.22 - Modelo em PN interpretada para simulação – tratamento da Falha crítica 2.

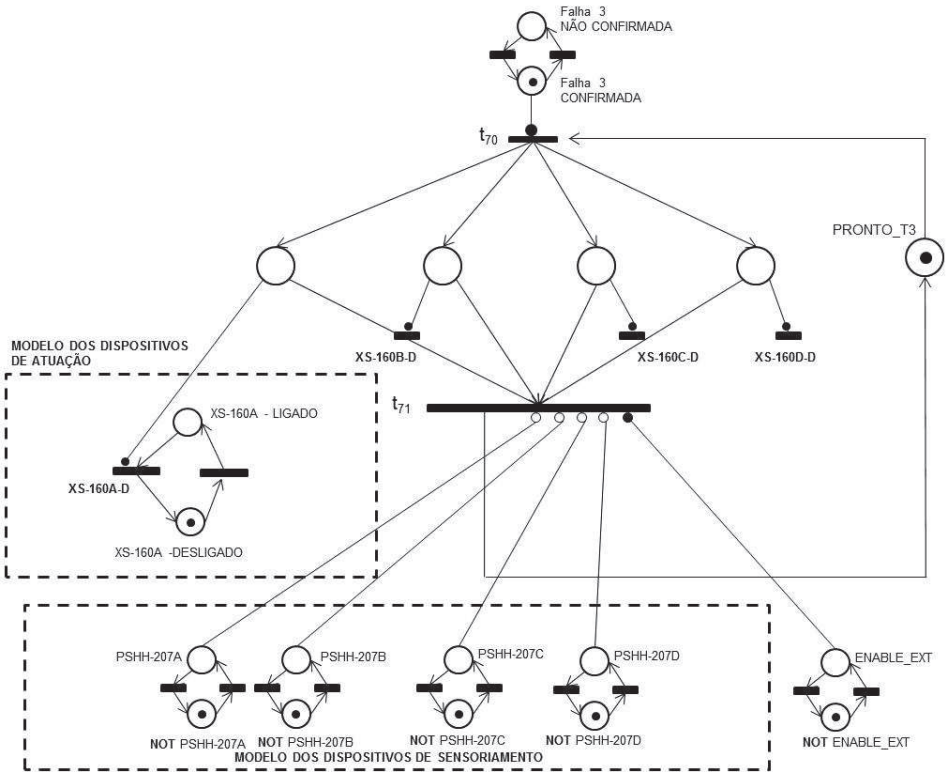


Figura 5.23 - Modelo em PN interpretada para simulação – tratamento da Falha crítica 3.

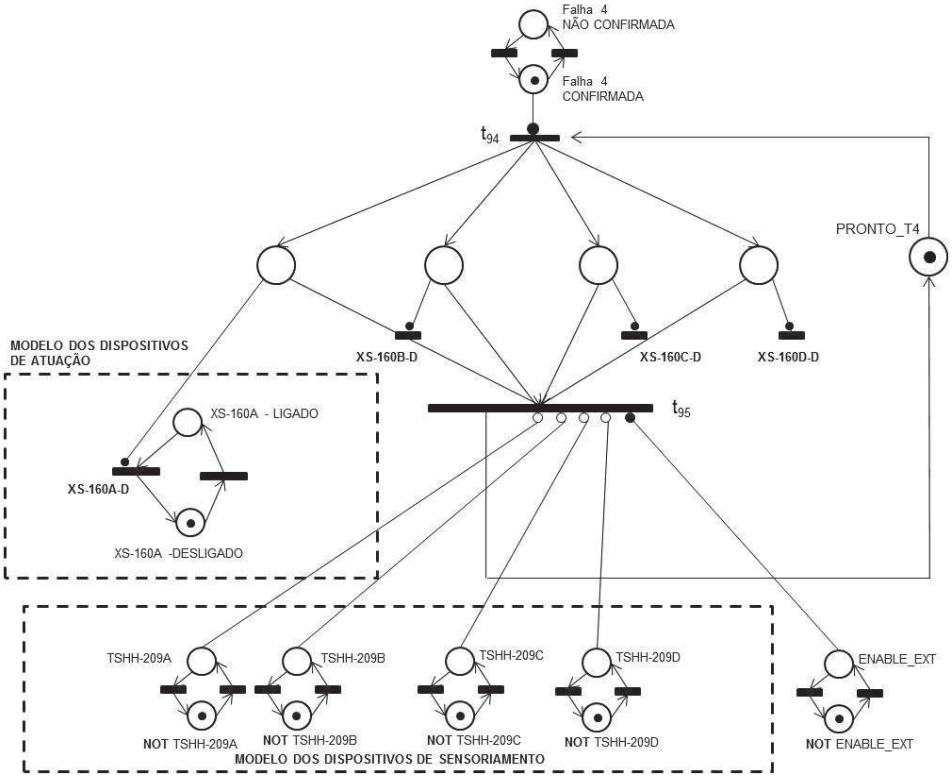


Figura 5.24 - Modelo em PN interpretada para simulação – tratamento da Falha crítica 4.

A fim de concluir este passo, as “boas propriedades” foram analisadas para os modelos de tratamento de falhas críticas construídos. A propriedade de reiniciabilidade foi analisada por meio da simulação dos modelos com o uso da ferramenta HPSim (ANSCHUETZ, 2010) e as propriedades de vivacidade e segurança foram analisadas com o uso da ferramenta PIPE2 (BONET et al., 2007). Um resumo da análise das “boas propriedades” para os modelos construídos é indicado na Tabela 5.14.

Tabela 5.14 – Resumo das “boas propriedades” das PN interpretadas.

Modelo em PN interpretada	**Propriedade comportamental**	**Resultado**
Tratamento da falha crítica 1	Vivacidade	Verificado com sucesso
	Segurança	Verificado com sucesso
	Reiniciabilidade	Verificado com sucesso
Tratamento da falha crítica 2	Vivacidade	Verificado com sucesso
	Segurança	Verificado com sucesso
	Reiniciabilidade	Verificado com sucesso
Tratamento da falha crítica 2	Vivacidade	Verificado com sucesso
	Segurança	Verificado com sucesso
	Reiniciabilidade	Verificado com sucesso
Tratamento da falha crítica 4	Vivacidade	Verificado com sucesso
	Segurança	Verificado com sucesso
	Reiniciabilidade	Verificado com sucesso

5.3.2.3 Passo 3: Construção do modelo de coordenação em PN interpretada para cada SIF.

O passo 3 foi executado de acordo com o procedimento proposto:

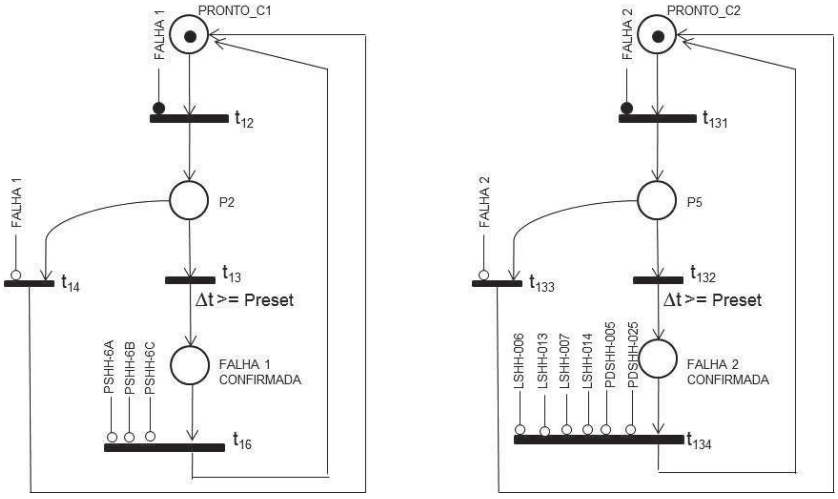
A. Construção dos modelos de coordenação em rede de Petri interpretada para cada “falha crítica”. Os modelos foram construídos de forma robusta com relação à ocorrência de falhas espúrias. Neste trabalho a solução empregada para a implementação desta robustez foi via transições temporizadas.

B. Edição e simulação de cada modelo de coordenação, usando a ferramenta computacional HPSim, a fim de validar se o modelo atende aos requisitos

técnicos especificados e adicionalmente foi feita a análise da propriedade de reiniciabilidade.

C. Edição de cada modelo de coordenação usando a ferramenta computacional PIPE2, a fim de analisar as propriedades de vivacidade e segurança (1-limitada).

Desta forma, os modelos para coordenação das "falhas críticas" em PN interpretada, são mostrados nas Figuras 5.25 e 5.26. Adicionalmente, as Tabelas 5.15 a 5.18, respectivamente descrevem as interpretações dadas aos elementos dos modelos gerados.



(a) (b)

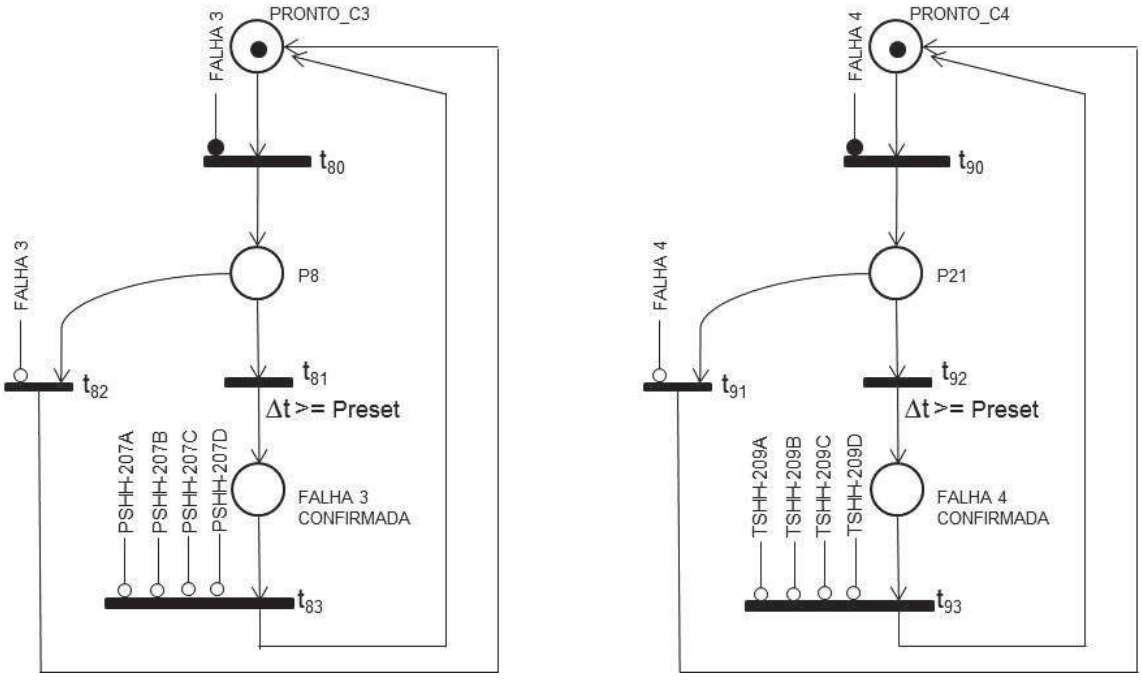
Figura 5.25 - Modelos em PN interpretada: Coordenação das (a) Falha crítica 1 e (b) Falha crítica 2.

Tabela 5.15 - Elementos do modelo em PN interpretada da Figura 5.25(a).

ELEMENTO	DESCRIÇÃO
Arcos habilitador / inibidor associado "FALHA 1"	Sinal de "FALHA" proveniente do modelo de diagnóstico da falha crítica 1.
Arco inibidor associado "PSHH-006A"	Desvio de pressão muito alta na descarga da ECOMP, detectado a partir do sensor PIT-006A
Arco inibidor associado "PSHH-006B"	Desvio de pressão muito alta na descarga da ECOMP, detectado a partir do sensor PIT-006B
Arco inibidor associado "PSHH-006C"	Desvio de pressão muito alta na descarga da ECOMP, detectado a partir do sensor PIT-006C
Lugar "PRONTO_C1"	Modelo de coordenação da falha crítica 1 pronto para ser reiniciado
Lugar "FALHA 1 CONFIRMADA"	Caso a "FALHA 1" permaneça ativada por um intervalo de tempo Δt >= PRESET, a mesma é confirmada e habilita a chamada do modelo de tratamento correspondente.

Tabela 5.16 - Elementos do modelo em PN interpretada da Figura 5.25(b).

ELEMENTO	DESCRIÇÃO
Arcos habilitador/inibidor associado "FALHA 2"	Sinal de "FALHA" proveniente do modelo de diagnóstico da falha crítica 2.
Arco inibidor associado "LSHH-006"	Desvio de nível de condensado muito alto no Filtro A na entrada da ECOMP, detectado a partir do sensor LIT-006
Arco inibidor associado "LSHH-013"	Desvio de nível de condensado muito alto no Filtro B na entrada da ECOMP, detectado a partir do sensor LIT-013
Arco inibidor associado "LSHH-007"	Desvio de nível de condensado muito alto no Filtro A na entrada da ECOMP, detectado a partir do sensor LIT-007
Arco inibidor associado "LSHH-014"	Desvio de nível de condensado muito alto no Filtro B na entrada da ECOMP, detectado a partir do sensor LIT-014
Arco inibidor associado "PDSHH-005"	Desvio de pressão diferencial muito alta no Filtro A na entrada da ECOMP, detectado a partir do sensor PDIT-005
Arco inibidor associado "PDSHH-025"	Desvio de pressão diferencial muito alta no Filtro B na entrada da ECOMP, detectado a partir do sensor PDIT-025
Lugar "PRONTO_C2"	Modelo de coordenação da falha crítica 2 pronto para ser reiniciado
Lugar "FALHA 2 CONFIRMADA"	Caso a "FALHA 1" permaneça ativada por um intervalo de tempo $\Delta t >= PRESET$, a mesma é confirmada e habilita a chamada do modelo de tratamento correspondente.



(a) (b)

Figura 5.26 - Modelos em PN interpretada: Coordenação das (a) Falha crítica 3 e (b) Falha crítica 4.

Tabela 5.17 - Elementos do modelo em PN interpretada da Figura 5.26(a).

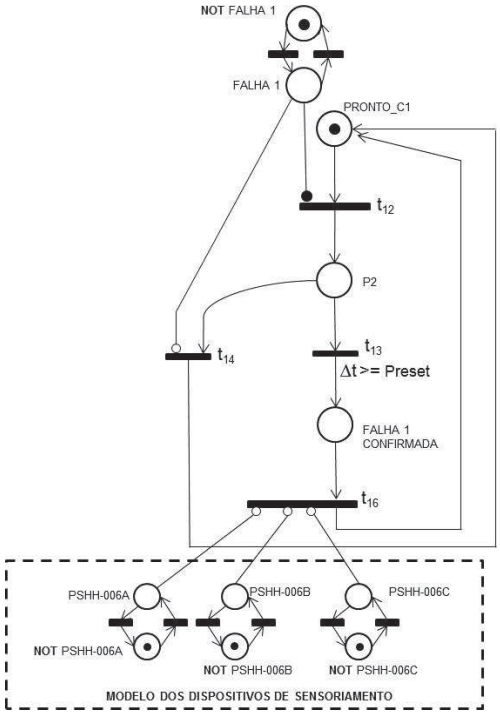
ELEMENTO	DESCRIÇÃO
Arcos habilitador/inibidor associado "FALHA 3"	Sinal de "FALHA" proveniente do modelo de diagnóstico da falha crítica 3.
Arco inibidor associado "PSHH-207A"	Desvio de pressão muito alta na descarga do turbo compressor A, detectado a partir do sensor PIT-207A
Arco inibidor associado "PSHH-207B"	Desvio de pressão muito alta na descarga do turbo compressor B, detectado a partir do sensor PIT-207B
Arco inibidor associado "PSHH-207C"	Desvio de pressão muito alta na descarga do turbo compressor C, detectado a partir do sensor PIT-207C
Arco inibidor associado "PSHH-207D"	Desvio de pressão muito alta na descarga do turbo compressor D, detectado a partir do sensor PIT-207D
Lugar "PRONTO_C3"	Modelo de coordenação da falha crítica 3 pronto para ser reiniciado
Lugar "FALHA 3 CONFIRMADA"	Caso a "FALHA 1" permaneça ativada por um intervalo de tempo $\Delta t >=$ PRESET, a mesma é confirmada e habilita a chamada do modelo de tratamento correspondente.

