EMÍLIA VILLANI

**MODELAGEM E ANÁLISE DE SISTEMAS SUPERVISÓRIOS
HÍBRIDOS**

Tese apresentada à Escola Politécnica
da Universidade de São Paulo para a
obtenção do título de Doutor em
Engenharia.

São Paulo

2004

EMÍLIA VILLANI

**MODELAGEM E ANÁLISE DE SISTEMAS SUPERVISÓRIOS
HÍBRIDOS**

Tese apresentada à Escola Politécnica
da Universidade de São Paulo para a
obtenção do título de Doutor em
Engenharia.

Área de Concentração:
Engenharia de Controle e Automação
Mecânica

Orientador:
Prof. Dr. Paulo Eigi Miyagi

São Paulo

2004

FICHA CATALOGRÁFICA

Villani, Emília

**Modelagem e análise de sistemas supervisórios híbridos,
São Paulo / Emília Villani. – São Paulo, 2004.
339 p.**

**Tese (Doutorado) - Escola Politécnica da Universidade de
São Paulo. Departamento de Engenharia Mecatrônica e de
Sistemas Mecânicos.**

**1. Sistemas híbridos (Análise; Modelagem) 2. Sistemas de
controle I. Universidade de São Paulo. Escola Politécnica.
Departamento de Engenharia Mecatrônica e de Sistemas
Mecânicos II. t.**

Ao meu marido Marco e a toda minha família.

AGRADECIMENTOS

Ao meu orientador Prof. Dr. Paulo Eigi Miyagi pela constante orientação, permanente disponibilidade e grande incentivo para o desenvolvimento deste trabalho.

Ao Prof. Dr. Robert Valette pelas inúmeras e valiosas contribuições, pelo consistente direcionamento e pelo incessante acompanhamento deste trabalho, não apenas durante meu estágio no *Laboratoire d'Analyse et d'Architecture de Systèmes* – LAAS (Toulouse, França), mas durante todo o seu desenvolvimento.

Aos professores e alunos do Laboratório de Automação de Sistemas – LAS pelas sugestões e contribuições – em especial ao Fabrício, à Gladys, ao Luis Alberto, ao Roger e ao David, pelas muitas discussões elucidativas e, sobretudo, pelo apoio e pela amizade.

Aos professores e alunos do grupo *Organisation et Conduite de Systèmes Discret* – OCSD (LAAS) que deram suporte para a realização do meu estágio no LAAS – em particular à colaboração do Prof. Dr. Jean-Claude Pascal.

Ao meus amigos e colegas de pós-graduação, particularmente àqueles da MC-01, pela companhia e amizade ao longo destes anos.

Aos brasileiros, franceses, mexicanos, italianos e outros tantos que me receberam, auxiliaram e fizeram da minha estadia em Toulouse uma grande experiência – em especial à Cristiane, à Cristiani, à Delmira, ao Eduardo, ao François, à Joana, à Karyn, à Laura, ao Magnos, ao Marcos, ao Paulo e à Roberta, que foram minha família em Toulouse.

À Escola Politecnica da USP, ao Departamento de Engenharia Mecatrônica e de Sistemas Mecânicos e ao LAAS, que institucionalmente viabilizaram este trabalho.

Ao Hospital das Clínicas da Faculdade de Medicina da USP, à Dassault Aviation e à Usina Cruz Alta do Grupo Açúcar Guarani por permitirem acesso às informações que subsidiaram a realização dos estudos de caso deste trabalho – em especial ao Sr. Tadashi Ueoka por proporcionar o contato com a Usina Cruz Alta.

À Fundação de Amparo a Pesquisa do Estado de São Paulo – FAPESP, à Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – CAPES, e ao Conselho Nacional de Desenvolvimento Científico e Tecnológico– CNPq, pelo apoio financeiro.

Ao Prof. Reinaldo e ao Marco A. Poli pelo esforço e tempo gasto para viabilizar a transmissão da defesa desta tese, por video-conferência, para o LAAS.

A todos aqueles que, mesmo não tem sido aqui citados nominalmente, colaboraram, direta ou indiretamente, de maneira não menos importante, na produção deste trabalho.

RESUMO

Sistemas Supervisórios Híbridos podem ser definidos como sistemas de controle cujos estados são representados por variáveis discretas e contínuas, e cuja dinâmica é determinada em função do tempo e da ocorrência de eventos discretos. O desenvolvimento desta classe de Sistemas Supervisórios pode ser dividido em duas fases. A 1ª Fase consiste na elaboração de um modelo protótipo para o Sistema Supervisório, que é descrito usando um formalismo, e que é validado com base nas especificações do problema. Na 2ª Fase, este modelo, já validado, é convertido na linguagem de programação do Sistema Supervisório propriamente dito. Esta tese concentra-se na 1ª Fase, para qual abordam-se três questões principais: (1) a escolha do formalismo de modelagem; (2) como construir o modelo do Sistema Supervisório Híbrido usando este formalismo; e (3) como validar o Sistema Supervisório Híbrido usando o modelo construído. Para questão (1), introduz-se um novo formalismo de modelagem baseado na aplicação dos conceitos de Orientação a Objetos (OO) às redes Predicado Transição Diferenciais (redes PTD). Este novo formalismo é chamado de redes PTD-OO. No que se refere a questão (2), é proposto um procedimento para obtenção do modelo do Sistema Supervisório em redes PTD-OO usando os diagramas da UML ('Unified Modeling Language'). Finalmente, para a questão (3), o problema de validação é abordado através da definição de um conjunto de propriedades que o modelo em redes PTD-OO deve respeitar afim de que sejam garantidos os requisitos do Sistema Supervisório. Estas propriedades são, então, verificadas através de um procedimento proposto para análise de redes PTD-OO.

ABSTRACT

Hybrid Supervisory Systems can be described as control systems with states that are represented by both discrete and continuous variables. Their dynamics are function of time and depend also on the occurrence of discrete events. The development of Hybrid Supervisory Systems can be divided in two phases. In the 1st Phase, a prototype-model for the Supervisory System is described using a specific formalism and is validated based on the system requirements. In the 2nd Phase, this validated model is converted to the programming language of the Supervisory System. This thesis is focused on the 1st Phase of Hybrid Supervisory System development. It approaches three main issues: (1) the choice of the modelling formalism; (2) how to build the Hybrid Supervisory System model using this formalism; and (3) how to validate the Hybrid Supervisory System using this model. For issue (1), a new modelling formalism is introduced based on Differential Predicate Transition nets (DPT nets) and object-oriented (OO) paradigm. This new formalism is called DPT-OO net. Then, for the issue (2), a modelling procedure that assists the building of the DPT-OO net model using Unified Modelling Language (UML) diagrams is proposed. Finally, for the issue (3), the validation problem is approached by defining a set of properties of the DPT-OO net model that assures the Supervisory System requirements. These properties are then formally verified using a proposed analysis procedure.

SUMÁRIO

Lista de Tabelas

Lista de Figuras

Lista de Símbolos

1	Introdução.....	1
1.1	<i>Conceitos Básicos.....</i>	<i>1</i>
1.1.1	Sistemas Híbridos	1
1.1.2	Sistemas Produtivos e Sistemas de Controle	4
1.1.3	Hierarquia de Controle e Sistemas Supervisórios.....	7
1.2	<i>Objetivo, Motivações e Contribuições.....</i>	<i>10</i>
2	Modelagem de Sistemas Híbridos.....	13
2.1.	<i>Escolha do Formalismo de Base</i>	<i>13</i>
2.2.	<i>Das redes de Petri às redes de Predicado-Transição Diferenciais.....</i>	<i>15</i>
2.3.	<i>Redes de Petri e Orientação a Objetos.....</i>	<i>22</i>
2.4.	<i>Aplicação dos conceitos de orientação a objetos para as redes PTD.....</i>	<i>24</i>
2.4.1.	Modelagem de Classes e Objetos	24
2.4.2.	Comunicação entre as sub-redes	33
2.4.3.	Interface com Elementos Externos	40
2.4.4.	Desdobramento da rede PTD-OO.....	41
2.5.	<i>Observações</i>	<i>46</i>
3	Desenvolvimento de Sistemas Supervisórios Híbridos.....	48
3.1.	<i>A Modelagem em Redes PTD-OO e os Diagramas da UML</i>	<i>51</i>
3.1.1.	Atividade 1 – Modelagem dos Fluxo de Materiais	53
3.1.2.	Atividade 2 – Definição dos Casos de Uso.....	54
3.1.3.	Atividade 3 – Construção dos Diagramas de Atividades.....	55
3.1.4.	Atividade 4 – Definição de Classes e Objetos	55
3.1.5.	Atividade 5 – Construção dos Diagramas de Seqüência e Diagramas de Colaboração	59
3.1.6.	Atividade 6 – Modelagem das Classes em Redes PTD-OO e Construção dos Diagramas de Classes	63
3.1.7.	Atividade 7 – Verificação dos Modelos.....	68
3.2.	<i>Relações entre classes para redes PTD-OO</i>	<i>72</i>
3.2.1.	Decomposição/Composição.....	73
3.2.2.	Generalização/Especialização.....	77
3.3.	<i>(Sistema de Controle Local + Planta) x Planta Controlada.....</i>	<i>78</i>
3.4.	<i>Observações</i>	<i>80</i>
4	Análise de Sistemas Híbridos	84