Tabela 5.18 - Elementos do modelo em PN interpretada da Figura 5.26(b).

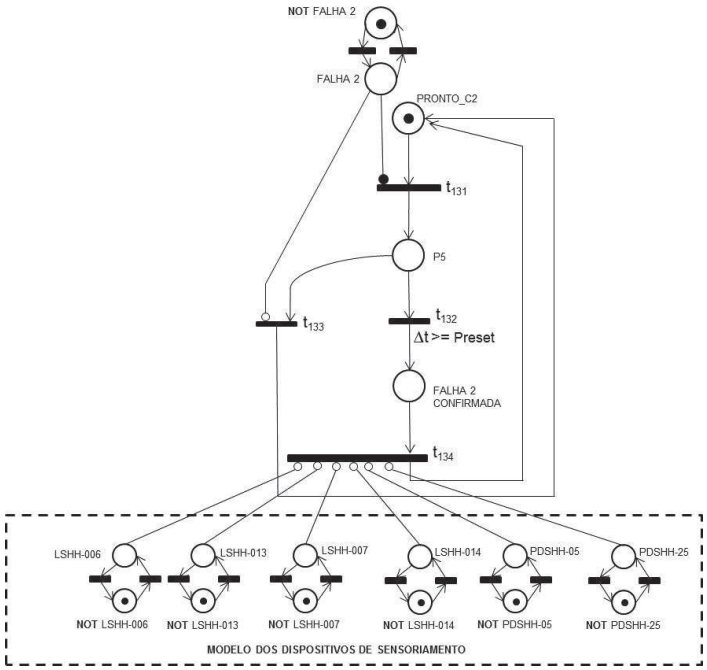
ELEMENTO	DESCRIÇÃO
Arcos habilitador/inibidor associado "FALHA 4"	Sinal de "FALHA" proveniente do modelo de diagnóstico da falha crítica 4.
Arco inibidor associado "TSHH-209A"	Desvio de temperatura muito alta na descarga do turbo compressor A, detectado a partir do sensor TIT-209A
Arco inibidor associado "TSHH-209B"	Desvio de temperatura muito alta na descarga do turbo compressor B, detectado a partir do sensor TIT-209B
Arco inibidor associado "TSHH-209C"	Desvio de temperatura muito alta na descarga do turbo compressor C, detectado a partir do sensor TIT-209C
Arco inibidor associado "TSHH-209D"	Desvio de temperatura muito alta na descarga do turbo compressor D, detectado a partir do sensor TIT-209D
Lugar "PRONTO_C4"	Modelo de coordenação da falha crítica 4 pronto para ser reiniciado
Lugar "FALHA 4 CONFIRMADA"	Caso a "FALHA 1" permaneça ativada por um intervalo de tempo $\Delta t >=$ PRESET, a mesma é confirmada e habilita a chamada do modelo de tratamento correspondente.

Construídos os modelos de coordenação das falhas críticas em PN interpretada; procedeu-se sua análise e validação de requisitos por meio de simulação com o uso da ferramenta HPSim (ANSCHUETZ, 2010).

Os modelos de coordenação de falhas críticas construídos para simulação contêm os modelos dos dispositivos de sensoriamento e modelos dos dispositivos de atuação. As Figuras 5.27 a 5.28 mostram os modelos resultantes que foram construídos a fim de se fazer a simulação dos mesmos.

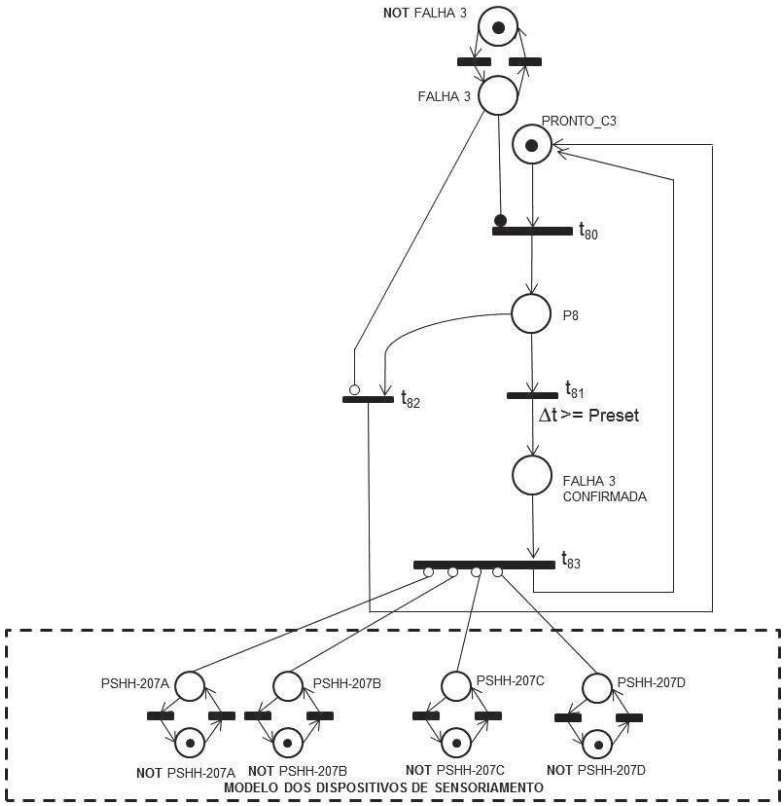


(a)

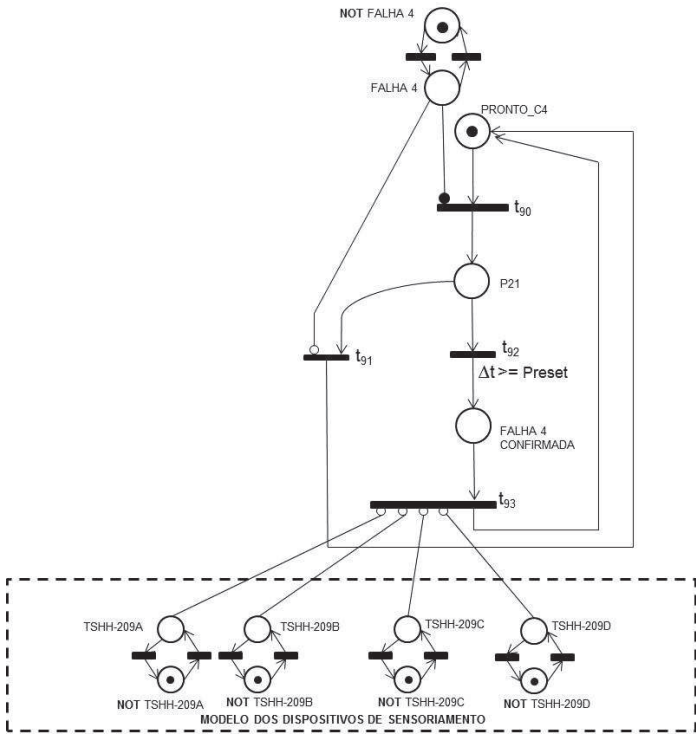


(b)

Figura 5.27 - Modelos em PN interpretada para simulação: Coordenação das (a) Falha crítica 1 e (b) Falha crítica 2.



(a)



(b)

Figura 5.28 - Modelos em PN interpretada para simulação: Coordenação das (a) Falha crítica 3 e (b) Falha crítica 4.

A fim de concluir este passo, as “boas propriedades” foram analisadas para os modelos de coordenação de falhas críticas construídos. A propriedade de reiniciabilidade foi analisada por meio de simulação dos modelos com o uso da ferramenta HPSim (ANSCHUETZ, 2010) e as propriedades de vivacidade e segurança foram analisadas com o uso da ferramenta PIPE2 (BONET et al., 2007). Um resumo da análise das “boas propriedades” para os modelos construídos é indicado na Tabela 5.19.

Tabela 5.19 – Resumo das “boas” propriedades das PN interpretadas.

Modelo em PN interpretada	**Propriedade comportamental**	**Resultado**
Coordenação da falha crítica 1	Vivacidade	Verificado com sucesso
	Segurança	Verificado com sucesso
	Reiniciabilidade	Verificado com sucesso
Coordenação da falha crítica 2	Vivacidade	Verificado com sucesso
	Segurança	Verificado com sucesso
	Reiniciabilidade	Verificado com sucesso
Coordenação da falha crítica 3	Vivacidade	Verificado com sucesso
	Segurança	Verificado com sucesso
	Reiniciabilidade	Verificado com sucesso
Coordenação da falha crítica 4	Vivacidade	Verificado com sucesso
	Segurança	Verificado com sucesso
	Reiniciabilidade	Verificado com sucesso

5.3.3 Etapa B: Análise dos modelos em PN integrados

Esta etapa B foi executada, integrando os modelos em PN para diagnóstico, coordenação e tratamento para cada “falha crítica”, de tal forma a compor as SIFs do SIS.

Uma vez que os modelos foram integrados executaram-se as seguintes atividades:

- ✓ Edição e simulação de cada modelo de SIF usando a ferramenta computacional HPSim, a fim de validação do mesmo. Adicionalmente, analisou-se a propriedade de reiniciabilidade. Para a simulação dos modelos,

foram introduzidos os modelos dos dispositivos de sensoriamento e dispositivos de atuação.

- ✓ Edição de cada modelo de SIF usando a ferramenta computacional PIPE2, a fim de analisar as propriedades de vivacidade e segurança (1-limitada).

As Figuras 5.29 a 5.32 mostram os modelos em PN, após a integração dos modelos de diagnóstico, coordenação e tratamento para cada SIF considerada neste estudo de caso.

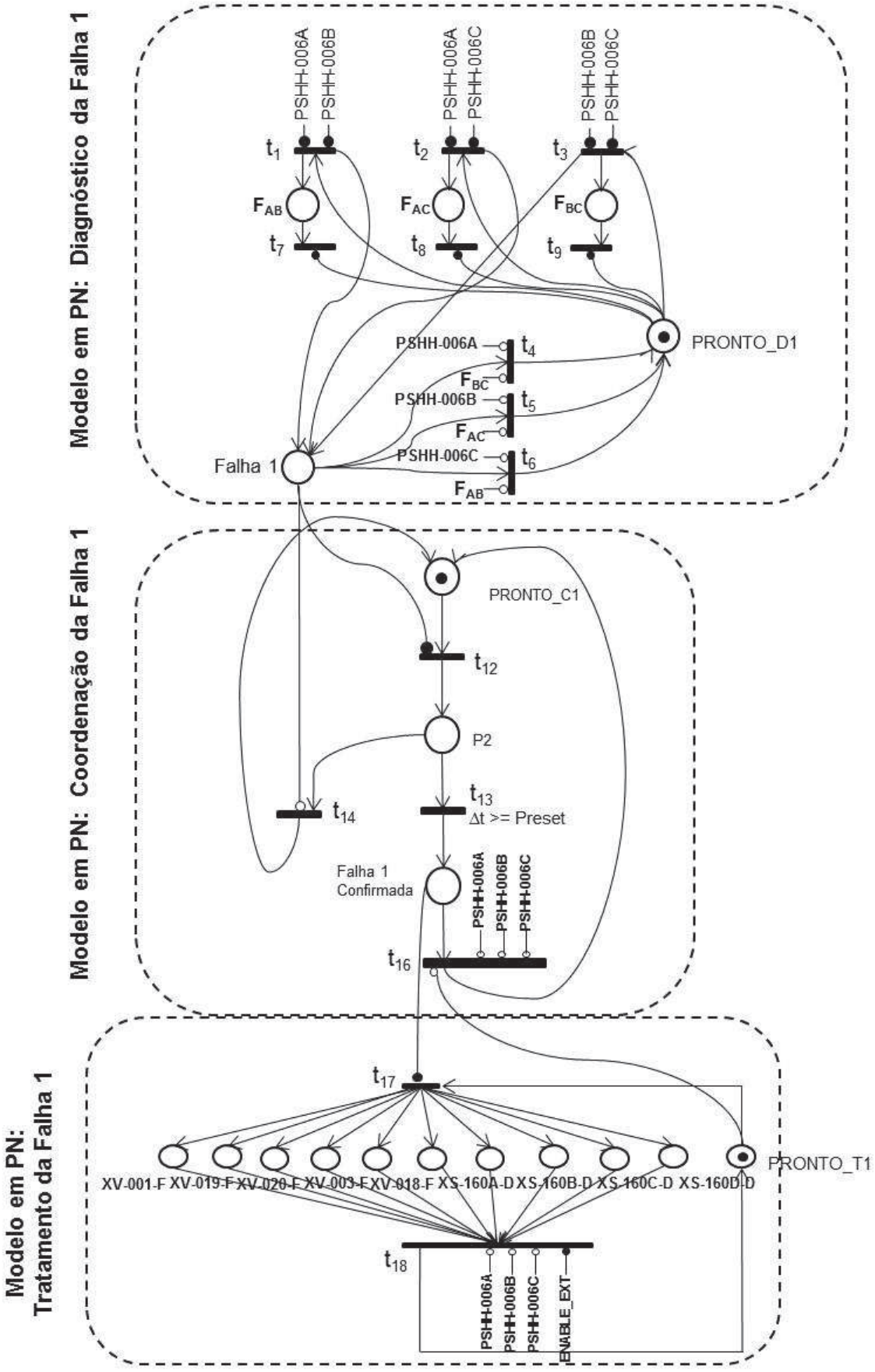


Figura 5.29 – Modelo em PN interpretada – SIF-01.

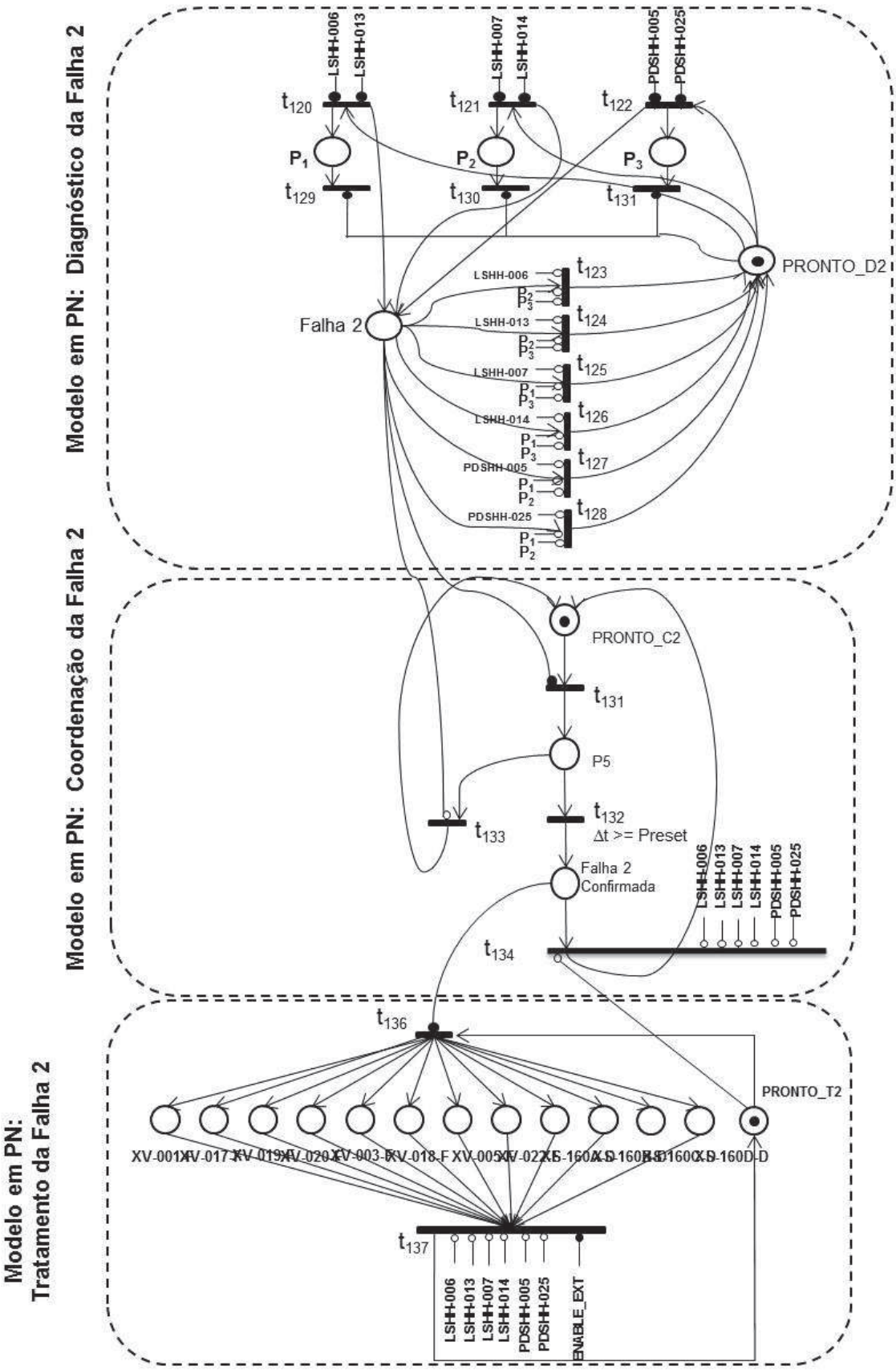


Figura 5.30 – Modelo em PN interpretada – SIF-02.

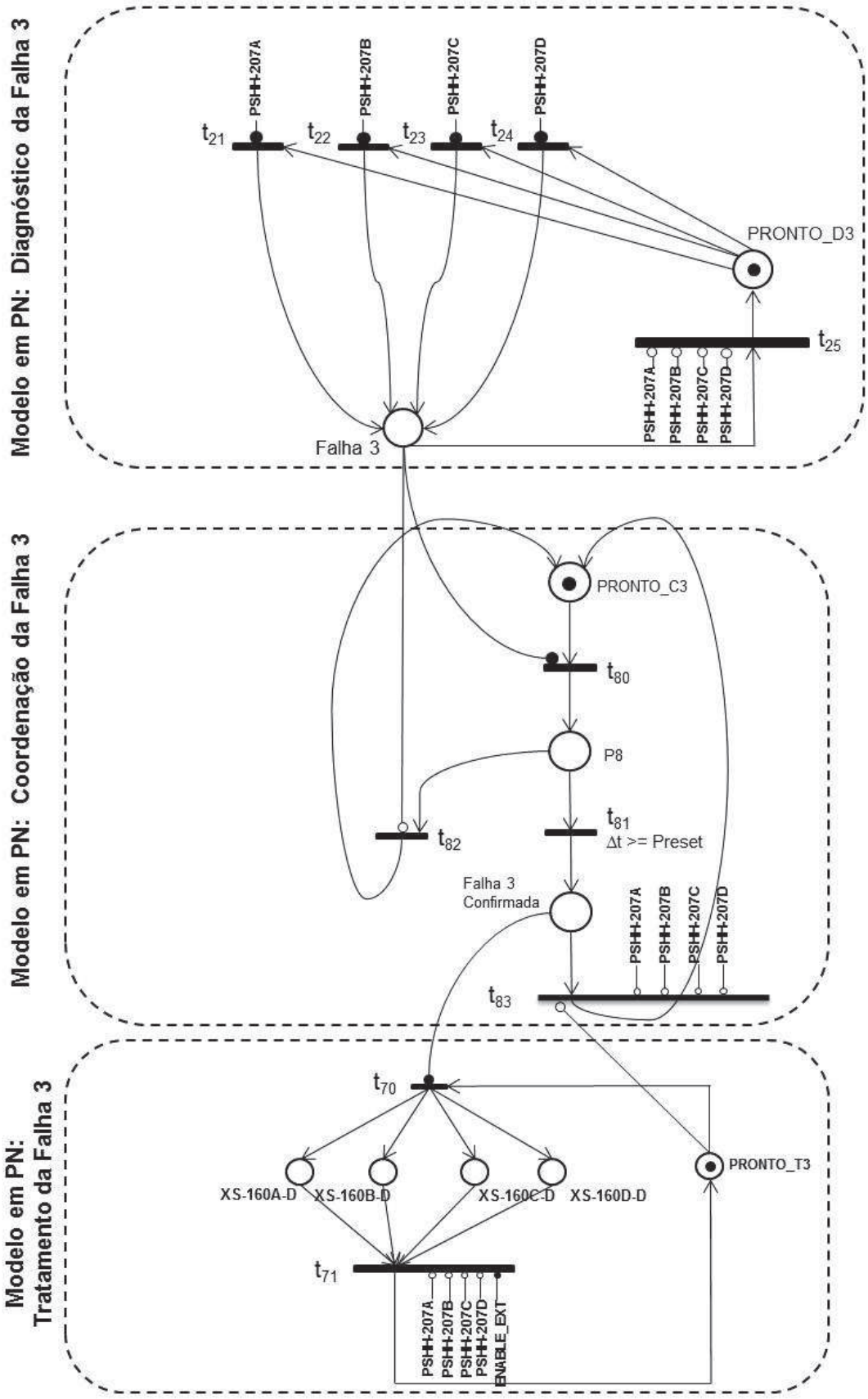


Figura 5.31 – Modelo em PN interpretada – SIF-03.

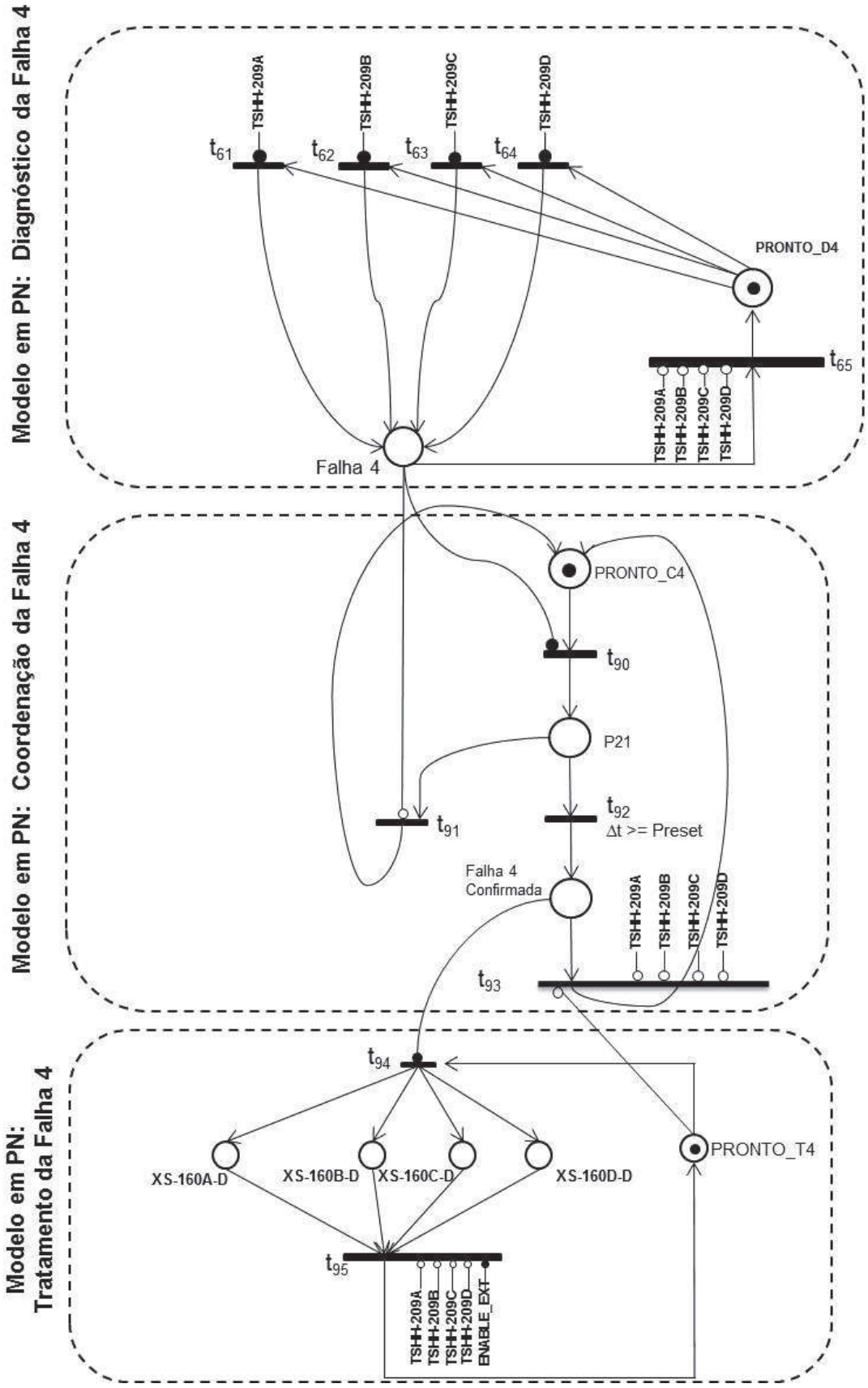


Figura 5.32 – Modelo em PN interpretada – SIF-04.

Construídos os modelos integrados das SIF-01, SIF-02, SIF-03 e SIF-04 em PN interpretada; procedeu-se suas análises e validação de requisitos por meio de simulação com o uso da ferramenta HPSim (ANSCHUETZ, 2010).

Os modelos em PN interpretada das SIFs construídos para simulação contêm os modelos dos dispositivos de sensoriamento e modelos dos dispositivos de atuação. As Figuras 5.33 a 5.36 mostram os modelos resultantes a fim de se fazer a simulação dos mesmos.

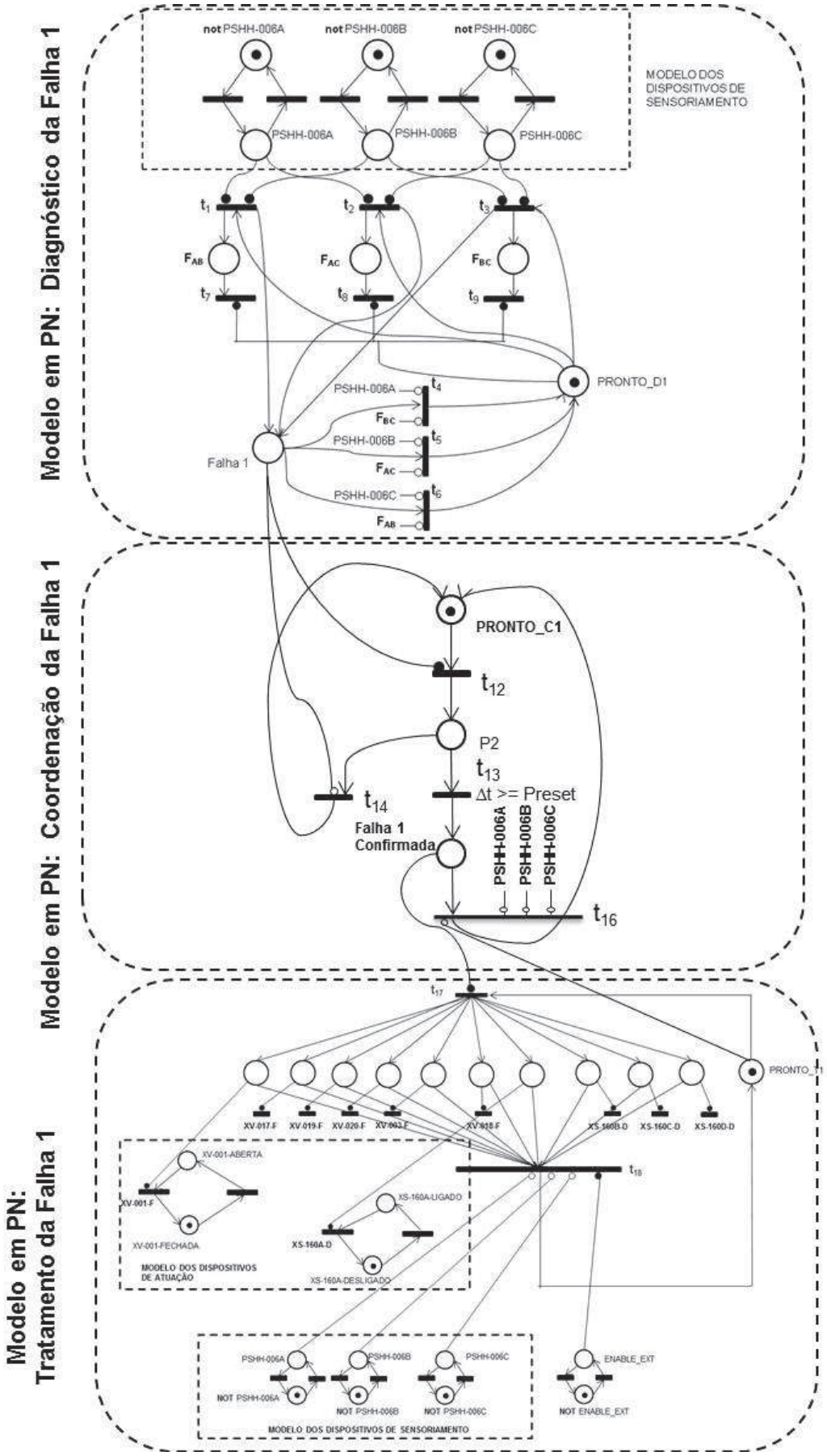


Figura 5.33 – Modelo em PN interpretada para simulação – SIF-01.

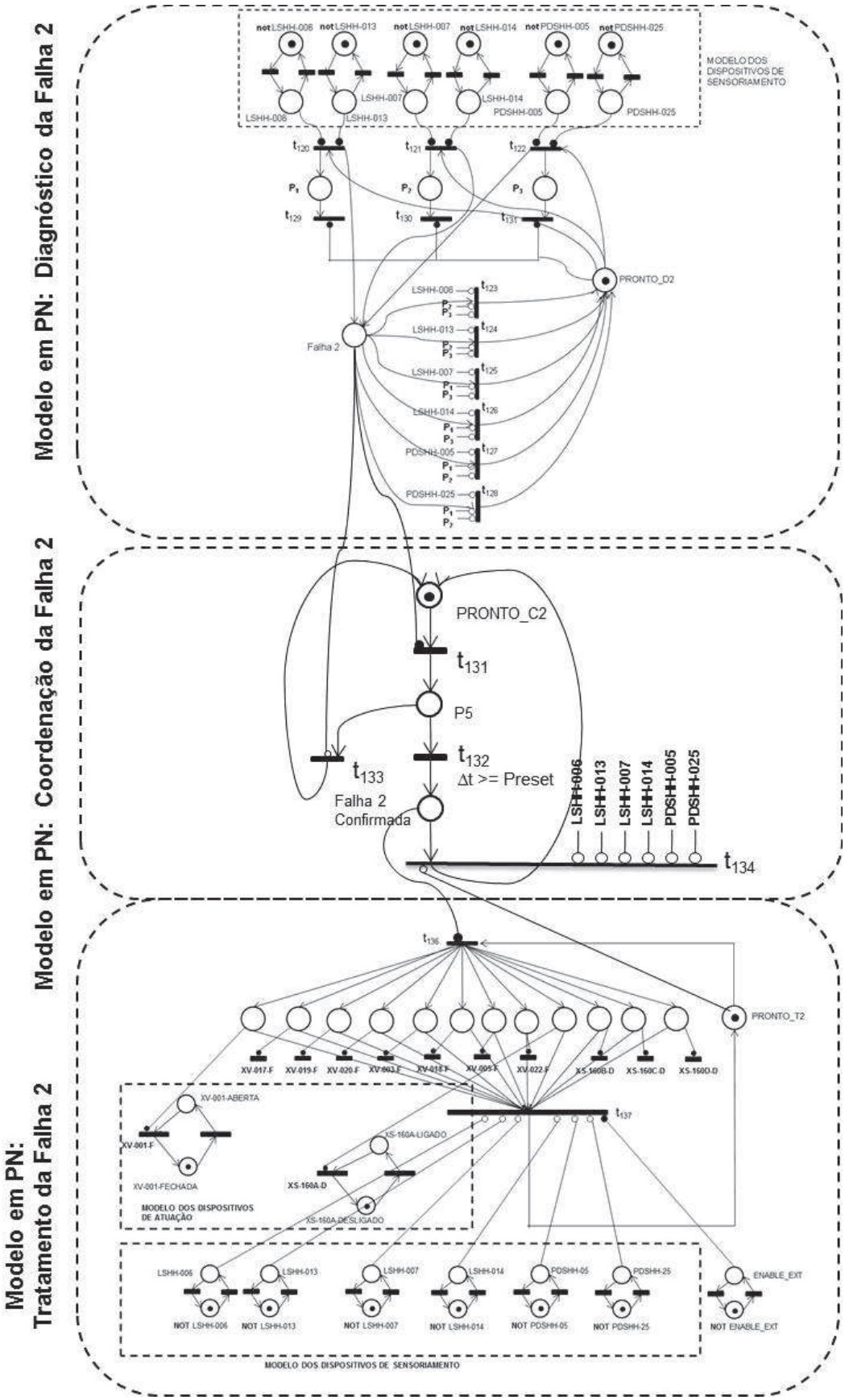


Figura 5.34 – Modelo em PN interpretada para simulação – SIF-02.