4.1.	<i>Verificação de Propriedades em Sistemas Híbridos</i>	85
4.2.	<i>Redes de Petri e Lógica Linear</i>	87
4.2.1.	Lógica Linear x Lógica Clássica.....	87
4.2.2.	Alcançabilidade em Redes de Petri x Prova de Seqüentes em Lógica Linear	90
4.2.3.	Lógica linear para a busca de cenários em redes de Petri	93
4.2.4.	A lógica linear e a Orientação a Objeto	96
4.3.	<i>O Procedimento Proposto para Análise das redes PTD-OO</i>	99
4.3.1.	Principais características	99
4.3.2.	Visão geral do procedimento de análise	101
4.3.3.	Propriedade de Alcançabilidade	105
4.3.4.	Propriedades de Segurança	122
4.4.	<i>Observações</i>	130
5	Estudo de Caso 1 – Sistema de Ar Condicionado.....	134
5.1.	<i>Descrição do Sistema</i>	135
5.1.1.	Objeto de Controle.....	135
5.1.2.	Requisitos do Sistema Supervisório.....	136
5.2.	<i>Modelagem do Sistema Supervisório e seu Objeto de Controle.....</i>	137
5.2.1.	Atividade 1 – Modelagem do Fluxo de Materiais.....	137
5.2.2.	Atividade 2 – Definição dos Casos de Uso.....	138
5.2.3.	Atividade 3 – Construção dos Diagramas de Atividades.....	138
5.2.4.	Atividade 4 – Definição das Classes e Objetos	139
5.2.5.	Atividade 5 – Construção dos Diagramas de Seqüência ou Colaboração	141
5.2.6.	Atividade 6 – Modelagem das Classes em redes PTD-OO	143
5.2.7.	Atividade 7 – Verificação dos Modelos.....	154
5.3.	<i>Análise dos Modelos em redes PTD-OO</i>	155
5.3.1.	Propriedade 1	156
5.3.2.	Propriedade 2	161
5.4.	<i>Observações</i>	167
6	Estudo de Caso 2 – Sistema de Aterrissagem	169
6.1.	<i>Descrição do Sistema</i>	170
6.1.1.	Objeto de Controle.....	170
6.1.2.	Requisitos do Sistema Supervisório.....	172
6.2.	<i>Modelagem do Sistema Supervisório e seu Objeto de Controle.....</i>	175
6.2.1.	Exemplos de Classes e Objetos.....	175
6.3.	<i>Análise dos Modelos em redes PTD-OO</i>	181
6.3.1.	Propriedade 1	181
6.4.	<i>Observações</i>	199
7	Estudo de Caso 3 – Usina de Cana de Açúcar	202
7.1.	<i>Descrição do Sistema</i>	203
7.1.1.	Objeto de Controle.....	203

7.1.2.	Requisitos do Sistema Supervisório.....	204
7.2.	<i>Modelagem do Sistema Supervisório e seu Objeto de Controle.....</i>	206
7.2.1.	Atividade 1 – Modelagem do Fluxo de Materiais.....	206
7.2.2.	Exemplos de Classes e Objetos.....	219
7.3.	<i>Análise dos Modelos em redes PTD-OO</i>	224
7.3.1.	Propriedade 1	224
7.4.	<i>Observações</i>	233
8	Conclusão	235
8.1.	<i>Principais Contribuições.....</i>	235
8.2.	<i>Trabalhos Futuros</i>	237
Anexo A -Dados complementares do Estudo de Caso 2 – Sistema de Aterrissagem		239
A.1.	<i>Modelagem do Sistema Supervisório e seu Objeto de Controle.....</i>	239
A.1.1.	Atividade 1 – Modelagem do Fluxo de Materiais.....	239
A.1.2.	Atividade 2 – Definição dos Casos de Uso.....	239
A.1.3.	Atividade 3 – Construção dos Diagramas de Atividades.....	240
A.1.4.	Atividade 4 – Definição das Classes e Objetos	242
A.1.5.	Atividade 5 – Construção dos Diagramas de Seqüência ou Colaboração	243
A.1.6.	Atividade 6 – Modelagem das Classes em redes PTD-OO	244
A.1.7.	Atividade 7 – Verificação dos Modelos.....	253
A.2.	<i>Observações</i>	256
Anexo B - Dados complementares do Estudo de Caso 3 – Usina de Cana de Açúcar .		261
B.1.	<i>Modelagem do Sistema Supervisório e seu Objeto de Controle.....</i>	261
B.1.1.	Atividade 2 – Definição dos Casos de Uso.....	261
B.1.2.	Atividade 3 – Construção dos Diagramas de Atividades.....	261
B.1.3.	Atividade 4 – Definição das Classes e Objetos	263
B.1.4.	Atividade 5 – Construção dos Diagramas de Seqüência ou Colaboração	268
B.1.5.	Atividade 6 – Modelagem das Classes em redes PTD-OO	268
B.1.6.	<i>Atividade 7 – Verificação dos Modelos</i>	320
B.2.	Análise dos Modelos em redes PTD-OO	321
B.2.1.	Propriedade 2	323
B.3.	<i>Observações</i>	334
Referencias Bibliográficas.....		335

LISTA DE FIGURAS

Fig. 1.1. Comportamento de variáveis em sistemas de diferentes naturezas.	2
Fig. 1.2. Exemplo de descontinuidade na planta.....	3
Fig. 1.3. Sistemas de Informação e Sistemas Produtivos.....	5
Fig. 1.4. Interações em um Sistema Produtivo.	6
Fig. 1.5. Fases do desenvolvimento de um Sistema de Controle.	7
Fig. 1.6. Níveis de controle.	8
Fig. 1.7. Sistema Supervisório como Sistema de Controle.	10
Fig. 2.1. Exemplo de rede de Petri, com correspondente representação matricial.....	16
Fig. 2.2. Exemplo de disparo em uma rede Predicado-Transição.....	19
Fig. 2.3. Exemplo de disparo de transição em uma rede PTD.	20
Fig. 2.4. Exemplo compartilhamento de variável em uma rede PTD.	21
Fig. 2.5. Exemplo a ser modelado em redes PTD-OO.....	25
Fig. 2.6. Modelo da <i>Classe 1 - Válvula</i>	26
Fig. 2.7. Modelo da <i>Classe 2 - Tanque</i>	26
Fig. 2.8. Modelo da <i>Classe 3 - Controlador</i>	27
Fig. 2.9. Possível marcação para os objetos do sistema da Fig. 2.5.....	28
Fig. 2.10. Marcações alcançáveis pelos objetos das classes do exemplo da Fig. 2.5.	29
Fig. 2.11. Vetores X_p para as classes do sistema da Fig. 2.5.	29
Fig. 2.12. Exemplo de vetores X_p inconsistentes.	30
Fig. 2.13. Tipos de variáveis para as classes do sistema da Fig. 2.5.....	30
Fig. 2.14. Tipos de variáveis para as classes do sistema da Fig. 2.5.....	31
Fig. 2.15. Associações das variáveis externas das classes do sistema da Fig. 2.5.	32
Fig. 2.16. Compartilhamento de variáveis para a marcação definida em Fig. 2.9.	32
Fig. 2.17. Interface fornecida pelas classes do sistema da Fig. 2.5 às demais classes.	34
Fig. 2.18. Interface utilizada pelas classes do sistema da Fig. 2.5.	35
Fig. 2.19. Modelo da <i>Classe 1 - Válvula</i>	35
Fig. 2.20. Modelo da <i>Classe 2 - Tanque</i>	36
Fig. 2.21. Modelo da <i>Classe 3 - Controlador</i>	36
Fig. 2.22. Exemplo de chamada de método.	37
Fig. 2.23. Rede da Fig. 2.22 após a fusão e o disparo das transições $t_{2,3}$ e $t_{1,1}$	38
Fig. 2.24. Exemplo de passagem de valores através da chamada de métodos.....	39
Fig. 2.25. Rede da Fig. 2.24 após o disparo das transições $t_{1,1}$ e $t_{1,2}$	40
Fig. 2.26. Interface fornecida pelas classes do sistema da Fig. 2.5 à elementos externos.	41
Fig. 2.27. Etapa 1 do desdobramento da rede para os objetos $O_{1,1}$ e $O_{2,1}$ do sistema da Fig. 2.5.....	42
Fig. 2.28. Etapa 1 do desdobramento da rede para os objetos $O_{1,2}$ e $O_{1,3}$ do sistema da Fig. 2.5.....	43
Fig. 2.29. Etapa 2 do desdobramento da rede do sistema da Fig. 2.5.	44
Fig. 2.30. Etapa 3 do desdobramento da rede para os objetos $O_{1,1}$ e $O_{2,1}$ do sistema da Fig. 2.5.....	44

Fig. 2.31. Etapa 3 do desdobramento da rede para o objetos $O_{1,2}$ do sistema da Fig. 2.5.....	45
Fig. 2.32. Etapa 4 do desdobramento da rede do sistema da Fig. 2.5.	46
Fig. 3.1. Etapas abordadas no decorrer de um ciclo (Jacobson; Booch; Rumbaugh, 1999). .	49
Fig. 3.2. A modelagem em redes PTD-OO e as etapas da Engenharia de Software.....	50
Fig. 3.3. Atividades para modelagem do Sistema Supervisório e seu Objeto de Controle....	52
Fig. 3.4. Exemplo de sistema a ser supervisionado.....	53
Fig. 3.5. PFS para o exemplo da Fig. 3.4.....	54
Fig. 3.6. Diagrama de Caso de Uso para o exemplo da Fig. 3.4.	55
Fig. 3.7. Diagrama de Atividades para o Caso de Uso ‘Produzir P1’.....	56
Fig. 3.8. Diagrama de Seqüência para o Caso de Uso ‘Produzir P1’.....	60
Fig. 3.9. Diagrama de Colaboração para o Caso de Uso ‘Produzir P1’.....	61
Fig. 3.10. Classes para o exemplo da Fig. 3.4.....	61
Fig. 3.11. Detalhamento do Diagrama de Atividades da Fig. 3.7.	62
Fig. 3.12. Modelo em rede PTD-OO da classe C_1 – <i>Tanque</i>	63
Fig. 3.13. Modelo em rede PTD-OO da classe C_2 – <i>Válvula A</i>	64
Fig. 3.14. Modelo em rede PTD-OO da classe C_3 – <i>Válvula B</i>	64
Fig. 3.15. Modelo em rede PTD-OO da classe C_4 – <i>Misturador</i>	64
Fig. 3.16. Modelo em rede PTD-OO da classe C_5 – <i>Controlador Misturador</i>	65
Fig. 3.17. Modelo em rede PTD-OO da classe C_6 – <i>Interface CM</i>	65
Fig. 3.18. Modelo em rede PTD-OO da classe C_7 – <i>Interface Válvula A</i>	66
Fig. 3.19. Modelo em rede PTD-OO da classe C_8 – <i>Receita</i>	66
Fig. 3.20. Modelo em rede PTD-OO da classe C_9 – <i>Ordem de Produção</i>	66
Fig. 3.21. Correspondência entre o Diagrama de Seqüência e o modelo em redes PTD-OO.	69
Fig. 3.22. Conversão do Diagrama de Atividades para redes de Petri – atividades discretas.	69
Fig. 3.23. Conversão do Diagrama de Atividades para redes de Petri – atividades contínuas.	70
Fig. 3.24. Conversão do Diagrama de Atividades para redes de Petri – barras de sincronização.	70
Fig. 3.25. Conversão do Diagrama de Atividades para redes de Petri – losango de decisão.	71
Fig. 3.26. Conversão do Diagrama de Atividades para redes de Petri – simplificação (tipo 1).	71
Fig. 3.27. Conversão do Diagrama de Atividades para redes de Petri – simplificação (tipo 2).	71
Fig. 3.28. Conversão do Diagrama de Atividades para redes de Petri – simplificação (tipo 3).	72
Fig. 3.29. Conversão em redes de Petri do Diagrama de Atividades da Fig. 3.11.	73
Fig. 3.30. Diagrama de classes para a composição da classe C_{10} – <i>Estação de Corante</i>	74
Fig. 3.31. Modelo em rede PTD-OO da classe C_{10} – <i>Estação de Corante</i>	74
Fig. 3.32. Simplificação do modelo da classe C_{10} – <i>Estação de Corante</i>	76
Fig. 3.33. Diagrama de classes para a especialização da classe C_{11} – <i>Válvula</i>	78
Fig. 3.34. Modelo da classe C_{11} , resultante da generalização das classes C_2 e C_3	78
Fig. 3.35. Modelo em rede PTD-OO da classe C_{12} – <i>Válvula A (Modelo 2)</i>	80
Fig. 4.1. Representação gráfica de uma regra.	88
Fig. 4.2. Regras da lógica linear.....	89