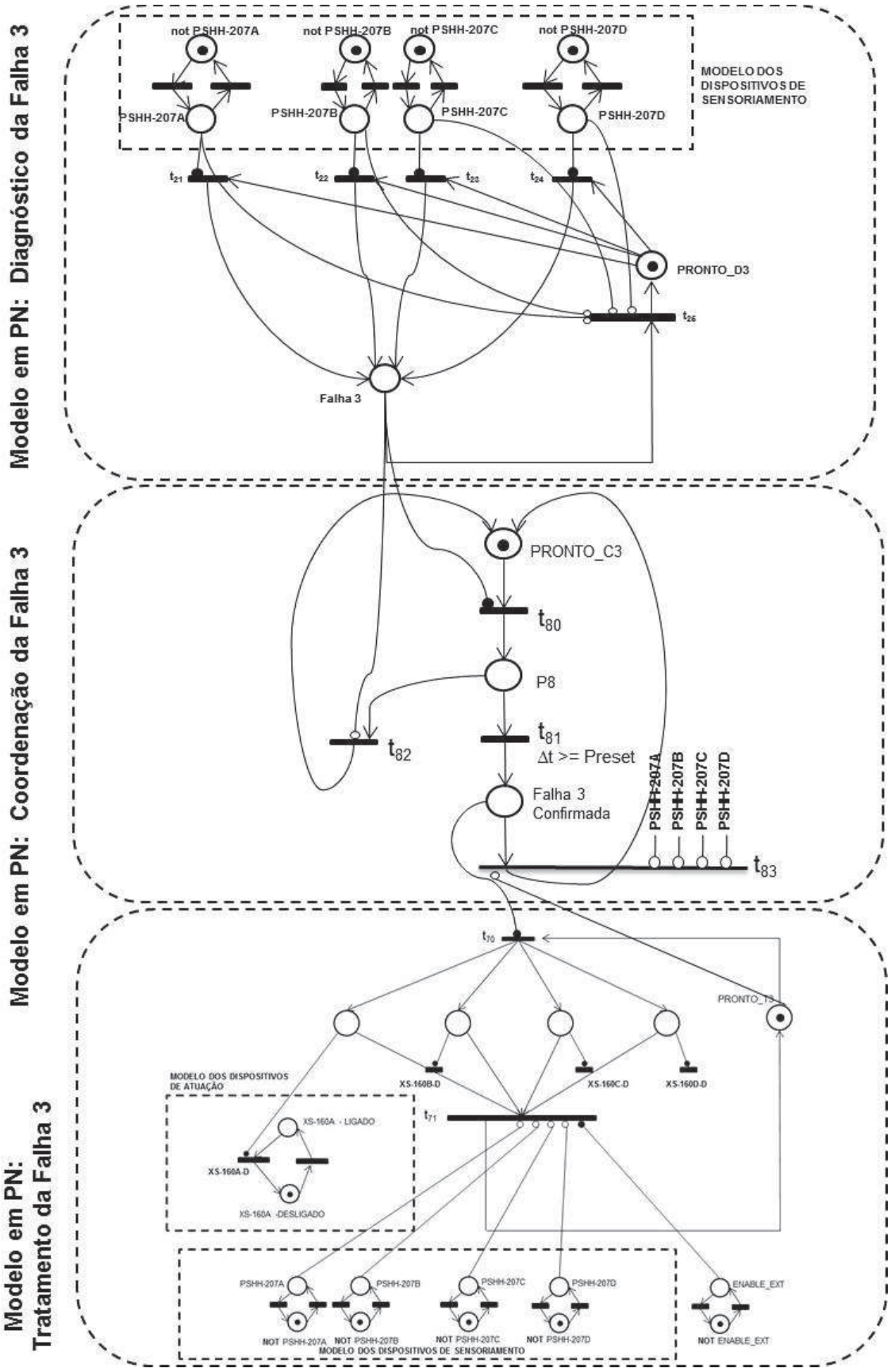


Figura 5.35 – Modelo em PN interpretada para simulação – SIF-03.

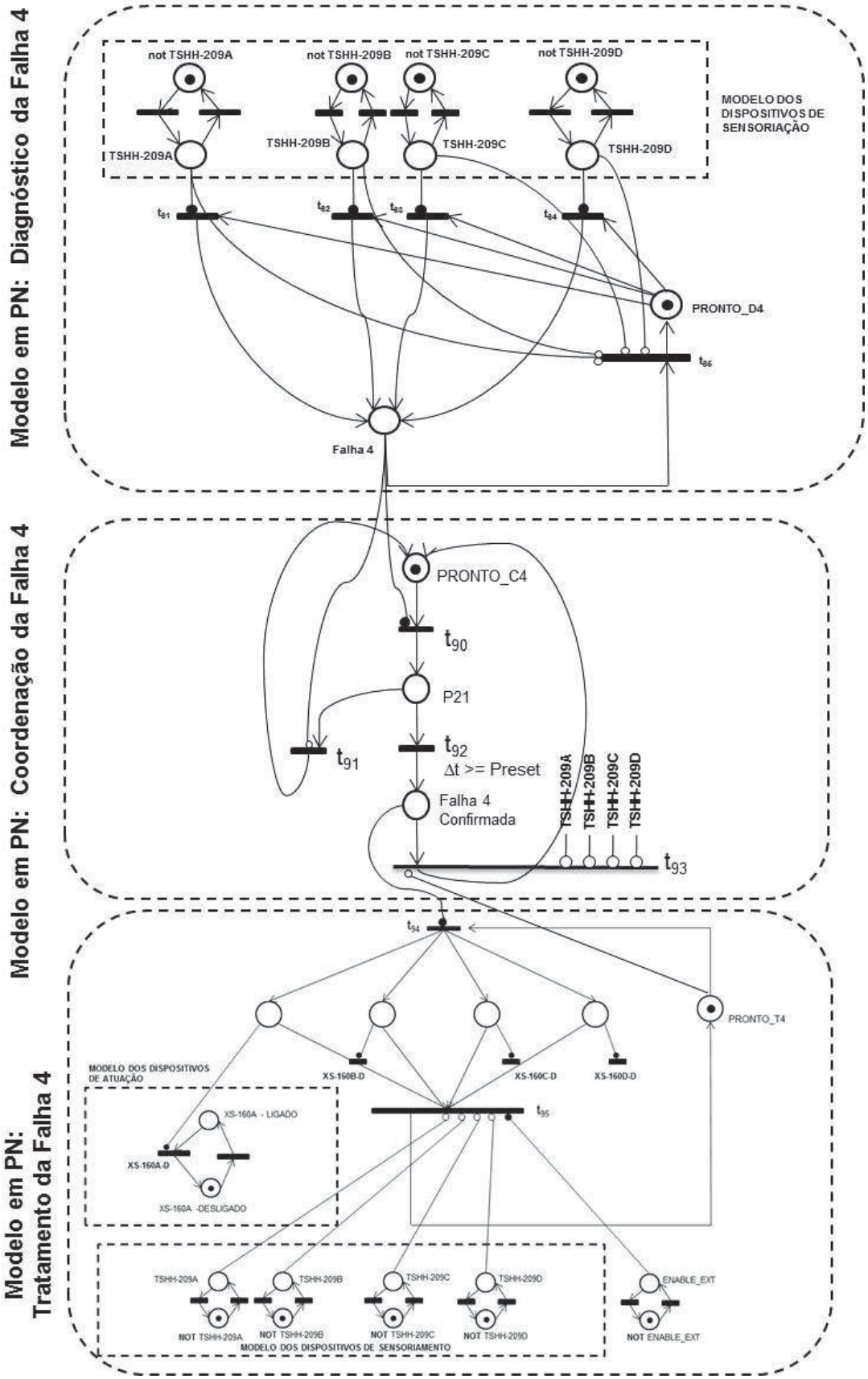


Figura 5.36 – Modelo em PN interpretada para simulação – SIF-04.

A fim de concluir esta etapa, as “boas propriedades” foram analisadas para os modelos das SIF-01, SIF-02, SIF-03 e SIF-04. A propriedade de reiniciabilidade foi analisada por meio de simulação dos modelos com o uso da ferramenta HPSim (ANSCHUETZ, 2010) e as propriedades de vivacidade e segurança foram analisadas com o uso da ferramenta PIPE2 (BONET et al., 2007). Um resumo da análise das “boas propriedades” para os modelos construídos é indicado na Tabela 5.20.

Tabela 5.20 – Resumo das “boas propriedades” dos modelos em PN.

Modelo em PN interpretada	Propriedade comportamental	Resultado
SIF-01	Vivacidade	Verificado com sucesso
	Segurança	Verificado com sucesso
	Reiniciabilidade	Verificado com sucesso
SIF-02	Vivacidade	Verificado com sucesso
	Segurança	Verificado com sucesso
	Reiniciabilidade	Verificado com sucesso
SIF-03	Vivacidade	Verificado com sucesso
	Segurança	Verificado com sucesso
	Reiniciabilidade	Verificado com sucesso
SIF-04	Vivacidade	Verificado com sucesso
	Segurança	Verificado com sucesso
	Reiniciabilidade	Verificado com sucesso

Os modelos foram editados e simulados para validar o comportamento dinâmico dos mesmos de acordo com os requisitos técnicos especificados para cada SIF e SIS. Para este estudo de caso específico, os modelos atenderam às especificações técnicas.

5.3.4 Etapa C: Geração dos programas de controle baseados nos algoritmos de controle

A etapa C foi executada, convertendo-se de forma sistemática e isomórfica os modelos integrados e validados das SIFs obtidos na etapa B, para programas de controle baseados em algoritmos de controle desenvolvidos em uma ou mais linguagens de programação prescritas pela IEC 61131-3 (2003). Para este estudo de

caso, a linguagem adotada foi o diagrama ladder (LD), pois é uma das linguagens mais comuns e amplamente utilizadas na programação de CPs.

Desta forma, no Anexo B deste trabalho, encontram-se os programas de controle baseados nos algoritmos de controle para diagnóstico, coordenação e tratamento da SIF-01.

5.3.5 Etapa D: Testes de aceitação

Conforme citado na seção 4.7 da sistemática proposta, na abordagem deste trabalho, esta etapa está de acordo com a recomendação das normas IEC 61508 (1998) e IEC 61511 (2003). Para esta aplicação, os programas dos algoritmos de controle foram editados, transferidos para a memória do CP e simulados, a partir de uma ferramenta de simulação baseada em um CP de segurança da Siemens (S7-300F, onde “F” significa “Falha segura”). Os programas dos algoritmos foram validados mediante simulação dos sinais dos sensores a partir de combinações conhecidas e definidas na especificação e os sinais de atuações para cada SIF foram verificados.

6 CONCLUSÕES FINAIS

Neste trabalho, foi proposta uma sistemática para desenvolvimento de programas de algoritmos de controle aplicados a sistemas eletrônicos programáveis (PES) no contexto de projetos de sistemas instrumentados de segurança (SIS). A abordagem deste trabalho foi dirigida para o desenvolvimento e validação de modelos de diagnóstico, coordenação e tratamento de falhas críticas; baseada em técnicas formais como a rede Bayesiana (BN) e rede de Petri interpretada (PN).

Como aspecto inicial, destaca-se a apresentação e discussão das normas vigentes relacionadas com a segurança funcional (ANSI/ISA 84.01, 1996; IEC 61508, 1998; IEC 61511, 2003); para definição dos requisitos necessários para o projeto de um SIS. Por sua vez, foi explorado o conceito de sistemas instrumentados de segurança (SIS) e sua classificação como um sistema a eventos discretos (SED), sendo apresentadas as técnicas para modelagem e validação de algoritmos de controle para SIS, abordando aspectos sobre o diagnóstico e tratamento de falhas críticas. Neste sentido, foram estudadas as técnicas de rede de Petri e variantes como a rede de Petri interpretada para a descrição de algoritmos de controle adequando à necessidade de modelar o processo de diagnóstico considerando as detecções espúrias. Foi estudada também, uma técnica de modelagem de diagnóstico que abrange a teoria de probabilidade condicional e incondicional, como a rede Bayesiana (BN) para definirem-se formalmente modelos causa-efeito.

Quanto à sistemática proposta neste trabalho, procurou-se assegurar que o desenvolvimento dos programas dos algoritmos de controle para sistemas eletrônicos programáveis (PES) em projetos de sistemas instrumentados de segurança (SIS); atende o ciclo de vida de segurança de projetos de SIS previsto nas normas IEC 61508 e IEC 61511.

Aplicou-se a sistemática proposta a um exemplo de aplicação baseado num processo industrial. O processo industrial considerado foi de uma estação de compressão de gás natural (ECOMP). Para a avaliação da sistemática proposta, foram considerados os seguintes documentos: um relatório proveniente de uma análise de riscos utilizando-se a metodologia de HAZOP, memorial descritivo do sistema de segurança (SIS), diagrama de processo e instrumentação (P&ID) e as

relações (causa → efeito) entre as variáveis que foram obtidas a partir destes documentos e do conhecimento dos especialistas, através de reuniões entre a equipe de projeto, equipe de operação e a equipe de manutenção. A sistemática mostrou-se eficiente para o desenvolvimento dos programas dos algoritmos de controle de diagnóstico e tratamento de falhas. É importante destacar que as verificações das “boas propriedades” e validações dos modelos de diagnóstico, coordenação e tratamento foram feitos a partir de ferramentas de simulação discreta, utilizando recursos computacionais. Com relação à etapa de testes finais de aceitação, os programas dos algoritmos de controle gerados, foram descarregados em um simulador de controlador programável (CP) de segurança, e as falhas críticas foram simuladas por meio da combinação de entradas a partir da especificação dada, e observadas as atuações do CP; com base em uma estação de simulação, comprovando que o comportamento do sistema de controle estava de acordo com os requisitos de segurança especificados.

6.1 CONTRIBUIÇÕES DO TRABALHO

O resultado do desenvolvimento deste trabalho traduz-se nas seguintes contribuições fundamentais:

- Proposta de uma sistemática que explora métodos formais para a modelagem e validação de algoritmos de controle aplicados a PES, no contexto de SIS; incluindo o diagnóstico, a coordenação e o tratamento de falhas críticas a partir de técnicas baseadas em rede de Petri (PN) interpretada e rede Bayesiana (BN). Este trabalho considera o diagnóstico e o tratamento para cada função instrumentada de segurança (SIF) a partir do resultado do estudo de análise de riscos baseado na metodologia de HAZOP.
- Proposta de uma nova abordagem para o desenvolvimento de projetos de sistemas de controle para sistemas instrumentados de segurança (SIS), atendendo a recomendação das normas aplicadas à segurança funcional da indústria de processos (IEC 61508, 1998) e (IEC 61511, 2003).