Fig. 4.3. Exemplo de rede de Petri e respectiva definição das transições usando lógica linear (Raciocínio para frente).....	91
Fig. 4.4. Exemplo de prova usando o raciocínio para frente.....	92
Fig. 4.5. Definição das transições usando lógica linear e o raciocínio para trás.....	92
Fig. 4.6. Exemplo de prova usando o raciocínio para trás.	93
Fig. 4.7. Exemplo.....	95
Fig. 4.8. Busca de cenários - exemplo de raciocínio para frente.	95
Fig. 4.9. Busca de cenários - exemplo de raciocínio para trás.	96
Fig. 4.10. O enfoque local da lógica linear.	97
Fig. 4.11. Análise através da construção do grafo de marcações alcançáveis.	98
Fig. 4.12. Rede PTD-OO dos objetos $O_{1,3}$ e $O_{1,4}$	99
Fig. 4.13. Ordem parcial de disparos para os objetos $O_{1,3}$ e $O_{1,4}$	99
Fig. 4.14. Decomposição da análise de um modelo.....	100
Fig. 4.15. Etapas da Validação de um Sistema Supervisório Híbrido.	102
Fig. 4.16. Sistema de embalagem e respectivo modelo em redes PTD-OO.	104
Fig. 4.17. Diagrama de Colaboração Estático para o exemplo da Fig. 4.16.	108
Fig. 4.18. Busca de cenários no 1o objeto para propriedades de alcançabilidade.	109
Fig. 4.19. Ordem de disparos dos Cenários 1 a 4 para $O_{1,1}$ - Propriedade 1.	113
Fig. 4.20. Busca de cenários nos demais objetos para propriedades de alcançabilidade.	117
Fig. 4.21. Ordem de disparos do Cenário 4 para $O_{1,2}$ - Propriedade 1.	119
Fig. 4.22. Ordem parcial de disparos – Propriedade 1, Cenário 4.	121
Fig. 4.23. Exemplos dos Casos 1 a 4, onde o disparo de $t_{i,y,ow}$ é impossível.....	124
Fig. 5.1. Sistema de Ar Condicionado A.	136
Fig. 5.2. Sistema de Ar Condicionado B.....	136
Fig. 5.3. PFS para o Sistema de Ar Condicionado A.....	137
Fig. 5.4. PFS para o Sistema de Ar Condicionado B.	137
Fig. 5.5. Diagrama de Casos de Uso para o Sistema de Ar Condicionado A.	138
Fig. 5.6. Diagrama de Atividades do Caso de Uso ‘Iniciar procedimento alarme’ - Sistema de Ar Condicionado A.	139
Fig. 5.7. Diagrama de Seqüência do Caso de Uso ‘Iniciar procedimento alarme’ - Sistema de Ar Condicionado A.	141
Fig. 5.8. Métodos e atributos das classes do Sistema de Ar Condicionado A.	142
Fig. 5.9. Detalhamento do Diagrama de Atividades da Fig. 5.6 - Sistema de Ar Condicionado A.....	142
Fig. 5.10. Diagrama de Classes dos Sistemas de Ar Condicionado A e B.	143
Fig. 5.11. Modelo em redes PTD-OO da classe C_1 – Ventilador.....	144
Fig. 5.12. Modelo em redes PTD-OO da classe C_2 – Caixa de Mistura.	144
Fig. 5.13. Modelo em redes PTD-OO da classe C_3 – Serpentina Genérica.....	145
Fig. 5.14. Modelo em redes PTD-OO da classe C_4 – Serpentina B.	145
Fig. 5.15. Modelo em redes PTD-OO da classe C_5 – Serpentina A.	146
Fig. 5.16. Modelo em redes PTD-OO da classe C_6 – Controle Genérico.....	146
Fig. 5.17. Modelo em redes PTD-OO da classe C_7 – Controle On/Off.	147
Fig. 5.18. Modelo em redes PTD-OO da classe C_8 – Controle PID.....	147

Fig. 5.19. Modelo em redes PTD-OO da classe C_9 – <i>Ambiente</i>	148
Fig. 5.20. Ciclo fechado de compartilhamento de variáveis entre as classes C_2 , C_4 , C_8 e C_9	148
Fig. 5.21. Modelo em redes PTD-OO da classe C_{11} – <i>Regulagem T_{sp}</i>	149
Fig. 5.22. Modelo em redes PTD-OO da classe C_{12} – <i>Interface Controlador</i>	149
Fig. 5.23. Modelo em redes PTD-OO da classe C_{13} – <i>Interface Genérica Equipamento</i>	150
Fig. 5.24. Modelo em redes PTD-OO da classe C_{14} – <i>Interface Ventilador</i>	150
Fig. 5.25. Modelo em redes PTD-OO da classe C_{15} – <i>Interface Caixa de Mistura</i>	151
Fig. 5.26. Modelo em redes PTD-OO da classe C_{16} – <i>Interface Gerenciamento do Edifício B</i>	151
Fig. 5.27. Modelo em redes PTD-OO da classe C_{17} – <i>Interface Gerenciamento Edifício A</i>	152
Fig. 5.28. Modelo em redes PTD-OO da classe C_{18} – <i>Interface Usuário Genérica</i>	152
Fig. 5.29. Modelo em redes PTD-OO da classe C_{19} – <i>Interface Usuário B</i>	153
Fig. 5.30. Modelo em redes PTD-OO da classe C_{20} – <i>Interface Usuário B</i>	153
Fig. 5.31. Relação entre o Diagrama de Seqüência da Fig. 5.7 e as transições das classes - Sistema de Ar Condicionado A.....	154
Fig. 5.32. Conversão para redes de Petri do Diagrama de Atividades da Fig. 5.9.....	155
Fig. 5.33. Interações relevantes para Propriedade 1.....	156
Fig. 5.34. Ordem parcial de disparos – Propriedade 1.....	160
Fig. 5.35. Interações relevantes para Propriedade 1.....	162
Fig. 5.36. Faixa de variação de T_{ar_out}	165
Fig. 5.37. Faixa de variação de T_{amb}	166
Fig. 5.38. Ordem parcial de disparos – Propriedade 2, Cenário 1.....	167
Fig. 6.1. Conjunto de porta e trem de pouso.....	170
Fig. 6.2. Seqüência de aterrissagem.....	170
Fig. 6.3. Componentes do Sistema de Aterrissagem.....	171
Fig. 6.4. Abertura e fechamento das portas.....	176
Fig. 6.5. Modelo da classe C_1 – <i>Equipamento 1 Pistão</i>	176
Fig. 6.6. Circuito hidráulico dedicado e eletro-válvulas correspondentes.....	177
Fig. 6.7. Modelo da classe C_6 – <i>Eletro-válvula Dedicada</i>	177
Fig. 6.8. Modelo da classe C_9 – <i>Circuito Hidráulico Dedicado</i>	178
Fig. 6.9. Modelo da classe C_{10} – <i>Circuito Elétrico Genérico</i>	179
Fig. 6.10. Modelo da classe C_{19} – <i>Interface EV Dedicadas</i>	180
Fig. 6.11. Interações relevantes para Propriedade 1.....	182
Fig. 6.12. Ordem parcial de disparos – Cenários 1p, 1c, 2p e 2c – Propriedade 1.....	184
Fig. 6.13. Ordem parcial de disparos – Cenários 1p, 1c, 2p e 2c – Propriedade 1.....	186
Fig. 6.14. Ordem parcial de disparos – Cenários 1p, 1c, 2p e 2c – Propriedade 1.....	190
Fig. 6.15. Ordem parcial de disparos – Cenário 1p-1-1 – Propriedade 1.....	192
Fig. 6.16. Ordem parcial de disparos – Cenário 1p-2-1 – Propriedade 1.....	193
Fig. 6.17. Ordem parcial de disparos – Cenários 1c – Propriedade 1.....	194
Fig. 6.18. Ordem parcial de disparos – Cenários 2p-1 – Propriedade 1.....	195
Fig. 6.19. Ordem parcial de disparos – Cenários 2p-2-1 – Propriedade 1.....	195

Fig. 6.20. Ordem parcial de disparos – Cenários 2c – Propriedade 1.	196
Fig. 7.1. PFS para a produção de açúcar cristal.	206
Fig. 7.2. Recepção da cana.	207
Fig. 7.3. Recepção e lavagem da cana.	207
Fig. 7.4. Refinamento de [Recepção].	208
Fig. 7.5. Instalações para o preparo da cana.	208
Fig. 7.6. Refinamento de [Preparo].	208
Fig. 7.7. Esquema de um difusor.	209
Fig. 7.8. Refinamento de [Extração].	210
Fig. 7.9. Instalações para sulfitação.	211
Fig. 7.10. Refinamento de [Sulfitação].	211
Fig. 7.11. Esquema da calagem.	212
Fig. 7.12. Refinamento de [Calagem].	212
Fig. 7.13. Séries de aquecedores.	213
Fig. 7.14. Refinamento de [Aquecimento].	213
Fig. 7.15. Esquema da Clarificação.	214
Fig. 7.16. Refinamento de [Clarificação].	214
Fig. 7.17. Esquema da evaporação.	215
Fig. 7.18. Refinamento de [Evaporação].	216
Fig. 7.19. Configuração da planta de cristalização.	217
Fig. 7.20. Refinamento de [Cozimento e Centrifugação].	217
Fig. 7.21. Refinamento de [Cozimento Massa A].	218
Fig. 7.22. Esquema da secagem e empacotamento.	218
Fig. 7.23. Refinamento de [Secagem e Empacotamento].	219
Fig. 7.24. Modelo da classe C_7 - <i>Mesa</i>	220
Fig. 7.25. Modelo da classe C_{13} - <i>Esteira 1- Picador</i>	221
Fig. 7.26. Modelo da classe C_{74} - <i>Interface Mesas</i>	222
Fig. 7.27. Modelo da classe C_{76} - <i>Interface Picador</i>	223
Fig. 7.28. Diagrama de Colaboração das interações relevantes p/ a Propriedade 1.	225
Fig. A.1. PFS para o fluxo de óleo nos circuitos do Sistema de Aterrissagem.	239
Fig. A.2. Diagrama de Casos de Uso para o Sistema de Aterrissagem.	240
Fig. A.3. Diagrama de Atividades do Caso de Uso ‘Executar seqüência Up’.	240
Fig. A.4. Detalhamento de ‘Pressuriza’ e ‘Despressuriza circuito hidráulico geral’.	241
Fig. A.5. Detalhamento de ‘Abre portas’.	241
Fig. A.6. Diagrama de Seqüência p/ Caso de Uso ‘Executar Seqüência Up’ – Parte 1.	243
Fig. A.7. Diagrama de Seqüência p/ Caso de Uso ‘Executar Seqüência Up’ – Parte 2.	244
Fig. A.8. Modelo da classe C_2 - <i>Equipamento 2 Pistões</i>	245
Fig. A.9. Modelo da classe C_3 - <i>Alavanca Up/Down</i>	245
Fig. A.10. Modelo da classe C_4 - <i>Sensor Discreto</i>	245
Fig. A.11. Posições da eletro-válvula geral.	246
Fig. A.12. Modelo da classe C_5 - <i>Eletro-válvula / Circuito Hidráulico Geral</i>	246
Fig. A.13. Modelo da classe C_{13} – <i>Relé Analógico</i>	247
Fig. A.14. Modelo da classe C_{14} – <i>Supervisor de Equipamento</i>	248

Fig. A.15. Modelo da classe C_{15} – <i>Supervisor de Conjunto</i>	248
Fig. A.16. Modelo da classe C_{16} – <i>Supervisor do Sistema</i>	249
Fig. A.17. Modelo da classe C_{17} – <i>Interface Alavanca</i>	250
Fig. A.18. Modelo da classe C_{18} – <i>Interface EV Geral</i>	250
Fig. A.19. Diagrama de Classes para o Sistema de Aterrissagem.	251
Fig. A.20. Correspondência entre Diagrama de Seqüência da Fig. A.6 e o modelo em redes PTD-OO.	254
Fig. A.21. Correspondência entre Diagrama de Seqüência da Fig. A.7 e o modelo em redes PTD-OO.	254
Fig. A.22. Detalhamento do Diagrama de Atividades da Fig. A.3.	255
Fig. A.23. Detalhamento do Diagrama de Atividades da Fig. A.4.	255
Fig. A.24. Detalhamento do Diagrama de Atividades da Fig. A.5.	256
Fig. A.25. Conversão para redes de Petri do Diagrama de Atividades da Fig. A.22 e da Fig. A.23.....	257
Fig. A.26. Conversão para redes de Petri do Diagrama de Atividades da Fig. A.22 e da Fig. A.24.....	258
Fig. A.27. Diagrama de Colaboração I – Sistema de Aterrissagem.....	258
Fig. A.28. Diagrama de Colaboração II – Sistema de Aterrissagem.	259
Fig. A.29. Diagrama de Colaboração III – Sistema de Aterrissagem.	259
Fig. A.30. Diagrama de Colaboração IV – Sistema de Aterrissagem.....	260
Fig. A.31. Diagrama de Colaboração V – Sistema de Aterrissagem.	260
Fig. B.1. Diagrama de Casos de Uso para Recepção, Preparo e Cozimento.	261
Fig. B.2. Movimentação do guindaste.	262
Fig. B.3. Descarregamento do caminhão c/ caçamba basculante.	262
Fig. B.4. Descarregamento do caminhão c/ correntes.....	262
Fig. B.5. Diagrama de Atividades do Caso de Uso ‘Descarregar caminhão c/ caçamba basculante’.....	263
Fig. B.6. Diagrama de Seqüência do Caso de Uso ‘Descarregar caminhão c/ caçamba basculante’.....	268
Fig. B.7. Modelo da classe C_1 - <i>Caminhão Externo</i>	269
Fig. B.8. Modelo da classe C_2 - <i>Caminhão c/ Caçamba Basculante</i>	270
Fig. B.9. Modelo da classe C_3 - <i>Caminhão com Correntes</i>	271
Fig. B.10. Modelo da classe C_4 – <i>Transportador c/ Garras</i>	271
Fig. B.11. Modelo da classe C_5 - <i>Guindaste</i>	272
Fig. B.12. Modelo da classe C_6 - <i>Fosso</i>	272
Fig. B.13. Modelo da classe C_8 - <i>Chuveiro</i>	273
Fig. B.14. Modelo da classe C_9 - <i>Variador de Velocidade</i>	273
Fig. B.15. Diagrama de classes p/ C_{13} e C_{15}	273
Fig. B.16. Modelo da classe C_{15} - <i>Esteira 2-Esteira 3</i>	274
Fig. B.17. Modelo da classe C_{16} - <i>Válvula de Água</i>	274
Fig. B.18. Composição da classe C_{22}	275
Fig. B.19. Modelo da classe C_{17} - <i>Aquecedor</i>	275
Fig. B.20. Modelo da classe C_{18} - <i>Válvula de Caldo</i>	275
Fig. B.21. Modelo da classe C_{19} - <i>Moenda</i>	276

Fig. B.22. Modelo da classe C_{20} - <i>Tanque-Bomba</i>	276
Fig. B.23. Modelo da classe C_{21} - <i>Transportador</i>	278
Fig. B.24. Modelo da classe C_{23} - <i>Controle Local do Difusor</i>	279
Fig. B.25. Modelo da classe C_{24} - <i>Tanque-Bomba</i>	279
Fig. B.26. Modelo da classe C_{25} - <i>Variador de Potencia</i>	279
Fig. B.27. Modelo das classe C_{26} - <i>Compressor</i>	279
Fig. B.28. Modelo da classe C_{27} - <i>Caixa de cal</i>	280
Fig. B.29. Modelo da classe C_{28} - <i>Válvula de Ar Comprimido</i>	280
Fig. B.30. Modelo da classe C_{29} - <i>Forno Rotativo</i>	281
Fig. B.31. Modelo da classe C_{30} - <i>Coluna de Sulfitação</i>	281
Fig. B.32. Modelo da classe C_{32} - <i>Trocador de calor</i>	281
Fig. B.33. Modelo da classe C_{33} - <i>Tanque Rotativo</i>	282
Fig. B.34. Modelo da classe C_{34} - <i>Tanque de Leite de Cal</i>	283
Fig. B.35. Modelo da classe C_{35} - <i>Tanque-Bomba</i>	283
Fig. B.36. Modelo da classe C_{36} - <i>Tanque Misturador</i>	283
Fig. B.37. Modelo da classe C_{38} - <i>Divisor de Fluxo - Aquecimento</i>	284
Fig. B.38. Modelo da classe C_{39} - <i>Válvula On/Off</i>	284
Fig. B.39. Modelo da classe C_{40} - <i>Válvula 2 Posições – Aquecedor</i>	285
Fig. B.40. Composição da classe C_{45} – <i>Clarificação</i>	285
Fig. B.41. Modelo da classe C_{41} - <i>Tanque-Bomba Clarificação</i>	285
Fig. B.42. Modelo da classe C_{42} - <i>Divisor de Fluxo</i>	286
Fig. B.43. Modelo da classe C_{44} - <i>Clarificador</i>	286
Fig. B.44. Modelo da classe C_{46} - <i>Filtro de Lodo</i>	287
Fig. B.45. Modelo da classe C_{47} - <i>Tanque-Bomba 1º Efeito</i>	287
Fig. B.46. Nomenclatura para um corpo.....	288
Fig. B.47. Modelo da classe C_{49} – <i>Corpo A</i>	291
Fig. B.48. Modelo da classe C_{50} – <i>Corpo 1º Efeito</i>	292
Fig. B.49. Modelo da classe C_{52} - <i>Tanque-Bomba 2º Efeito</i>	292
Fig. B.50. Modelo da classe C_{53} – <i>Divisor de Vapor 2º Efeito</i>	293
Fig. B.51. Modelo da classe C_{54} – <i>Corpo 2º Efeito</i>	293
Fig. B.52. Modelo da classe C_{56} - <i>Tanque-Bomba 3º Efeito</i>	294
Fig. B.53. Modelo da classe C_{57} - <i>Divisor de Vapor 3º Efeito</i>	294
Fig. B.54. Modelo da classe C_{58} – <i>Corpo 3º Efeito</i>	295
Fig. B.55. Modelo da classe C_{59} – <i>Corpo B</i>	295
Fig. B.56. Modelo da classe C_{60} – <i>Corpo 4º Efeito</i>	296
Fig. B.57. Modelo da classe C_{61} – <i>Corpo 5º Efeito</i>	296
Fig. B.58. Modelo da classe C_{63} – <i>Tanque Genérico</i>	297
Fig. B.59. Modelo da classe C_{64} – <i>Tanque Xarope</i>	297
Fig. B.60. Modelo da classe C_{65} - <i>Cozedor</i>	301
Fig. B.61. Modelo da classe C_{66} – <i>Tanque Massa</i>	302
Fig. B.62. Modelo da classe C_{67} - <i>Centrífuga</i>	302
Fig. B.63. Modelo da classe C_{68} – <i>Tanque Magma</i>	303
Fig. B.64. Modelo da classe C_{69} – <i>Tanque de Mel</i>	303