- Proposta de uma técnica, que auxilia na construção do relatório de HAZOP, a partir da identificação das SIFs e das suas relações causas → efeitos, obtidas através das estruturas das redes Bayesianas, construídas a partir de um banco de dados.
- Planejamento e validação de programas de controle baseados no algoritmo de controle, em conformidade com o ciclo de vida de segurança de software para projetos de SIS conforme prescrito na norma IEC 61511.

6.2 TRABALHOS FUTUROS

A seguir listam-se alguns trabalhos futuros que contribuem com o desenvolvimento de projetos de sistemas instrumentados de segurança (SIS):

- Pesquisa na área de “comissionamento virtual” no contexto de sistemas instrumentados de segurança (SIS); para o desenvolvimento de um método formal para o atendimento da fase “Testes de Aceitação” das SIFs e SIS instalados, conforme ciclo de vida de segurança (IEC 61511, 2003).

- Desenvolvimento de um sistema de comissionamento dinâmico capaz de testar os dispositivos de segurança de acordo com a norma IEC 61508;

- Desenvolvimento de um sistema de controle para mitigação de falhas críticas;

- Desenvolvimento de procedimentos para validação e verificação do sistema de controle para diagnóstico e tratamento de falhas críticas para a mitigação.

REFERÊNCIAS BIBLIOGRÁFICAS

ADAM, N.R.; ATLURI, V.; HUANG, W.-K. Modeling and analysis of workflows using Petri nets. *Journal of Intelligent Information System*, Kluwer Academic Publisher, Boston, vol 10, n. 2, pp. 131–158, 1998.

ANSCHUETZ, H. HPSim . Disponível em http://www.winpesim.de/3.html, acessado em 31/03/2011.

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

BOBBIO, A et al. Comparison of methodologies for the safety and dependability assessment of an industrial programmable logic controller. *In: N. Piccinini and E. Zio, eds., European Safety Dependability Conference* (ESREL), pp. 411-418, 2001.

BONET, P. et al. PIPE2. Disponível em http://pipe2.sourceforge.net/, acessado em 11/06/2011.

BRAUER, W.; REISIG, W. Carl Adam Petri and “Petri nets”. *Informatik-Spektrum*, Springer Berlin / Heidelberg, vol 29, n. 5, pp. 369-381, 2006.

CALVEZ, J.P. *Embedded Real-Time Systems*. New York, USA: John Wiley & Sons, 1993. ISBN 0 471 93563 8

CARDOSO, J.; VALETTE, R. Redes de Petri. Florianópolis, SC: Editora da UFSC, - 1997, CDU: 681.31:519.1

CASSANDRAS, C.G. Discrete Event Systems: Modeling and Performance Analysis. Burr Ridge: Richard D. Irwin Inc., 1993.

CASSANDRAS, C.G.; LaFORTUNE, S. Introduction to Discrete Event System. Springer, 1999.

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

CHENG, J.; BELL, D.; LIU, W. Learning Bayesian networks from data: An efficient approach based on information theory. *Technical report*, *Department of Computing Science*, University of Alberta, Canada, 1998.

CHIEN, C.F.; CHEN, S.L.; LIN, Y.S. Using Bayesian network for fault location on distribution feeder, *IEEE Transaction in Power Delivery*, vol 17, n. 3, pp. 785–793, 2002.

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

COZMAN, F.G. JavaBayes: Bayesian Networks in Java, 2001. Disponível em http://www-2.cs.cmu.edu/~javabayes/ , acessado em 13/04/2011.

CRUZ-CAMPA, H.J.; CRUZ-GOMEZ, M.J. Determine SIS and SIL using HAZOPS, *Published on-line in Wiley InterScience* (www.interscience.wiley.com), DOI 10.1002/prs. 10293, 2009.

CURY, J.E.R. Teoria de controle supervisório de sistemas a eventos discretos. *Anais do V Simpósio Brasileiro de Automação Inteligente*, Canela, RS, Brasil, pp. 68-75, 2001.

DAVID, R.; ALLA, H. Petri nets for modeling of dynamic systems - a survey. *Automatica*, vol 30, n. 2, pp. 175–202, 1994.

DARWICHE, A. What are Bayesian networks and why are their applications growing across all fields ?. *Communications of the ACM*, vol 53, pp. 80-90, 2010.

DEI-SVALDI, D; VAUTRIN, J.P. Les automates programmables. Nouvelles Technologies, nouveaux risques, príncipes de sécurité à appliquer. *Cahiers de notes documentaires*, n. 117, pp. 467-473, 1989.

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

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*, Elsevier Science Publisher Ltd., 2008b.

FALLER, R. Project experience with IEC 61508 and its consequences, *Springer Berlin / Heidelberg*, vol 2187, pp. 200-210, 2001.

FREY, G.; LITZ, L. Formal methods in PLC programming. *In Proceedings of IEEE - International Conference on Systems, Man and Cybernetics (SMC.* Nashville, pp. 2431-2436, 2000.

GOBLE, W.M – Control Systems Safety Evaluation & Reliability. *ISA – The instrumentation, Systems and Automation Society*, 2nd edition, ISBN 1-55617-636-8, 1998.

GUO, H.; YANG, X. Automatic creation of Markov models for reliability assessment of safety instrumented system". *Reliability Engineering and System Safety*, pp. 807 – 815, Elsevier Science Publisher Ltd., 2007.

HAN, R et al. A Petri net theory-based method for modeling web service-based systems. *In: Proc. of 4th Intern. Conf. on Wireless Communications, Networking and Mobile Computing* (*WiCOM*), pp. 1–7, Dalian, China, 2008.

HAMADI, R.; BENATALLAH, B.A. A Petri net-based model for web service composition*. In Proceedings of the 14th Australasian Database Conference (ADC'03)*. Adelaide, Austrália: Australian Computer Society, pp. 191-200, 2003.

HO, Y.-C. Performance evalution and perturbation analysis of discrete event dynamic systems. *IEEE Transaction on Automatic control*, vol 32, issue 7, pp. 563-572, 1987.

HO, Y.-C. Discrete event dynamics systems analysing complexity and performance in the Modern World. *IEEE Press*, New York, 1992.

HRUSCHKA JR, E.R. Imputação Bayesiana no contexto da Mineração dos Dados. Tese (Doutorado) – Universidade Federal do Rio de Janeiro, Rio de Janeiro, Brasil, 2003. Disponível em http://wwwp.coc.ufrj.br/teses/doutorado/inter/2003/teses/HRUSCHKA%20JUNIOR_ER_03_t_D_int.pdf , acessado em 13/04/2011

IEC, International Electrotechnical Commission. Functional Safety of Electrical / Electronic / Programmable Electronic Safety-related Systems (IEC 61508), International Electrotechnical Commission, Geneva, Switzerland, 1998. Disponível em http://www.iec.ch; acessado em 02/04/2011.

IEC, International Electrotechnical Commission. Functional safety - Safety instrumented systems for the process industry sector - (IEC 61511), International Electrotechnical Commission, Geneva, Switzerland, 2003. Disponível em http://www.iec.ch; acessado em 02/04/2011

ISA, Application of Safety Instrumented Systems for the Process Industries, ANSI/ISA-SP 84.01-1996, ISA, Research Triangle Park, NC,1996.

IEC, International Electrotechnical Comission, Programmable Controllers (IEC 61131: Part 3) Programming Languages, 2003.

ITO, Y. A desirable production structure looking toward the 21st century – Anthropocentric Intelligence-based Manufacturing. In: Anais do *XI Congresso Brasileiro de Engenharia Mecânica (COBEM)*, Brasil, São Paulo, pp. 23-32, 1991.

JENSEN, K. Coloured Petri nets: Basic Concepts, Analysis Methods and Practical Use. Berlin: Springer Verlag, 1992.

KAMTEKAR, D.M. Implementation of Functional Safety in a robotic manufacturing cell using IEC 61508 Standard and Siemens Technology. Master Thesis, Kate Gleason College of Engineering, Rochester Institute of Technology, New York, 2009.

KANESHIRO, P.J. et al. Modeling of collision resolution algorithm in Lonworks networks. In: *Proceedings of ASME International Mechanical Engineering Congress and Exposition*. Seattle: vol 9, pp. 743-749, 2008. ISBN 0791843033

KANNAN, P.R. Bayesian networks: application in safety instrumentation and risk reduction. *ISA Transactions*, pp. 255-259, 2007.

KIEPUSZEWSKI, B.; HOFSTED, A.; AALST, W. Fundamentals of control flow in workflows. *Acta Informatica*, vol 39, n. 3, pp. 143-209, 2003, ISSN 0001-5903.

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 Electronics*, vol 52, n. 5, pp. 1220-1226, 2005, ISSN 0278-0046.

LEE, G.-B.; ZANDONG, H.; LEE, J.-S. Automatic generation of ladder diagram with control Petri net. *Journal of Intelligent Manufacturing*, vol 15, pp. 245-252, 2004.

LERNER, U. et al. Monitoring a complex physical system using a hybrid dynamic Bayes net. In: *Proceeding 18th Conf. on Uncertainty in AI (UAI),* Edmonton, Canada, pp. 301–310, 2002.

LI, Z.; ZHOU, M. Elementary siphons of Petri nets and their application to deadlock prevention in flexible manufacturing systems. *IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans*, vol 34, n. 1, pp. 38–51, 2004, ISSN 1083-4427.

LI, Z.; ZHOU, M. Control of elementary and dependent siphons in Petri nets and their application, *IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans*, vol 38, n. 1, pp. 133–148, 2008, ISSN 1083.4427.

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

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

LUNDTEIGEN, M.-A; RAUSAND, M; UTNE, I.-B. Integrating RAMS engineering and management with the safety life cycle of IEC 61508. *Reliability Engineering and System Safety*, pp. 1894 -1903, Elsevier Science Publisher Ltd., 2009.

LUO, J; TU, H; PATTIPATI, K; QIAO, L; CHIGUSA, S. Graphical models for diagnosis knowledge representation and inference, *Autotestcon 2005*, *IEEE*, pp. 483-489, 2005. ISBN: 0-7803-9101-2, DOI 10.119/AUTEST.2005.1609185

MARCOS, J.; ÁLVAREZ, J.; FERNÁNDEZ, S. Design of safety systems with Programmable Logic. Disponível em

http://www.dte.uvigo.es/home/jacobo_alvarez/documentos/Curriculum/sprts05.pdf, acessado em 13/04/2011.

MIYAGI, P.E Controle Programável – Fundamentos do Controle de Sistemas a Eventos Discretos. São Paulo, SP: Editora Edgard Blucher Ltda, 3ª reimpressão-2007, ISBN 85-212-0079-X.

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. In: *Proceeding of IEEE International Conference on Automation Science and Engineering (CASE 2007)*, pp. 357 - 362, 2007.

MURATA, T. Petri nets: properties, analysis and applications, *Proceedings of IEEE*, vol 77, pp. 541–580, 1989.

MURPHY, K. Bayes Net Toolbox for Matlab, 2007. Disponível em http://code.google.com/p/bnt/, acessado em 01/04/2011.

MUSIC, G.; GRADISAR, D.; MATKO, D. IEC 61131-3 compliant control code generation from discrete event models. pp. 346-351, 2005.

NASSAR, M.G.V. et al. Modeling and analyzing of the material entry flow system in a pickling line process using Petri nets. In: *ABCM Symposium Series in Mechatronics*, vol 3, pp. 444-453, 2008.

NILSSON, N. J. Artificial Intelligence: A new synthesis. San Francisco: Morgan Kaufmann, 1998.

PEARL, J. Causality: Models Reasoning and Inference, Cambridge University Press, 2000.

PETERSON, J.L. Petri nets. *ACM Computing Surveys*, ACM, New York, USA, vol 9, n. 3, pp. 223-252, 1977, ISSN 0360-0300.

RAMADGE, P.J.; WONHAM, W.M. The control of discrete event systems. In: *Proceedings of the IEEE*, vol 77, n. 1, 1989.

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, 2002.

RIASCOS, L.A.M.; MIYAGI, P.E. Modeling and analysis of fault-tolerant systems for machining operations based on Petri nets, *Control Engineering Practice*, vol 14, pp. 397-408, 2006.

RIASCOS, L.A.M.; SIMÕES, M.G.; MIYAGI, P.E. A Bayesian network fault diagnostic system for proton exchange membrane fuel cells, *Journal of Power Sources*, vol 165, n. 1, pp. 267-278, 2007.

ROUVROYNE, J.L.; BLIEK, E.G. – Comparing safety analysis techniques, *Reliability Engineering and System Safety*, Elsevier Science Publisher Ltd, pp. 289 – 294, 2002.

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

RUSSELL, S.; NORVIG, P. *Artificial Intelligence: A modern approach.* New Jersey: Prentice-Hall, pp. 932, 1995.

SALLAK, M.; SIMON, C.; AUBRY, J., A fuzzy probabilistic approach for determining safety integrity level, *IEEE Transaction on Fuzzy Systems*, vol 16, n.1, pp. 239-248, 2008

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

SEIXAS DE OLIVEIRA, L. Lifecycle cost analysis of alternatives for complying with required safety integrity level (SIL) at a petrochemical plant. In: *Proceeding of CCPS Health and Safety Conference*, Buenos Aires, Argentina, 2008.

STAVRIANIDIS, P.; BHIMAVARAPU, K. Safety instrumented functions and safety integrity levels (SIL), *ISA Transactions*, vol 37, pp. 337-351, 1998.

SQUILLANTE JR, R.; SANTOS FILHO, D.J.; JUNQUEIRA, F.; MIYAGI, P.E. Desenvolvimento de sistemas de controle para sistemas instrumentados de segurança. In: Anais do *9th IEEE/IAS International Conference on Industry Applications* (INDUSCON), São Paulo, 2010a, ISBN 978-85-99916-02-5.

SQUILLANTE JR, R.; SANTOS FILHO, D.J.; GARCIA MELO, J.I.; JUNQUEIRA, F.; FATTORI, C.; MIYAGI, P.E. Safety instrumented system designed based on Bayesian network and Petri net, *In: Proceedings of 8th International Conference on Mathematical problems in Engineering, Aerospace and Sciences* (ICNPAA), São Jose dos Campos, Brazil, 2010b.

SQUILLANTE JR, R.; SANTOS FILHO, D.J.; RIASCOS, L.A.M.; JUNQUEIRA, F.; MIYAGI, P.E. Mathematical method for modeling and validating of safety instrumented system designed according to IEC 61508 and IEC 61511, In: Anais do *21st International Congress of Mechanical Engineering (COBEM)*, Natal – RN, Brazil, 2011a.

SQUILLANTE JR, R.; SANTOS FILHO, D.J.; JUNQUEIRA, F.; MIYAGI, P.E. Development of Control Systems for Safety Instrumented Systems, In: revista IEEE América Latina, vol. 9, Issue 4, pp. 451-457, 2011b, ISSN: 1548-0992.

SUMMERS, A.; RANEY, G. Common cause and common sense, designing failure out of your safety instrumented systems (SIS). In: *ISA Transactions*, vol 38, pp. 291-299, 1999.

THAPA, D.; DANGOL, S.; WANG, G. Transformation from Petri net model to Programmable Logic Controller using one-to-one mapping technique. vol 2, pp. 229-233, 2005.

WANG, X.; CHEN, G.; XIE, Y.;GUO, Z. Fault detection and diagnosis based on time Petri net. In: *Proceedings of Eighth International Conference on Electronic Measurement and Instruments*, Beijing, China, 2007.

WIGHTKIN, N.; BUY, U.; DARABI, H. Formal modeling of sequential function charts with time petri nets. *IEEE Transactions on Control Systems*, vol 99, pp. 1-10, 2010.

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

XU, X et al. A novel modeling design method for automated storage and retrieval system based on Petri nets. In: *Proceedings of the IEEE International Conference on Automation and Logistics*, Jinan, China, pp. 2046–2051, 2007.

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

ZHOU, M; DiCesare, F. Petri Net Synthesis for Discrete Event Control of Manufacturing Systems, Boston, USA, Kluwer Ac. Publisher, 1993.

ZURAWSKI, R.; ZHOU, M. Petri nets and industrial applications: A tutorial**.** *IEEE Transactions on Industrial Electronics*, vol 41, n. 6, pp. 567-583, 1994.

YOO, T; JEONG, B; CHO, H., A Petri nets based functional validation for services composition, *Expert Systems with Applications*, vol 37, pp. 3768–3776, 2010.

ANEXO A

Segue abaixo, o programa computacional baseado no algoritmo K2 que foi aplicado para o exemplo de aplicação da estação de compressão de gás (ECOMP).

```
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%           Geração da estrutura da rede Bayesiana (BN)                  %
%           aplicando o algoritmo K2 (busca e pontuação)                 %
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

clear;

%variáveis
%N = 21;                                                      %número de nós
Falha1=1; Falha2=2; Falha3=3; Falha4=4;                       %causas

Pshh006A=5; Pshh006B=6; Pshh006C=7; Lshh006=8; Lshh007=9; Pdshh005=10;
%sensores
Lshh013=11; Lshh014=12; Pdshh025=13;Pshh207A=14; Pshh207B=15; Pshh207C=16;
%sensores
Pshh207D=17; Tshh209A=18; Tshh209B=19; Tshh209C=20; Tshh209D=21;
%sensores

% Carregando o arquivo texto (Tabela causa --> efeito)
dat = load('Ftable_Ecomp_rev3.txt');

[Ncases N]=size(dat);

for j=1:N-1
    for i=1:Ncases
        date(j,i)=dat(i,j+1);     %eliminando a 1ª coluna da Tabela (LOAD)
    end;
end;

N=N-1;

k=0;
for j=1:Ncases
    k=k+1;
    c=0;
    for i=1:N
        c=c+date(i,j);              %eliminando casos sem efeitos
        dato(i,k)=date(i,j);
    end;
end;

Ncases=k;

for i=1:N
    for j=1:Ncases
        data(i,j)=dato(i,j)+1;       %falso=1  verdadeiro=2
    end;
end;

node_size = 2*ones(1,N);
```

```
% Aprendizagem da estrutura da BN
order = [Falha1 Falha2 Falha3 Falha4 Pshh006A Pshh006B Pshh006C Lshh006
         Lshh007 Pdshh005 Lshh013 Lshh014 Pdshh025 Pshh207A Pshh207B
         Pshh207C Pshh207D Tshh209A Tshh209B Tshh209C Tshh209D];
max_fan_in = 3;                    %número máximo de pais
dagK2 = learn_struct_K2(data, node_size, order,'max_fan_in', max_fan_in);

% NetStructure in Matrix form
dagK2

arcs=0;
for i=1:N
    for j=1:N
        arcs=arcs+dagK2(i,j);
    end;
end;
arcs                                          %número de arcos

%pdag = learn_struct_pdag_pc('dsep', N, max_fan_in, dagK2);
%pdag

% Visualizing The net
figure(1);
draw_graph(dagK2);
%figure (2);
%draw_graph(pdag);
```

ANEXO B

Os programas de controle baseados nos algoritmos de controle para diagnóstico, coordenação e tratamento das falhas críticas, foram gerados a partir dos modelos integrados em PN mostrados nas Figuras 5.29, 5.30, 5.31 e 5.32 para a linguagem ladder (LD). A ferramenta utilizada para edição dos programas de controle foi o STEP 7 da empresa Siemens, e os programas de controle foram organizados de forma estruturada, de acordo com o fluxograma apresentado na Figura B.1 onde se destacam os seguintes elementos:

OB100 Rotina de inicialização: É a rotina executada pelo CP de segurança somente no 1º scan. Esta rotina contém o algoritmo necessário para definição das marcas iniciais da PN dos modelos de diagnóstico, coordenação e tratamento da SIF-01.

OB1 Rotina principal: É a rotina executada pelo CP de segurança a cada ciclo de “scan”. Esta rotina contém os algoritmos de chamada das rotinas FC1, FC2 e FC3 de forma sequencial.

FC1 Rotina de diagnósticos: contém o algoritmo de diagnóstico da falha crítica – SIF-01.

FC2 Rotina de coordenação: contém o algoritmo de coordenação da falha crítica – SIF-01.

FC3 Rotina de tratamento: contém o algoritmo de tratamento da falha crítica – SIF-01.

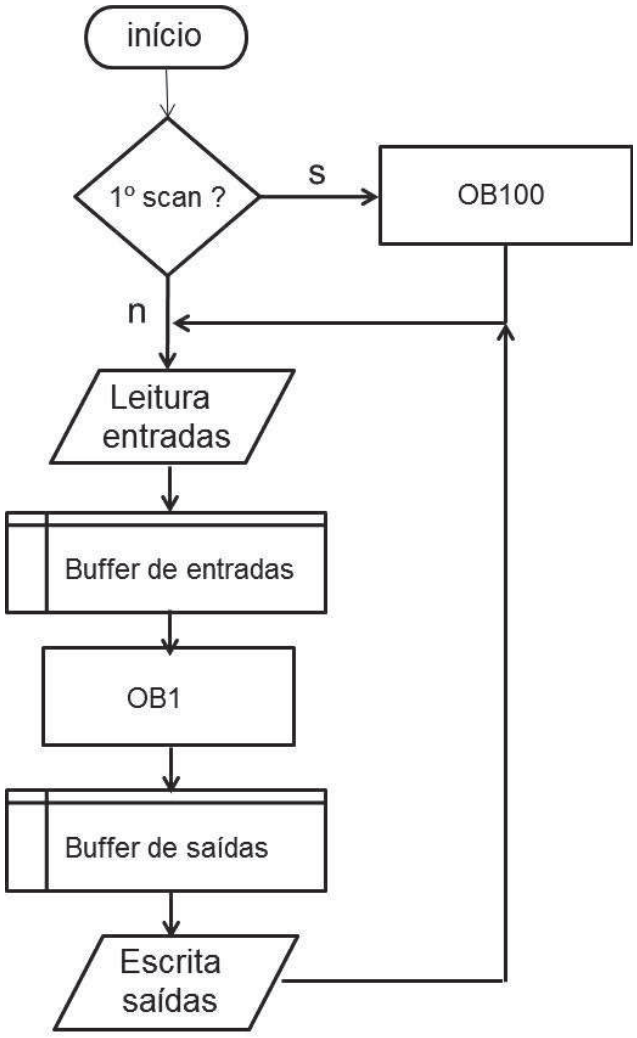


Figura B.1 – Fluxograma de execução do programa de controle.

B.1 DESCRIÇÃO DO MÉTODO DE CONVERSÃO

Os modelos em PN foram convertidos para os programas dos algoritmos de controle de forma sistemática e isomórfica obedecendo-se o seguinte método:

a) Etapa 1: Habilitação das transições

Nesta etapa 1, constrói-se cada linha de programa contendo a lógica de habilitação de cada transição do modelo em PN interpretada;

b) Etapa 2: Disparo das transições

Nesta etapa 2, constrói-se cada linha de programa contendo a lógica de disparo das transições do modelo em PN interpretada, atualizando a marcação dos lugares por meio de comandos do tipo *set* e *reset* associados às variáveis internas e externas.

Um exemplo de aplicação deste método é mostrado a seguir. A Figura B.2 mostra um modelo em PN interpretada.

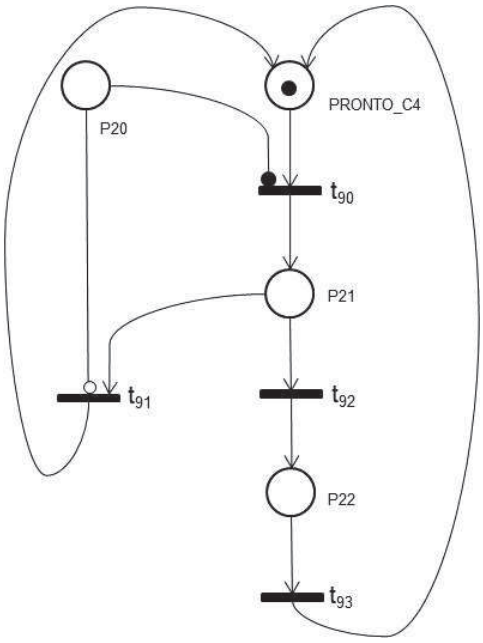


Figura B.2 - Modelo em PN.

A Figura B.3 mostra a Etapa 1: Habilitação das transições

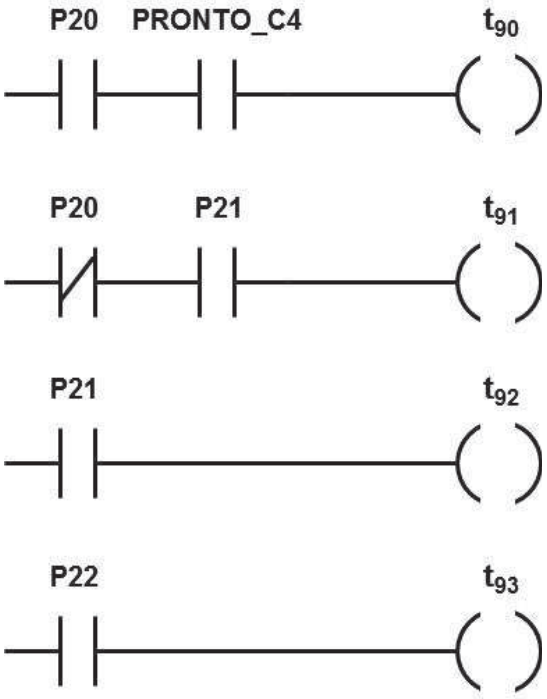


Figura B.3 - Lógica de habilitação das transições.

A Figura B.4 mostra a Etapa 2: Disparo das transições

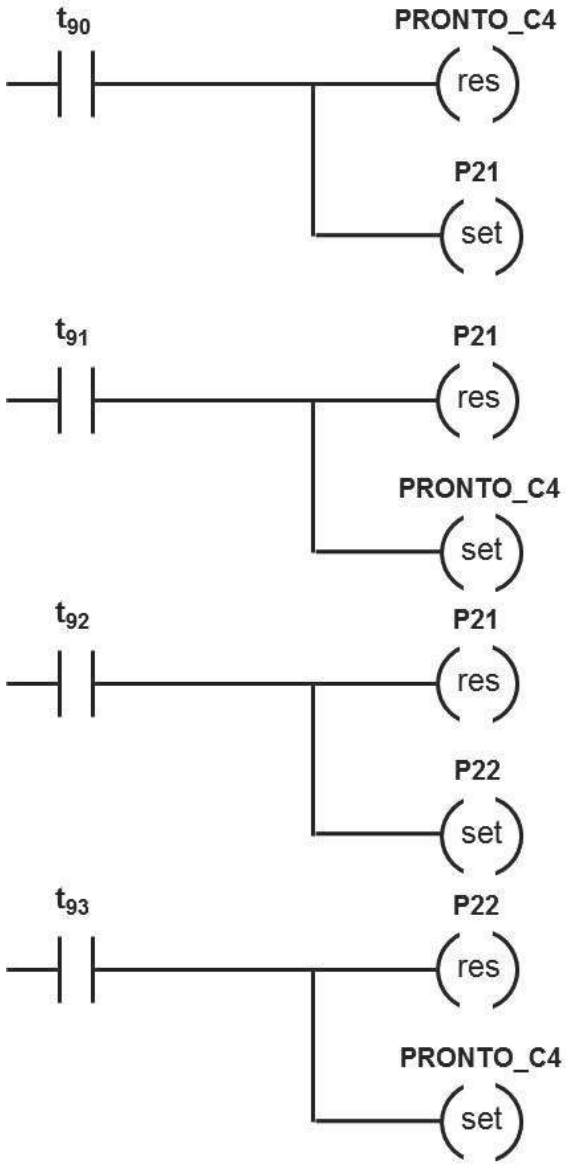


Figura B.4 - Lógica de disparo das transições.

B.2 GERAÇÃO DO PROGRAMA DE CONTROLE DA SIF-01

A Tabela B.1 mostra a lista de entradas e saídas usada na programação do algoritmo de diagnóstico da SIF-01.

Tabela B.1 – Lista de entradas e saídas – Diagnóstico da SIF-01

ELEMENTO	ENDEREÇO	Tipo de dado
Arco habilitador associado "PSHH-006A"	M100.0	BOOLEANO
Arco habilitador associado "PSHH-006B"	M100.1	BOOLEANO
Arco habilitador associado "PSHH-006C"	M100.2	BOOLEANO
Lugar "FAB"	M1.3	BOOLEANO
Lugar "FAC"	M1.4	BOOLEANO
Lugar "FBC"	M1.5	BOOLEANO
Lugar "PRONTO_D1"	M1.0	BOOLEANO
Lugar "Falha 1"	M1.1	BOOLEANO
Transição "t1"	M80.0	BOOLEANO
Transição "t2"	M80.1	BOOLEANO
Transição "t3"	M80.2	BOOLEANO
Transição "t4"	M80.3	BOOLEANO
Transição "t5"	M80.4	BOOLEANO
Transição "t6"	M80.5	BOOLEANO
Transição "t7"	M80.6	BOOLEANO
Transição "t8"	M80.7	BOOLEANO
Transição "t9"	M83.0	BOOLEANO

A Tabela B.2 mostra a lista de entradas e saídas usada na programação do algoritmo de coordenação da SIF-01.

Tabela B.2 – Lista de entradas e saídas – Coordenação da SIF-01

ELEMENTO	ENDEREÇO	Tipo de dado
Arco habilitador associado “PSHH-006A"	M100.0	BOOLEANO
Arco habilitador associado “PSHH-006B”	M100.1	BOOLEANO
Arco habilitador associado “PSHH-006C”	M100.2	BOOLEANO
Lugar “PRONTO_C1”	M2.0	BOOLEANO
Lugar “P2”	M2.1	BOOLEANO
Lugar “FALHA 1 CONFIRMADA”	M2.2	BOOLEANO
Transição “t12”	M81.0	BOOLEANO
Transição “t13”	M81.1	BOOLEANO
Transição “t14”	M81.2	BOOLEANO
Transição “t16”	M80.3	BOOLEANO

A Tabela B.3 mostra a lista de entradas e saídas usada na programação do algoritmo de tratamento da SIF-01.

Tabela B.3 – Lista de entradas e saídas – Tratamento da SIF-01

ELEMENTO	ENDEREÇO	Tipo de dado
Arco habilitador associado “PSHH-006A"	M100.0	BOOLEANO
Arco habilitador associado “PSHH-006B”	M100.1	BOOLEANO
Arco habilitador associado “PSHH-006C”	M100.2	BOOLEANO
Lugar “PRONTO_T1”	M3.0	BOOLEANO
Lugar “ENABLE-EXT”	M110.0	BOOLEANO
Lugar “XY-001”	Q32.0	BOOLEANO
Lugar “XY-017”	Q32.1	BOOLEANO
Lugar “XY-019”	Q32.2	BOOLEANO

ELEMENTO	ENDEREÇO	Tipo de dado
Lugar “XY-020”	Q32.3	BOOLEANO
Lugar “XY-003”	Q32.4	BOOLEANO
Lugar “XY-018”	Q32.5	BOOLEANO
Lugar “XY-160A”	Q33.0	BOOLEANO
Lugar “XY-160B”	Q33.1	BOOLEANO
Lugar “XY-160C”	Q33.2	BOOLEANO
Lugar “XY-160D”	Q33.3	BOOLEANO
Transição “t17”	M82.0	BOOLEANO
Transição “t18”	M82.1	BOOLEANO

Assim sendo, nas próximas páginas seguem os programas de controle dos algoritmos de controle de diagnóstico, coordenação e tratamento gerados para a SIF-01.