Fig. B.65. Modelo da classe C_{70} – <i>Caminhão de Mel C</i> .	303
Fig. B.66. Modelo da classe C_{71} – <i>Tanque de Açúcar</i> .	304
Fig. B.67. Modelo da classe C_{72} – <i>Secador</i> .	304
Fig. B.68. Modelo da classe C_{73} – <i>Empacotador</i> .	304
Fig. B.69. Modelo da classe C_{75} – <i>Supervisor Fosso</i> .	305
Fig. B.70. Modelo da classe C_{77} – <i>Gerenciador da Produção de Caldo</i> .	305
Fig. B.71. Modelo da classe C_{78} – <i>Interface Variadores de Velocidade</i> .	306
Fig. B.72. Modelo da classe C_{79} – <i>Interface Válvula de Caldo</i> .	307
Fig. B.73. Modelo da classe C_{80} – <i>Supervisor Tanque-Bomba Sulfitação</i> .	307
Fig. B.74. Modelo da classe C_{81} – <i>Interface Bandeja de Cal</i> .	307
Fig. B.75. Modelo da classe C_{82} – <i>Interface Forno</i> .	308
Fig. B.76. Modelo da classe C_{83} – <i>Gerenciador da Sulfitação</i> .	308
Fig. B.77. Modelo da classe C_{84} – <i>Supervisor Tanque</i> .	309
Fig. B.78. Modelo da classe C_{85} – <i>Supervisor Tanque Leite de Cal</i> .	309
Fig. B.79. Modelo da classe C_{86} – <i>Supervisor Tanque Misturador</i> .	309
Fig. B.80. Modelo da classe C_{87} – <i>Interface Variador de Potência</i> .	310
Fig. B.81. Modelo da classe C_{88} – <i>Interface Aquecedor</i> .	310
Fig. B.82. Modelo da classe C_{89} – <i>Serie de Aquecedores</i> .	311
Fig. B.83. Modelo da classe C_{90} – <i>Gerenciador Aquecimento</i> .	312
Fig. B.84. Modelo da classe C_{91} – <i>Interface Clarificador - Filtro</i> .	312
Fig. B.85. Modelo da classe C_{92} – <i>Supervisor Tanque-Bomba Clarificação</i> .	313
Fig. B.86. Modelo da classe C_{93} – <i>Gerenciador Clarificação</i> .	313
Fig. B.87. Modelo da classe C_{94} – <i>Supervisor Tanque-Bomba Evaporação</i> .	314
Fig. B.88. Modelo da classe C_{95} – <i>Interface Variadores de Potência - Evaporação</i> .	314
Fig. B.89. Modelo da classe C_{96} – <i>Gerenciador Evaporação</i> .	315
Fig. B.90. Modelo da classe C_{97} – <i>Interface Cozedor</i> .	316
Fig. B.91. Modelo da classe C_{101} – <i>Gerenciador Cozimento C</i> .	317
Fig. B.92. Modelo da classe C_{102} – <i>Gerenciador Cozimento</i> .	317
Fig. B.93. Modelo da classe C_{109} – <i>Supervisor Tanque Xarope</i> .	319
Fig. B.94. Modelo da classe C_{113} – <i>Interface Caminhão de Mel C</i> .	320
Fig. B.95. Modelo da classe C_{114} – <i>Interface Secador-Empacotador</i> .	320
Fig. B.96. Detalhamento do Diagrama de Atividades da Fig. B.5.	321
Fig. B.97. Conversão para redes de Petri do Diagrama de Atividades da .	322
Fig. B.98. Diagrama de Sequência do Caso de Uso ‘Descarregar caminhão c/ caçamba basculante’.	322
Fig. B.99. Diagrama de Colaboração das interações relevantes para a Propriedade 2.	324
Fig. B.100. Ordem parcial de disparos – Cenários 1 e 2 – Propriedade 2.	325
Fig. B.101. Ordem parcial de disparos – Cenário 1-1 – Propriedade 2.	333

LISTA DE TABELAS

Tabela 6.1. Estados das portas.	172
Tabela 6.2. Estados dos trens.	172
Tabela 6.3. Estados do conjunto porta-trem.	173

LISTA DE SÍMBOLOS

Redes de Petri

- N – rede de Petri marcada.
- R – rede de Petri sem marcação.
- M_0 – marcação inicial de uma rede de Petri.
- M – marcação de uma rede de Petri.
- P – conjunto de lugares de uma rede de Petri.
- p_i – lugar ‘i’ qualquer de uma rede de Petri.
- T – conjunto de transições de uma rede de Petri.
- t_i – transição ‘i’ qualquer de uma rede de Petri.
- Pre – matriz de pré-condição de uma rede de Petri.
- Pos – matriz de pós-condição de uma rede de Petri.
- W – matriz de incidência de uma rede de Petri.
- s – vetor de disparos para uma rede de Petri.

Redes Predicado Transição

- N_{PT} – rede Predicado-Transição marcada.
- R – rede de Petri sem marcação.
- A – inscrição de uma rede Predicado-Transição.
- M_0 – marcação inicial de uma rede Predicado-Transição.
- X – conjunto de variáveis de uma rede Predicado-Transição.
- A_x – associação de um conjunto variáveis de X a cada arco de uma rede Predicado-Transição.
- A_c – associação de uma condição de disparo a cada transição de uma rede Predicado-Transição.
- A_a – associação de uma ação de disparo a cada transição de uma rede Predicado-Transição.

Redes Predicado-Transição Diferenciais

- N_{PTD} – rede Predicado-Transição Diferencial marcada
- R – rede de Petri sem marcação.

A – inscrição de uma rede Predicado-Transição Diferencial.
 M_0 – marcação inicial de uma rede Predicado-Transição Diferencial.
 X – conjunto de variáveis de uma rede Predicado-Transição Diferencial.
 A_p – associação de um conjunto variáveis de X a cada lugar de uma rede Predicado-Transição Diferencial.
 X_{p_i} – vetor de variáveis associado a cada lugar p_i de uma rede Predicado-Transição Diferencial.
 A_c – associação de uma função de habilitação a cada transição de uma rede Predicado-Transição Diferencial.
 e_i – função de habilitação de uma transição t_i de uma rede Predicado-Transição Diferencial.
 A_a – associação de uma função de junção a cada transição de uma rede Predicado-Transição Diferencial.
 j_i – função de junção de uma transição t_i de uma rede Predicado-Transição Diferencial.
 A_F – associação de um sistema de equações diferenciais a cada lugar de uma rede Predicado-Transição Diferencial.
 F_i – sistema de equações diferenciais de um lugar p_i de uma rede Predicado-Transição Diferencial.
 θ – variável que representa o tempo.
 θ_i – instante de disparo de uma transição t_i de uma rede Predicado-Transição Diferencial.
 X_{input_i} – união dos vetores X_{p_i} dos lugares de entrada da transição t_i de uma rede Predicado-Transição Diferencial.
 X_{output_i} – união dos vetores X_{p_i} dos lugares de saída da transição t_i de uma rede Predicado-Transição Diferencial.

Redes PTD-OO

N_{PTD-OO} – rede PTD-OO.
 N_{PTD-OO_i} – sub-rede ‘i’ qualquer de uma rede PTD-OO.
 C_i – nome da classe representada pela sub-rede N_{PTD-OO_i} .
 R_i – rede de Petri sem marcação associada a C_i .

P_i – conjunto de lugares de R_i .
 p_{k_i} – lugar ‘k’ qualquer de R_i .
 T – conjunto de transições de R_i .
 t_{k_i} – transição ‘k’ qualquer de R_i .
 Pre_i – matriz de pré-condição de R_i .
 Pos_i – matriz de pós-condição de R_i .
 A_i – inscrição da sub-rede N_{PTD-OO_i} .
 M_{0_i} – marcação inicial da sub-rede N_{PTD-OO_i} .
 X_i – conjunto de variáveis associado a C_i .
 A_{pi} – associação de um conjunto variáveis de X_i a cada lugar de R_i .
 $X_{p_{k_i}}$ – vetor de variáveis associado a cada lugar p_{k_i} de R_i .
 A_{ei} – associação de uma função de habilitação a cada transição de R_i .
 e_{k_i} – função de habilitação de uma transição t_{k_i} de R_i .
 A_{ji} – associação de uma função de junção a cada transição de R_i .
 j_{k_i} – função de junção de uma transição t_{k_i} de R_i .
 A_{Fi} – associação de um sistema de equações diferenciais a cada lugar de R_i .
 F_{k_i} – sistema de equações diferenciais de um lugar p_{k_i} de R_i .
 M_i – marcação da sub-rede N_{PTD-OO_i} .
 $O_{j,i}$ – nome de um objeto ‘j’ qualquer da classe C_i .
 $M_{j,i}$ – marcação referente ao objeto $O_{j,i}$ da classe C_i .
 $m_{j,i}$ – marcas da rede R_i referentes ao objeto $O_{j,i}$.
 $X_{j,i}$ – instância de X_i referentes ao objeto $O_{j,i}$.
 X_{int_i} – conjunto de variáveis internas associado a C_i .
 X_{comp_i} – conjunto de variáveis compartilhadas associado a C_i .
 X_{ext_i} – conjunto de variáveis externas associado a C_i .
 $X_{ext_c_i}$ – sub-conjunto de X_{ext_i} referente às variáveis outros objetos.
 $X_{ext_ext_i}$ – sub-conjunto de X_{ext_i} referente às variáveis externas ao sistema modelado.
 I_z – variável qualquer de interface de uma classe.
 n_{I_z,C_j} – variável de $X_{ext_c_i}$ correspondente a variável ‘n’ de uma classe qualquer C_j e associada a variável de interface I_z pertencente a X_i da classe qualquer C_i .

t_{w_i} – transição ‘w’ qualquer de R_i associada a uma operação disponibilizada por C_i .