OB100 - <offline>

"ESTADOS INICIAIS" Complete Restart
Name: **Family:**
Author: **Version:** 0.1
Block version: 2
Time stamp Code: 8/30/2011 12:17:13 PMPM
Interface: 2/15/1996 4:51:10 PMPM
Lengths (block/logic/data): 00128 00012 00020

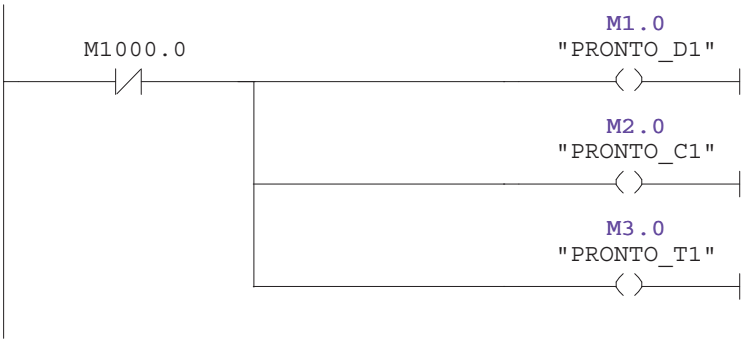
Name	Data Type	Address	Comment
TEMP		0.0	
OB100_EV_CLASS	Byte	0.0	16#13, Event class 1, Entering event state, Event logged in diagnostic buffer
OB100_STRTUP	Byte	1.0	16#81/82/83/84 Method of startup
OB100_PRIORITY	Byte	2.0	Priority of OB Execution
OB100_OB_NUMBR	Byte	3.0	100 (Organization block 100, OB100)
OB100_RESERVED_1	Byte	4.0	Reserved for system
OB100_RESERVED_2	Byte	5.0	Reserved for system
OB100_STOP	Word	6.0	Event that caused CPU to stop (16#4xxx)
OB100_STRT_INFO	DWord	8.0	Information on how system started
OB100_DATE_TIME	Date_And_Time	12.0	Date and time OB100 started

Block: OB100 "Complete Restart"

```
DEFINIÇÃO DOS ESTADOS INICIAIS DOS MODELOS DE DIAGNÓSTICO, COORDENAÇÃO E
TRATAMENTO DA SIF-01
ESTES ESTADOS SÃO ATUALIZADOS NO 1o SCAN DO CP DE SEGURANÇA
=========================================================================
ESTUDO DE CASO: ESTAÇÃO DE COMPRESSÃO DE GÁS (ECOMP)
=========================================================================
AUTOR: REINALDO SQUILLANTE JÚNIOR
DATA: 30/08/2011
```

Network: 1

DEFINE OS ESTADOS INICIAIS DOS MODELOS SIF-01



OB1 - <offline>

"PRINCIPAL"

Name: **Family:**
Author: **Version:** 0.1
Block version: 2
Time stamp Code: 8/31/2011 10:14:27 AMAM
Interface: 2/15/1996 4:51:12 PMPM
Lengths (block/logic/data): 00168 00050 00022

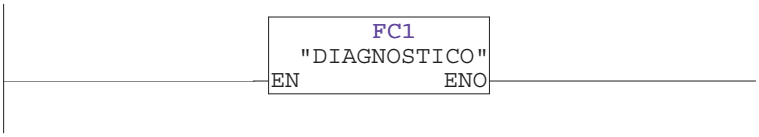
Name	Data Type	Address	Comment
TEMP		0.0	
OB1_EV_CLASS	Byte	0.0	Bits 0-3 = 1 (Coming event), Bits 4-7 = 1 (Event class 1)
OB1_SCAN_1	Byte	1.0	1 (Cold restart scan 1 of OB 1), 3 (Scan 2-n of OB 1)
OB1_PRIORITY	Byte	2.0	Priority of OB Execution
OB1_OB_NUMBR	Byte	3.0	1 (Organization block 1, OB1)
OB1_RESERVED_1	Byte	4.0	Reserved for system
OB1_RESERVED_2	Byte	5.0	Reserved for system
OB1_PREV_CYCLE	Int	6.0	Cycle time of previous OB1 scan (milliseconds)
OB1_MIN_CYCLE	Int	8.0	Minimum cycle time of OB1 (milliseconds)
OB1_MAX_CYCLE	Int	10.0	Maximum cycle time of OB1 (milliseconds)
OB1_DATE_TIME	Date_And_Time	12.0	Date and time OB1 started

Block: OB1 BLOCO DE FUNÇÃO "PRINCIPAL" (SCAN TIME)

```
ESTE BLOCO EXECUTA A CHAMADA DOS MODELOS DE DIAGNÓSTICO, COORDENAÇÃO E
TRATAMENTO DA SIF-01
=====================================================================
ESTUDO DE CASO: ESTAÇÃO DE COMPRESSÃO DE GÁS (ECOMP)
=====================================================================
AUTOR: REINALDO SQUILLANTE JÚNIOR
DATA: 30/08/2011
```

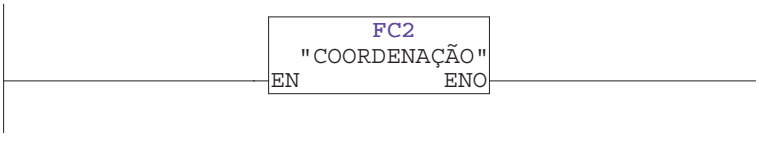
Network: 1

CHAMADA DO MODELO DE DIAGNÓSTICO DA SIF-01



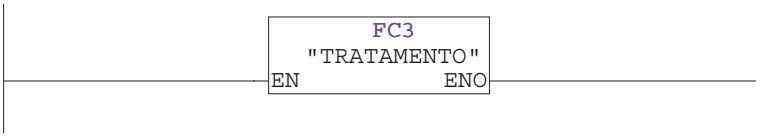
Network: 2

CHAMADA DO MODELO DE COORDENAÇÃO DA SIF-01



Network: 3

CHAMADA DO MODELO DE TRATAMENTO DA SIF-01



FC1 - <offline>

"DIAGNOSTICO"

Name: **Family:**
Author: **Version:** 0.1
Block version: 2
Time stamp Code: 8/30/2011 8:52:16 PMPM
Interface: 2/12/2011 12:35:28 PMPM
Lengths (block/logic/data): 00306 00128 00000

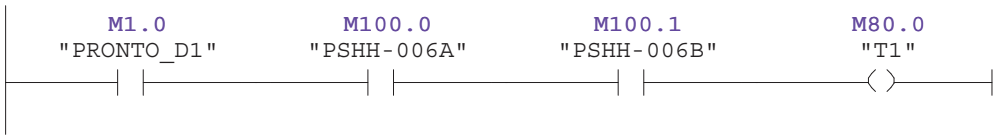
Name	Data Type	Address	Comment
IN		0.0	
OUT		0.0	
IN_OUT		0.0	
TEMP		0.0	
RETURN		0.0	
RET_VAL		0.0	

Block: FC1

```
==========================================================================
                  ALGORITMO DE DIAGNÓSTICO DA SIF-01
==========================================================================
ESTUDO DE CASO: ESTAÇÃO DE COMPRESSÃO DE GÁS (ECOMP)
==========================================================================
AUTOR: REINALDO SQUILLANTE JÚNIOR
DATA: 30/08/2011
```

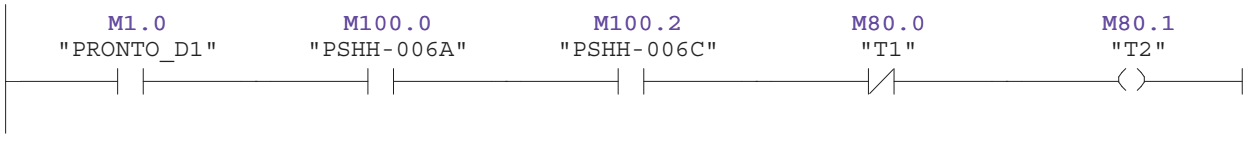
Network: 1

```
PRESSÃO MUITO ALTA NA DESCARGA DA ECOMP
=======================================
HABILITAÇÃO DA TRANSIÇÃO "T1"
```



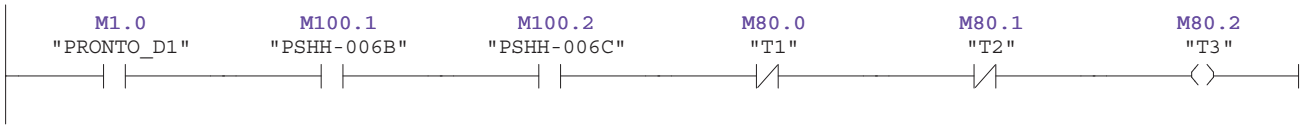
Network: 2

```
HABILITAÇÃO DA TRANSIÇÃO "T2"
```



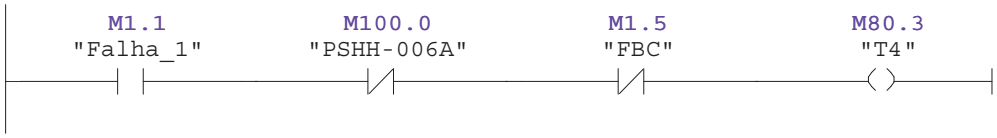
Network: 3

HABILITAÇÃO DA TRANSIÇÃO "T3"

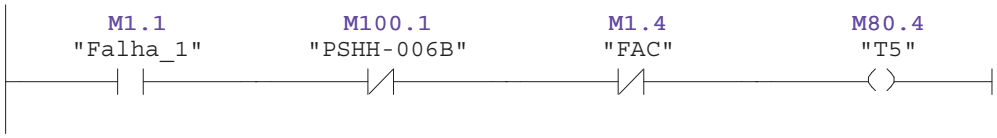


Network: 4

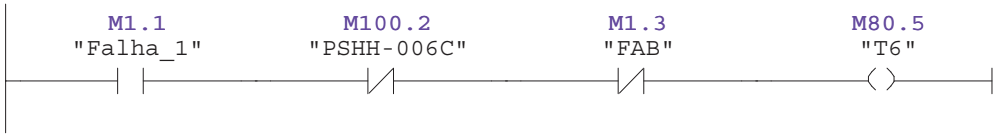
HABILITAÇÃO DA TRANSIÇÃO "T4"



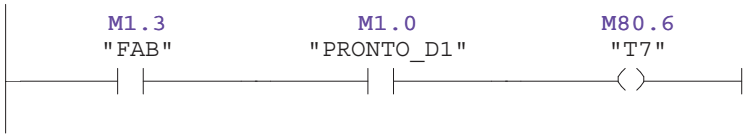
Network: 5



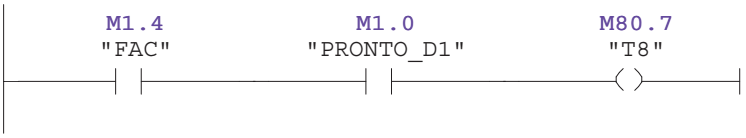
Network: 6



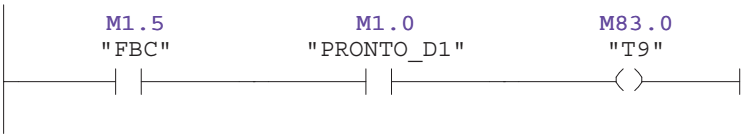
Network: 7



Network: 8

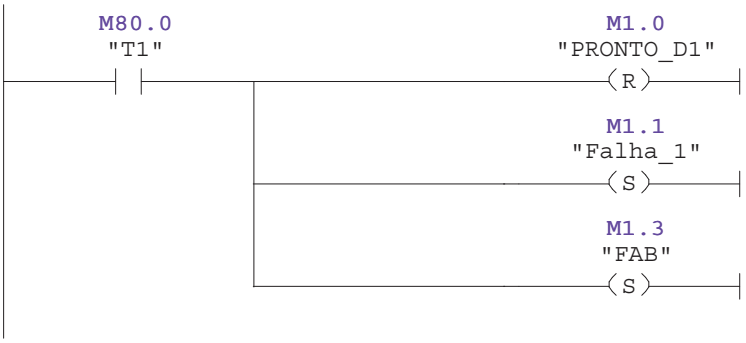


Network: 9



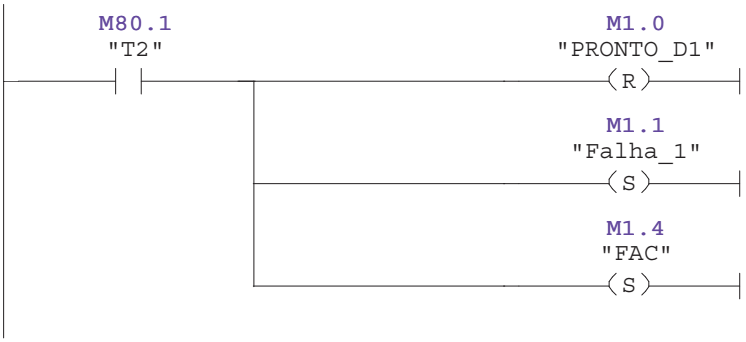
Network: 10

DISPARO DA TRANSIÇÃO "T1"



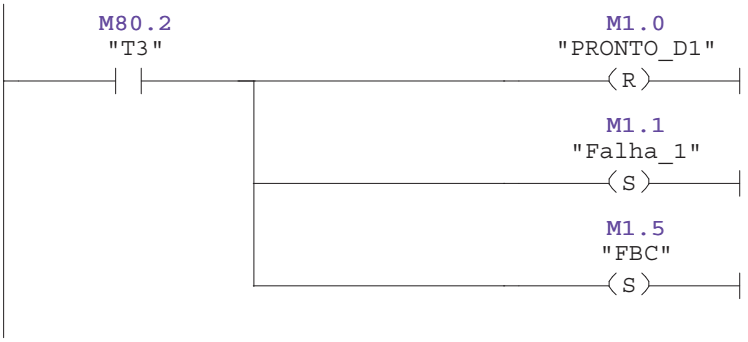
Network: 11

DISPARO DA TRANSIÇÃO "T2"



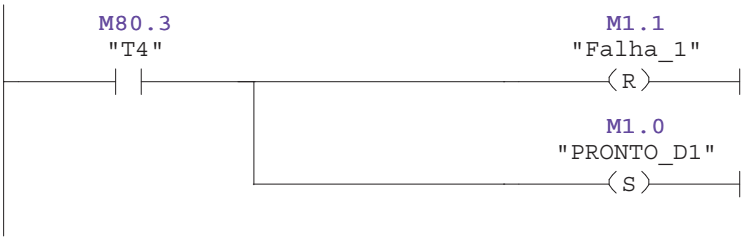
Network: 12

DISPARO DA TRANSIÇÃO "T3"



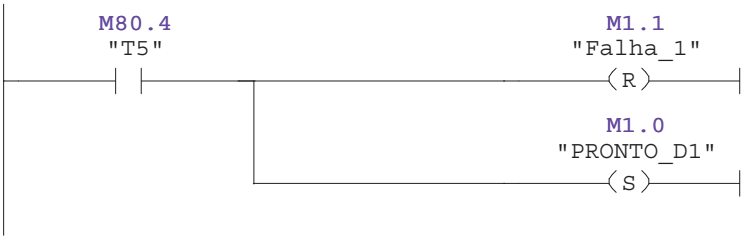
Network: 13

DISPARO DA TRANSIÇÃO "T4"



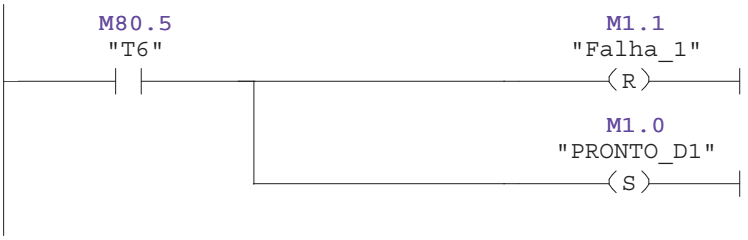
Network: 14

DISPARO DA TRANSIÇÃO "T4"



Network: 15

DISPARO DA TRANSIÇÃO "T4"



Network: 16

Network: 17

Network: 18

FC2 - <offline>

"COORDENAÇÃO"

Name: **Family:**
Author: **Version:** 0.1
Block version: 2
Time stamp Code: 8/30/2011 4:58:47 PMPM
Interface: 2/12/2011 12:35:45 PMPM
Lengths (block/logic/data): 00230 00068 00000

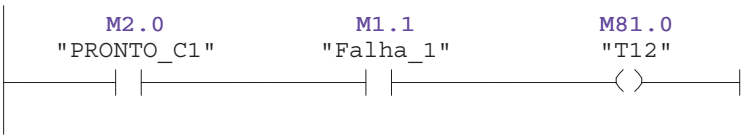
Name	Data Type	Address	Comment
IN		0.0	
OUT		0.0	
IN_OUT		0.0	
TEMP		0.0	
RETURN		0.0	
RET_VAL		0.0	

Block: FC2

```
==========================================================================
                  ALGORITMO DE COORDENAÇÃO DA SIF-01
==========================================================================
ESTUDO DE CASO: ESTAÇÃO DE COMPRESSÃO DE GÁS (ECOMP)
==========================================================================
AUTOR: REINALDO SQUILLANTE JÚNIOR
DATA: 30/08/2011
```

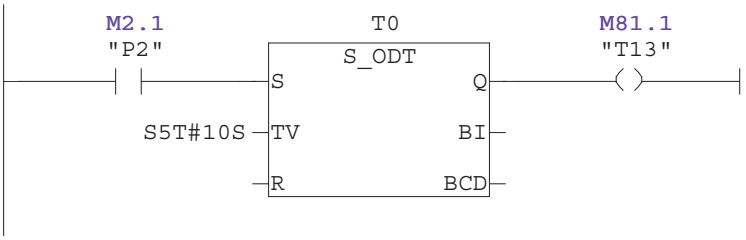
Network: 1

PRESSÃO MUITO ALTA NA DESCARGA DA ECOMP
HABILITAÇÃO DA TRANSIÇÃO "T12"



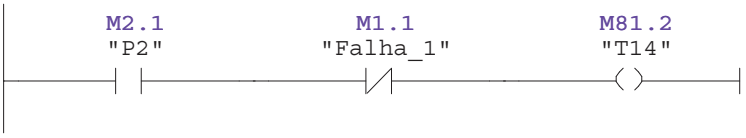
Network: 2

HABILITAÇÃO DA TRANSIÇÃO "T13"



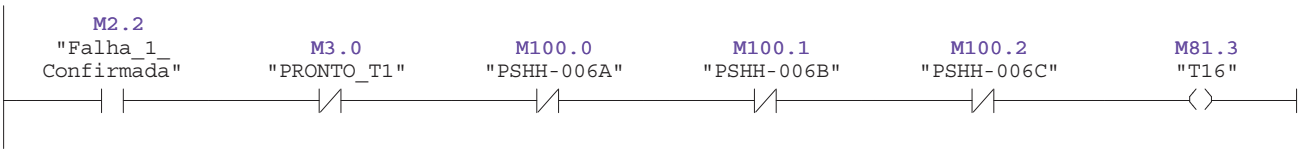
Network: 3

HABILITAÇÃO DA TRANSIÇÃO "T14"



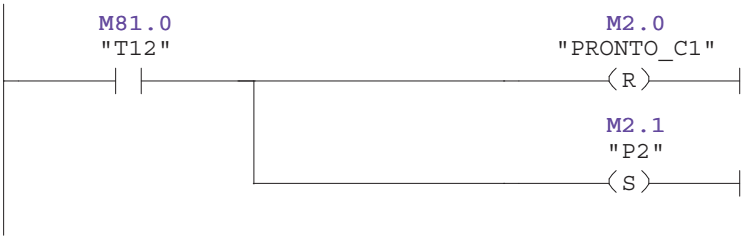
Network: 4

HABILITAÇÃO DA TRANSIÇÃO "T16"



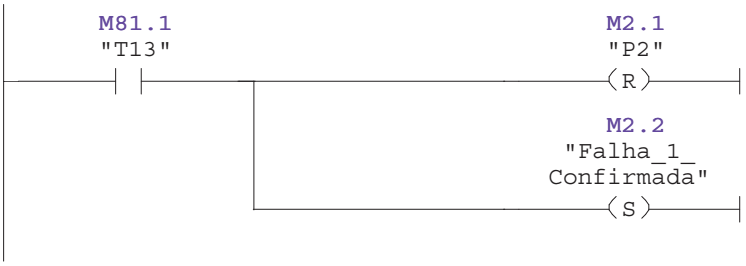
Network: 5

DISPARO DA TRANSIÇÃO "T12"



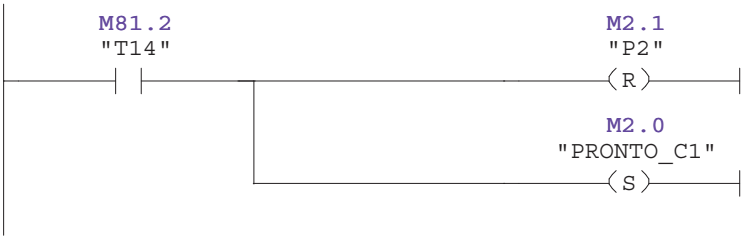
Network: 6

DISPARO DA TRANSIÇÃO "T13"



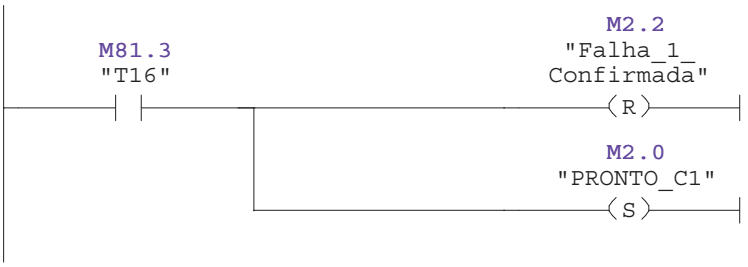
Network: 7

DISPARO DA TRANSIÇÃO "T14"



Network: 8

DISPARO DA TRANSIÇÃO "T16"



FC3 - <offline>

"TRATAMENTO"

Name: **Family:**
Author: **Version:** 0.1
Block version: 2
Time stamp Code: 8/30/2011 12:11:01 PMPM
Interface: 2/12/2011 12:35:57 PMPM
Lengths (block/logic/data): 00200 00086 00000

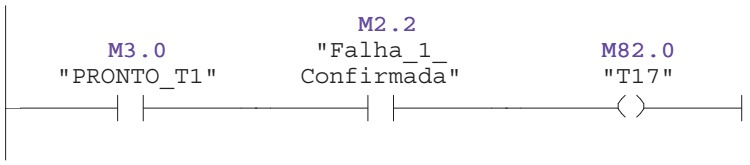
Name	Data Type	Address	Comment
IN		0.0	
OUT		0.0	
IN_OUT		0.0	
TEMP		0.0	
RETURN		0.0	
RET_VAL		0.0	

Block: FC3

```
=========================================================================
                  ALGORITMO DE TRATAMENTO DA SIF-01
=========================================================================
ESTUDO DE CASO: ESTAÇÃO DE COMPRESSÃO DE GÁS (ECOMP)
=========================================================================
AUTOR: REINALDO SQUILLANTE JÚNIOR
DATA: 30/08/2011
```

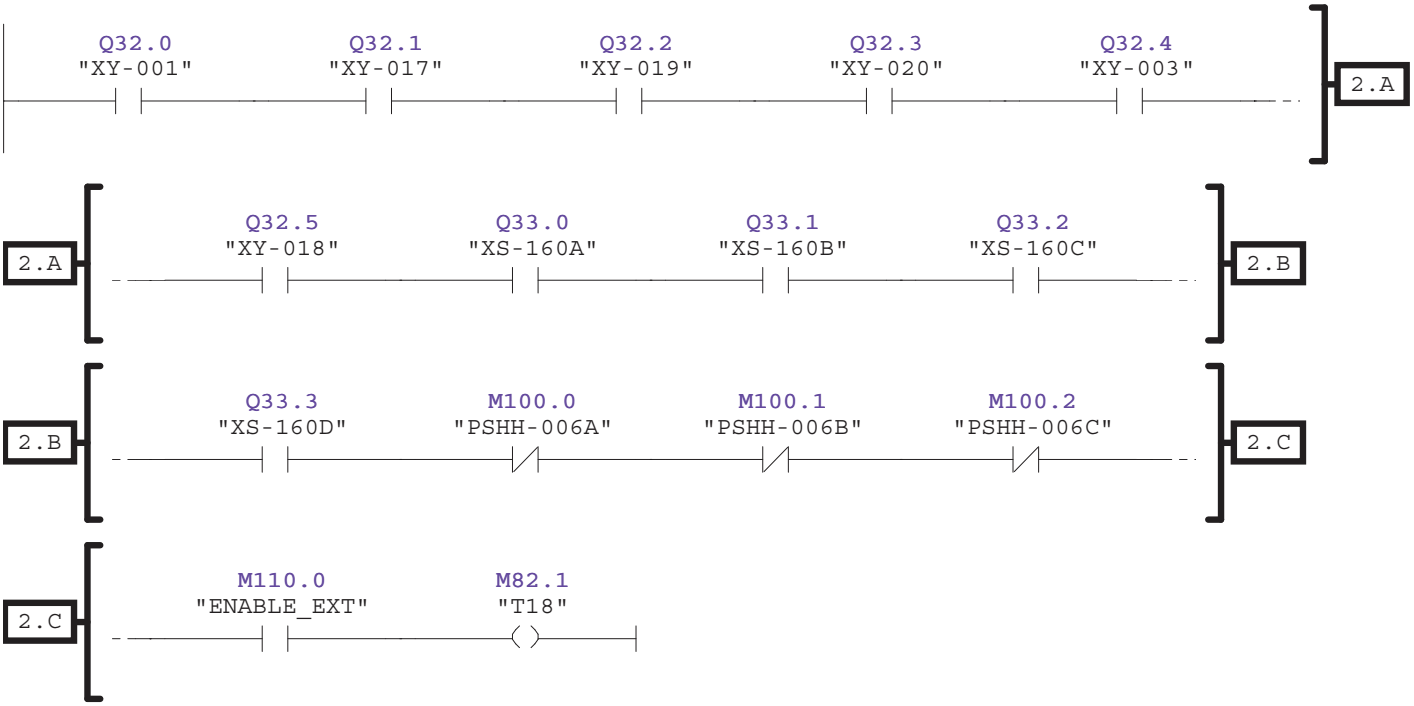
Network: 1

```
PRESSÃO MUITO ALTA NA DESCARGA DA ECOMP
=======================================
HABILITAÇÃO DA TRANSIÇÃO "T17"
```



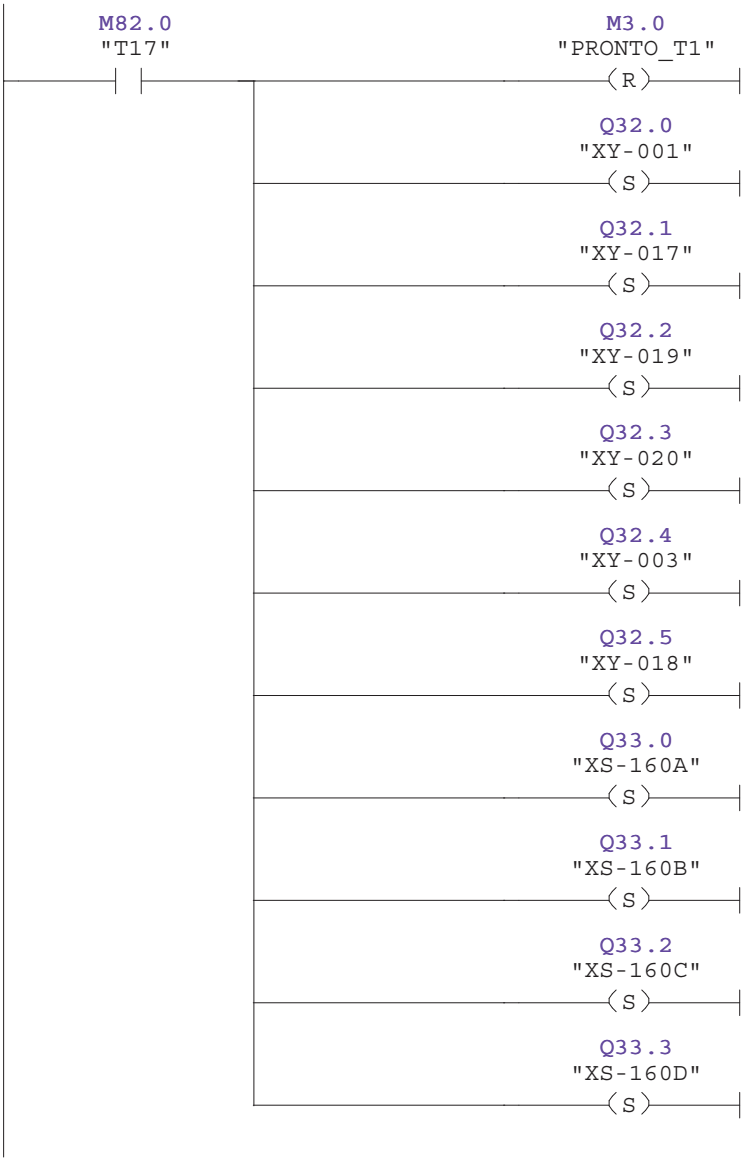
Network: 2

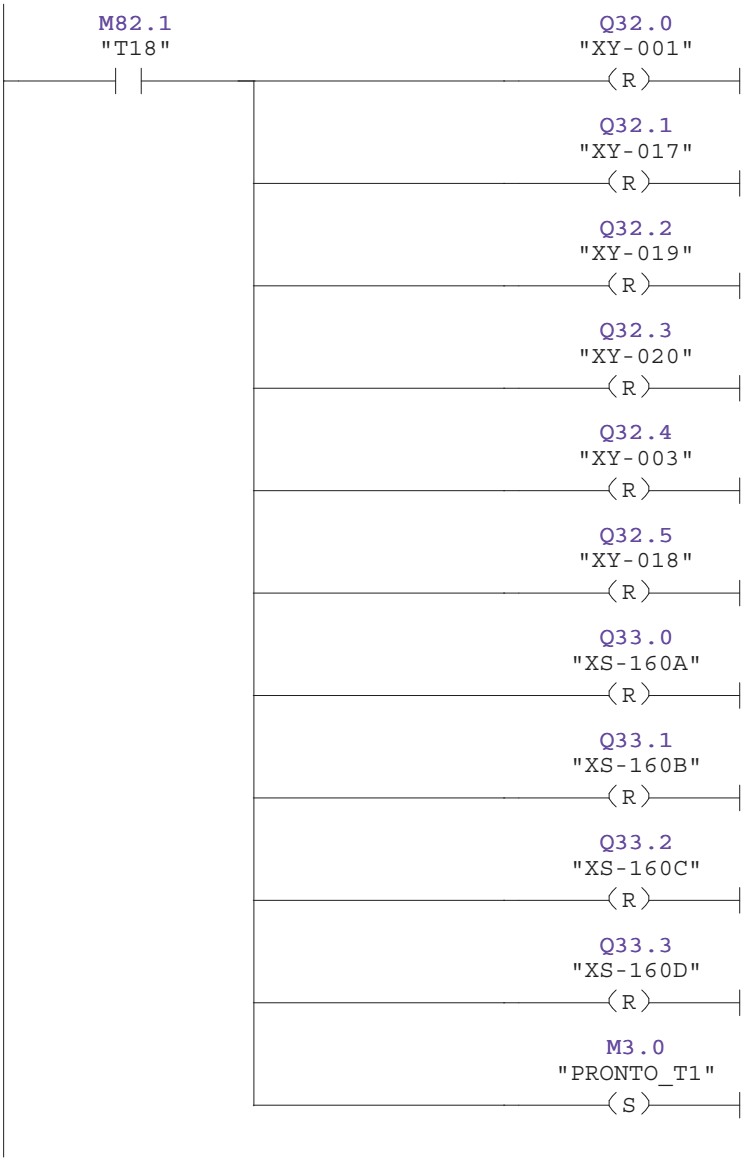
HABILITAÇÃO DA TRANSIÇÃO "T18"



Network: 3

DISPARO DA TRANSIÇÃO "T17"



Network: 4

DISPARO DA TRANSIÇÃO "T18"