T_{f_i} – conjunto de transições representando as operações disponibilizadas pela classe C_i às demais classes do modelo.

t_{x_i} – transição ‘x’ qualquer de R_i associada a uma chamada de método.

T_{u_i} – conjunto de transições da classe C_i representando as chamadas de métodos de outras classes do modelo.

A_{w_i} – ‘assinatura’ do método associado à transição t_{x_i} .

$T_{f_{ext_i}}$ – conjunto de transições representando as operações disponibilizadas pela classe C_i a elementos externos ao modelo.

$T_{u_{ext_i}}$ – conjunto de transições da classe C_i representando as chamadas de métodos de elementos externos ao modelo.

$p_{k_i.O_m}$ – transição ‘k’ qualquer da rede desdobrada correspondente ao objeto $O_{m.i}$.

$t_{k_i.O_m}$ – transição ‘k’ qualquer da rede desdobrada correspondente ao objeto $O_{m.i}$.

$t_{x_i.O_m}$ – transição ‘x’ qualquer pertencente a T_{u_i} da rede desdobrada correspondente ao objeto $O_{m.i}$.

$t_{w_i.O_n}$ – transição ‘w’ qualquer pertencente a T_{f_j} da rede desdobrada correspondente ao objeto $O_{n.j}$.

$t_{x_i.O_m/w_j.O_n}$ – transição correspondente a fusão das transições $t_{x_i.O_m}$ e $t_{w_i.O_n}$ (rede desdobrada).

$t_{w_j.O_n/x_i.O_m}$ – mesmo que a $t_{x_i.O_m/w_j.O_n}$ (rede desdobrada).

1 INTRODUÇÃO

A problemática abordada nesta tese é a do desenvolvimento de *Sistemas Supervisórios Híbridos*. Inicia-se este capítulo introdutório apresentando alguns conceitos básicos necessários para a compreensão do domínio deste problema. Assim, a Seção 1.1.1 introduz o conceito de *Sistemas Híbridos*. Em seguida, define-se o que são *Sistemas Produtivos*, *Sistemas de Controle* e *Sistemas Supervisórios* (Seções 1.1.2 e 1.1.3). A partir destas definições, apresenta-se na Seção 1.2 o que este trabalho considera como *Sistemas Supervisórios Híbridos*, quais as motivações e os objetivos deste trabalho, e como o texto está organizado.

1.1 Conceitos Básicos

1.1.1 *Sistemas Híbridos*

O termo “híbrido” refere-se a heterogeneidade, ou seja, a uma natureza heterogênea. No presente trabalho, este termo refere-se a natureza das variáveis que compõem o modelo de um sistema.

De acordo com Alla; David (1998), o modelo de um sistema pode ser caracterizado pela natureza de suas variáveis de estado e da variável independente que representa o tempo. As *variáveis discretas* inserem-se num conjunto enumerável de valores (ex.: números inteiros, variáveis booleanas, etc.). As *variáveis contínuas* têm seu valor definido dentro do conjunto de números reais e podem assumir infinitos valores durante um determinado intervalo de tempo.

Como consequência desta dicotomia, os modelos de um sistema podem ser classificados em *Sistemas de Variáveis Contínuas* e *Sistemas a Eventos Discretos* (Cardoso; Valette, 1997) e (Ho, 1987). Nos Sistemas de Variáveis Contínuas, o conjunto de variáveis que representa seu estado evolui de forma contínua no tempo.

Esta característica é encontrada principalmente em sistemas da natureza, cuja dinâmica é regida por leis físicas. Uma forma de modelar este tipo de sistema é através de equações diferenciais.

Em contrapartida, nos Sistemas a Eventos Discretos, as variáveis de estado são modificadas de forma discreta de acordo com a ocorrência de eventos instantâneos, isto é, de duração nula. Os valores das variáveis que representam o estado do sistema permanecem constante entre a ocorrência de eventos. Apresentam este comportamento sistemas concebidos com base em regras e procedimentos definidos pelo homem (*'man-made systems'*), como sistemas de manufatura, redes de comunicação, entre outros. Nestes casos, exemplos de eventos discreto são início do funcionamento de uma máquina, chegada de uma mensagem, etc.

A partir desta classificação definem-se como *Sistemas Híbridos* aqueles sistemas onde encontram-se simultaneamente *variáveis de estado* de natureza *contínua* e de natureza *discreta*. A evolução do sistema pode ocorrer parcialmente em função do tempo e em função da ocorrência de eventos discretos. Isto significa que, em um sistema híbrido coexistem simultaneamente sub-sistemas que pertencem às duas classes apresentadas anteriormente. A Fig. 1.1 ilustra possíveis comportamentos para uma variável de estado de um Sistema a Eventos Discreto, de um Sistema de Variáveis Contínuas e de um Sistema Híbrido.

Fig. 1.1. Comportamento de variáveis em sistemas de diferentes naturezas.

O estudo de Sistemas Híbridos teve início com a utilização de computadores no controle de processos contínuos. Uma das principais motivações foi o interesse em explicitar em um único modelo descontinuidades inerentes a processos

tradicionalmente representados por variáveis contínuas, nas quais o comportamento do sistema é modificado de modo abrupto. Exemplos de descontinuidade são (Lennartson et al., 1996):

⇒ *Descontinuidades na planta.* Um exemplo de descontinuidade na planta ocorre no processo de enchimento do tanque da Fig. 1.2. Quando o nível do tanque atinge a altura $h=h_1$, a equação que rege a evolução do nível do tanque em função do tempo e da vazão de entrada é modificada. Outros exemplos são encontrados quando a planta não é necessariamente descontínua mas apresenta um comportamento não linear. Neste caso, por uma questão de simplificação, pode-se chavear modelos lineares que representem aproximadamente o mesmo comportamento (por partes).

Fig. 1.2. Exemplo de descontinuidade na planta.

⇒ *Descontinuidades nas saídas da planta (variáveis medidas).* São devidas principalmente a dispositivos de detecção discretos (chaves de nível, chaves de fim-de-curso, etc.) e de dispositivos de monitoração (lâmpadas, sinalizadores, sirenes, etc.) que indicam restrições e limites no processo a serem considerados durante o projeto do sistema de controle.

⇒ *Descontinuidades nas entradas da planta (sinais de comando e atuação).* São resultantes da ação de dispositivos de atuação discretos (válvulas binárias, bombas, etc.) e de dispositivos de comando discretos (botões, chaves, etc.).

⇒ *Descontinuidades no controle.* São encontradas quando se tem uma divisão do processo em fases, utilizando-se, por exemplo, estratégias de controle adaptativo (onde se tem o chaveamento entre diferentes controladores contínuos). Nestes casos, eventos discretos podem ser uma abstração efetiva para modelar o chaveamento de vários modos na operação e controle de um processo contínuo.

Simultaneamente, para alguns processos considerados tradicionalmente como dirigidos a eventos discretos, foi verificada a necessidade de introdução do tempo para representar a duração de algumas atividades ou a permanência em alguns

estados. Em alguns casos, este tempo pode ser representado como uma constante. Em outros casos, entretanto, deve-se representar o tempo como uma variável cujo valor depende de características do sistema. Como resultado, tem-se a necessidade de integração de descrições da dinâmica do sistema através de equações diferenciais (que representam a evolução de determinadas variáveis contínuas no tempo) aos modelos discretos (que definem os estados em função da ocorrência de eventos instantâneos). Esta necessidade, por sua vez, propicia a utilização de abordagens híbridas em campos antes considerados unicamente discretos.

Os campos de aplicação para a teoria de sistemas híbridos são inúmeros. Alguns exemplos são controle de sistemas prediais, processos industriais (entre os quais se encontram os processos por bateladas - *batch processes*), sistemas de fornecimento de energia elétrica, sistemas aeroespaciais, etc. (Lemmon; He; Markovsky, 1999).

É importante salientar que a classificação de um sistema real em Sistema Híbrido, Sistema a Eventos Discretos ou Sistema de Variáveis Contínuas refere-se a uma abstração de determinada realidade. Um mesmo sistema físico pode ser considerado e modelado como pertencente a diversas classes. Por exemplo, a evolução da temperatura dentro de uma sala com um aquecedor pode ser modelada como um Sistema a Eventos Discretos, onde a dinâmica do sistema é regida por relações de causa e efeito do tipo “quando o aquecedor é ligado, a sala se aquece” e “quando o aquecedor é desligado, a sala se esfria”. O mesmo sistema também pode ser modelado como um Sistema de Variáveis Contínuas, onde equaciona-se a troca de calor entre o aquecedor e o ambiente da sala e obtém-se a evolução da variável temperatura em todos os instantes de tempo. Finalmente, este mesmo sistema pode ser considerado como híbrido e seu modelo apresentar a evolução da temperatura na sala após o aquecedor ser ligado ou desligado, sendo a decisão de ligá-lo ou desligá-lo tomada quando a temperatura da sala ultrapassa certos limites.

1.1.2 *Sistemas Produtivos e Sistemas de Controle*

Enquanto a seção anterior apresentou uma possível classificação de sistemas tendo por base a natureza das variáveis modeladas, esta seção inicia apresentando

uma segunda classificação onde se considera a natureza abstrata ou concreta das entidades manipuladas pelo sistema.

Neste sentido, os *Sistemas Produtivos* são definidos como sendo aqueles que realizam um processo, utilizando *entidades físicas*, para a produção de bens ou serviços. Exemplos de Sistemas Produtivos incluem não apenas sistemas de manufatura, mas também sistemas prediais, sistemas de transporte, etc. Em contrapartida, nos *Sistemas de Informação* apenas dados computacionais (informações abstratas) são manipulados. Exemplos de Sistemas de Informação são redes de comunicação, sistemas de gerenciamento de bancos de dados, etc.

A evolução da tecnologia e a crescente disponibilidade de recursos computacionais impulsionaram as aplicações de Sistemas de Informação para o controle de Sistemas Produtivos como uma forma de garantir requisitos de eficácia, eficiência e integridade desses sistemas. Assim, uma forma simplificada de se conceber um Sistema Produtivo é como sendo composto por sistema físico que troca informações com um Sistema de Informação. Neste caso, diferentemente dos demais Sistemas de Informação, as informações trocadas são apenas um meio de se atingir o objetivo final do Sistema Produtivo, e resultam em ou são resultado de modificações nas entidades físicas envolvidas. Este tipo particular de Sistema de Informação pode ser chamado de *Sistema de Controle* e o sistema físico por ele modificado pode ser entendido como *Objeto de Controle*. Assim, a partir deste ponto, sempre que o termo ‘Sistemas de Informação’ for utilizado, ele estará se referindo apenas aos Sistemas de Informação tradicionais, isto é, excluindo a classe especial de Sistema de Informação que são os Sistemas de Controle.

A Fig. 1.3 ilustra os conceitos acima apresentados, enquanto a Fig. 1.4 classifica as diversas interações em um Sistema Produtivo (Miyagi, 1996).

Fig. 1.3. Sistemas de Informação e Sistemas Produtivos.

Fig. 1.4. Interações em um Sistema Produtivo.

No entanto, existem ainda algumas diferenças entre os Sistemas de Informação tratados pela área de informática e os Sistemas de Controle considerados no presente trabalho. Estas diferenças fazem com que as técnicas, teorias e ferramentas desenvolvidas para Sistemas de Informação, não possam ser diretamente aplicadas para Sistemas de Controle. Entre elas, destacam-se:

- Uma vez que nos Sistemas de Controle a modificação de um dado pode implicar a alteração do estado de uma entidade física, existem operações que não podem ser desfeitas, pois as respectivas modificações nas entidades físicas em geral não são reversíveis. Além disso, os danos gerados por uma falha podem atingir dimensões catastróficas, envolvendo até vidas humanas. Neste sentido, a validação do comportamento de um Sistema Produtivo é um ponto crítico.
- Diferentemente dos dados nos Sistemas de Informação, as entidades físicas dos Sistemas Produtivos têm um comportamento dinâmico próprio, incluindo eventos controláveis e não controláveis, e interagindo entre si. Isto implica a consideração do comportamento próprio do Objeto de Controle para validação do respectivo Sistema de Controle.

Como resultado destas diferenças, é recomendável a divisão do processo de desenvolvimento de um Sistema de Controle em duas fases (Di Benedetto; Lygeros, 2003). De forma resumida, na primeira fase, a partir da definição do objetivo do Sistema Produtivo e da especificação das entidades físicas envolvidas, deve ser desenvolvida uma proposta para a lógica e a estrutura conceitual do Sistema de Controle deste Sistema Produtivo. Esta proposta é descrita, juntamente com o Objeto de Controle, em um *modelo para validação* que representa o comportamento do Sistema Produtivo. Este modelo deve ser baseado em alguma linguagem que permita a validação do Sistema de Controle proposto através da verificação de propriedades

do modelo do Sistema Produtivo. Uma vez que tal proposta do Sistema de Controle está devidamente validada, prossegue-se para a segunda fase, onde, a partir da parte do modelo correspondente ao Sistema de Controle, desenvolve-se e implementa-se, em alguma linguagem de programação, o Sistema de Controle propriamente dito, que deverá fazer interface com as entidades físicas e reais. Esta concepção do desenvolvimento de um Sistema de Controle é ilustrada pela Fig. 1.5.

Fig. 1.5. Fases do desenvolvimento de um Sistema de Controle.

1.1.3 Hierarquia de Controle e Sistemas Supervisórios

A seção anterior apresentou o conceito de Sistemas de Controle. Nesta seção, apresenta-se uma possível organização do Sistema de Controle de Sistemas Produtivos em níveis hierárquicos que diferem entre si no que diz respeito às características dinâmicas e funcionais.

De acordo com Silva et al. (1998) e Andreu (1996) o controle de um Sistema Produtivo hierárquico pode ser organizado nos seguintes níveis: *Planta*, *Controle Local*, *Supervisão*, *Ordenação* e *Planejamento* (Fig. 1.6). Nesta figura, a forma piramidal reflete quantitativamente os recursos humanos envolvidos em cada nível de controle em uma empresa. Para sistemas automatizados esta forma tem sido mantida como referência ilustrativa tanto do número de controladores utilizados (um controlador do nível de Ordenação é responsável por diversos controladores do nível de Supervisão, etc.) quanto da frequência com que são tomadas as decisões.

Fig. 1.6. Níveis de controle.

O Controle Local interage diretamente com os dispositivos físicos da Planta a ser controlada. Em geral, é formado por controladores como PLC (Controladores Lógico Programável) e PID (Controladores Proporcional-Integral-Derivativo).

O nível de Supervisão tem duas funções principais:

- Agir sobre o sistema de Controle Local de modo a executar as tarefas determinadas pelo nível de controle superior (nível de Ordenação), como, por exemplo, executar um plano de produção pré-determinado.
- Supervisionar a evolução de processo na Planta de modo a detectar e diagnosticar falhas, e tomar as medidas necessárias de acordo com o tipo de falha.

O nível de Ordenação determina previamente, para um certo intervalo de tempo e de acordo com uma estratégia pré-definida, as tarefas a serem executadas pelo nível de Supervisão. Ele é responsável, por exemplo, em um sistema de manufatura, pelo escalonamento das atividades e pela determinação do plano de produção a serem aplicados sobre um horizonte temporal, decidindo como será a utilização dos recursos.

O nível de Planificação toma decisões para um horizonte de tempo relativamente maior. Também é chamado de nível tático.

De uma forma genérica os níveis mais baixos são mais reativos, enquanto os mais altos agregam mais informações. De acordo com este conceito, podem-se classificar os níveis de Controle Local e de Supervisão como de tomada de decisão em tempo-real, o nível de Ordenação como reativo e o de Planificação como predominantemente não reativo, onde a tomada de decisão em tempo real, reativa e não reativa são entendidas da seguinte forma (Champagnat, 1998):

- Nos *sistemas não reativos*, as decisões são tomadas em instantes pré-definidos ao fim de cada horizonte temporal sobre o qual o plano correspondente é elaborado. Fluxos de informação indicando a ocorrência de eventos não determinam tomadas de decisão.
- Em *sistemas reativos*, existe um horizonte de tempo ao final do qual algumas decisões são tomadas. No entanto, algumas decisões são tomadas em reação à chegada de determinadas informações sem considerar o final do horizonte de tempo. O processamento das informações e a tomada de decisão não são necessariamente de duração nula.
- Em *sistemas de tempo-real*, a tomada de decisão é sincronizada com a chegada de informações (ou seja, a ocorrência de eventos), não existe noção de horizonte de tempo. A resposta do sistema a ocorrência de eventos tem constantes de tempo muito menores que as dos processos controlados na Planta.

A estrutura hierárquica apresentada na Fig. 1.6, em geral, é flexível. De acordo com a complexidade do Sistema Produtivo, os níveis de controle superiores podem não existir. Ou ainda, um determinado nível pode ser suficientemente complexo para justificar a sua organização em outros sub-níveis de controle.

É importante salientar que não apenas o conjunto de todos os níveis pode ser definido como um Sistema de Controle, mas também cada nível, de forma isolada, também constitui em si próprio um Sistema de Controle. Assim, tendo como referência a Fig. 1.4, quando o Controle Local é considerado como um Sistema de Controle, a Planta corresponde ao Objeto de Controle, e os demais níveis são parte dos elementos externos que podem interferir na evolução do Sistema Produtivo. Quando o nível de Supervisão é considerado como um Sistema de Controle, o Objeto de Controle passa a ser composto pelo Controle Local associado a Planta e o conjunto destes três níveis é então considerado como Sistema Produtivo. De forma semelhante, também pode-se considerar os demais níveis como um Sistema de Controle, sendo que o Objeto de Controle será sempre composto pela associação dos níveis inferiores.

Neste contexto, a proposta deste trabalho enquadra-se no desenvolvimento do nível de Supervisão, que é considerado como Sistema de Controle e chamado, de

forma mais específica, de *Sistema Supervisório*. A Fig. 1.7 especifica a Fig. 1.4 para este caso.

Fig. 1.7. Sistema Supervisório como Sistema de Controle.

Observa-se que ‘supervisório’ é um termo relativamente genérico que pode englobar uma série de conceitos, tanto da linguagem coloquial quanto da linguagem técnica ou científica. Até mesmo na literatura técnica, este termo vem sendo utilizado com diferentes significados, muitas vezes contrastantes. Assim, é importante salientar que, neste trabalho, este termo é utilizado apenas para indicar o nível de controle de Supervisão dentro da hierarquia apresentada e nenhuma definição formal é adotada.

1.2 Objetivo, Motivações e Contribuições

Uma vez apresentados os conceitos de Sistemas Supervisórios e Sistemas Híbridos, este trabalho define como *Sistemas Supervisórios Híbridos* aqueles Sistemas Supervisórios cujos *modelos para validação* (Fig. 1.5) do Sistema Produtivo são híbridos. Esta abordagem engloba desde o caso onde o Sistema de Controle e o Objeto de Controle são híbridos até aquele onde o Sistema de Controle é puramente discreto e o Objeto de Controle é puramente contínuo.

A necessidade de uma abordagem genérica que sistematize o desenvolvimento de Sistemas de Supervisórios Híbridos tem sido apontada por diversos autores (Lemmon; He; Markovsky, 1999). A bibliografia consultada confirma que a pesquisa relacionada ao desenvolvimento de Sistemas Supervisórios Híbridos é relativamente recente, quando comparada aos estudos na área de Sistemas de Variáveis Contínuas ou de Sistemas a Eventos Discretos, e teve início somente na década de 90. Muitos trabalhos desenvolvidos nesta área consideram o Sistema Supervisório como tendo um comportamento exclusivamente discreto, enquanto o seu Objeto de Controle

pode ser puramente contínua ou híbrido. Entretanto, este é de fato apenas um caso específico do conjunto de problemas considerados neste trabalho.

Para Nimmo (1999), o aumento da demanda por maior produtividade e eficiência em Sistemas Produtivos resultou no aumento da sofisticação e da complexidade dos processos a serem supervisionados, requerendo Sistemas Supervisórios cada vez mais elaborados. Garcia (1997) aponta também como causa da complexidade do desenvolvimento de Sistemas Supervisórios a necessidade de incorporar em um sistema em tempo-real a monitoração contínua de mudanças no estado do Objeto de Controle e a reação imediata a comandos e sinais aperiódicos enviados por níveis de controle superiores ou por usuários do Sistema Produtivo. Atualmente, o desenvolvimento de Sistemas Supervisórios é realizado de modo não formal, baseando-se principalmente na experiência prática de quem faz o projeto, evidenciando a necessidade de uma abordagem sistemática.

Considerando os problemas gerados pela natureza híbrida do Sistema Supervisório a ser desenvolvido, não existe uma abordagem formalizada e consolidada para análise e síntese de sistemas com comportamento dinâmico discreto e contínuo simultaneamente (Lemmon; He; Markovsky, 1999). Soluções *ad hoc* são ainda hoje adotadas, justificando, também sob este aspecto, a necessidade de uma sistematização de uma abordagem genérica.

Neste contexto, o objetivo desta tese é propor uma abordagem sistemática para o desenvolvimento de Sistemas Supervisórios Híbridos. O foco deste trabalho está nas atividades relacionadas a 1ª Fase do processo de desenvolvimento de um Sistema de Controle (Fig. 1.5), isto é, como obter um modelo para validação (que neste caso é híbrido) do Sistema Produtivo e como validar tal modelo. Entre os principais requisitos desta abordagem está a flexibilidade para se adaptar e adequar a diferentes tipos de Sistemas Produtivos.

Dentro do objetivo apresentado, as principais metas deste trabalho podem ser resumidas em três pontos:

1. Proposta de um formalismo para modelagem de Sistemas Híbridos, onde se considera incorporação dos conceitos de orientação a objetos às redes Predicado Transição Diferencial. Estas redes são uma técnica de modelagem onde a parte

discreta é baseada em redes de Petri e a parte contínua em equações diferenciais. Tal formalismo é apresentado no Capítulo 2.

2. Proposta de um procedimento para construção do modelo de um Sistema Supervisório Híbrido e seu respectivo Objeto de Controle, de acordo com o formalismo apresentado no Capítulo 2. Este procedimento tem como ponto de partida os objetivos do Sistema Supervisório e a especificação do Objeto de Controle a ser supervisionado. Ele define o conjunto de modelos a serem construídos, baseados nos diagramas da ‘Unified Modeling Language’, que visam auxiliar e direcionar a obtenção do modelo em redes Predicado Transição Diferencial para a 1ª Fase do processo de desenvolvimento do Sistema Supervisório (Fig. 1.5). Esta abordagem é apresentada no Capítulo 3.
3. Proposta de um procedimento para validação do Sistema Supervisório através da verificação de propriedades do modelo construído utilizando o formalismo proposto no Capítulo 2. Este procedimento é apresentado no Capítulo 4.

As propostas apresentadas são verificadas através de sua aplicação em três estudos de caso. O Estudo de Caso 1 refere-se ao sistema de ar condicionado do Edifício dos Ambulatórios do Hospital das Clínicas da Faculdade de Medicina da Universidade de São Paulo e é apresentado no Capítulo 5. O Estudo de Caso 2 é o sistema de aterrissagem do avião militar Rafale, fabricado pela empresa Dassault Aviation e é apresentado no Capítulo 6. O Estudo de Caso 3 refere-se a Usina Cruz Alta do Grupo Açúcar Guarani S/A, localizada no município de Olímpia – SP e é apresentado no Capítulo 7.

As conclusões obtidas através do desenvolvimento desta tese e algumas sugestões de trabalhos futuros são apresentadas no Capítulo 8.

2 MODELAGEM DE SISTEMAS HÍBRIDOS

Considerando o propósito deste trabalho, a construção de modelos tem um papel crucial, uma vez que a escolha do formalismo utilizado para modelagem tem uma profunda influência em como um problema é abordado e como sua solução é emoldurada (Booch; Rumbaugh; Jacobson, 1999). Além disso, a escolha do formalismo define os recursos disponíveis para análise e detecção de falhas na solução proposta.

Neste contexto, o objetivo deste capítulo é apresentar o formalismo proposto neste trabalho para modelagem de sistemas híbridos. Este formalismo é derivado da aplicação dos conceitos de orientação a objetos às redes Predicado-Transição Diferenciais.

Este capítulo está organizado da seguinte forma: a Seção 2.2 justifica a escolha das redes Predicado-Transição Diferenciais como formalismo de base para o presente trabalho. As redes Predicado-Transição Diferenciais, por sua vez, são definidas com base nas redes Predicado-Transição, derivadas das redes de Petri. Estes três formalismos são brevemente apresentados na Seção 2.2.

Em seguida, a Seção 2.4 discute alguns trabalhos onde conceitos de orientação a objeto foram incorporados às redes de Petri. Estes trabalhos formam a base para a definição do formalismo proposto, que é apresentado na Seção 2.4. Finalmente, alguns comentários são elencados na Seção 2.5.

2.1. Escolha do Formalismo de Base

O objetivo aqui não é apresentar uma revisão bibliográfica detalhada sobre os diversos formalismos propostos na literatura para a modelagem de sistemas híbridos.

Tais revisões pode ser encontrada em Guéguen; Lefebvre (2000), Champagnat (1998), entre outros.

De uma forma geral, alguns formalismos consistem em extensões de modelos contínuos, como equações diferenciais ordinárias nas quais são incluídas variáveis cujos valores podem ser modificados de forma descontínua no tempo (Antsaklis; Nerode, 1998). Outros formalismos consistem na modificação de técnicas de modelagem utilizadas em sistemas a eventos discretos, onde são introduzidos novos elementos que permitem a representação da dinâmica contínua do sistema, como nas redes de Petri Híbridas (Alla; David, 1998). Existem, também, abordagens intermediárias que combinam modelos de sistemas contínuos, descritos por equações diferenciais, e de sistemas discretos descritos por autômatos finitos ou redes de Petri, onde foi introduzida uma interface para a comunicação entre os dois tipos de modelos (Alur et al., 1995).

No presente trabalho consideram-se apenas as soluções do último grupo, pois a extensão de formalismos discretos, em geral, leva a uma ferramenta com capacidade de modelagem da parte contínua relativamente restrita e específica. O equivalente pode ser afirmado para as extensões de formalismos contínuos. Por outro lado, as abordagens que especificam uma solução a partir da mistura de um formalismo discreto com um formalismo contínuo apresentam maior flexibilidade e poder de modelagem.

Entre as abordagens deste grupo, este trabalho considerou, em especial, aquelas onde o formalismo discreto é baseado em redes de Petri. Esta escolha foi realizada tendo em consideração as já bem conhecidas propriedades deste formalismo. Entre estas vantagens destacam-se a habilidade para representar a sincronização de processos, eventos concorrentes, causalidade, compartilhamento de recursos, presença de conflitos, entre outros (David; Alla, 1994) e (Murata, 1989).

Os principais formalismos para modelagem de sistemas híbridos derivados de redes de Petri e que definem uma interface entre a parte discreta e a parte contínua, são as redes de Petri Mistas (Valentin-Roubinet, 1999) e as redes Predicado-Transição Diferenciais (Champagnat, 1998). Em ambos os casos, no entanto a aplicação destes formalismos para sistemas de elevada complexidade evidencia a necessidade de uma maior estruturação dos aspectos relacionados a modularidade e

reutilização de modelos. Visando responder a esta necessidade, considerou-se a introdução dos conceitos de orientação a objetos (Booch, 1994) a estes formalismos. Isto resultou na seleção, entre as duas propostas, da rede de Petri Predicado-Transição Diferencial, pois esta rede apresenta características como a não utilização de variáveis globais e a possibilidade de lugares conterem mais de uma marca, o que, como será visto adiante, facilita a aplicação de uma abordagem orientada a objetos.

As redes de Petri, as redes Predicado-Transição e as redes Predicado-Transição Diferenciais são apresentadas a seguir.

2.2. Das redes de Petri às redes de Predicado-Transição Diferenciais

O modelo básico de redes de Petri, também chamado de redes de Petri ordinárias, foi proposto por Carl Adam Petri em 1962 (Petri, 1962 apud Murata, 1989) e foi rapidamente reconhecido como sendo um dos formalismos mais adequados para descrição e análise de sincronismo, paralelismo, comunicação e compartilhamento de recursos entre processos concorrentes.

Uma rede de Petri é um grafo bipartido composto de dois tipos de nós: lugares e transições. Os lugares são representados por círculos e as transições por barras. Arcos orientados conectam lugares a transições e vice-versa. Uma rede de Petri marcada contém um número inteiro de marcas que são distribuídas entre os lugares. Esta repartição descreve o estado discreto do modelo. A definição formal das redes de Petri ordinárias é apresentada a seguir.

⇒ **Definição** (Cardoso; Valette, 1997) – Uma *rede de Petri marcada* é um par $N = \langle R, M_0 \rangle$, onde:

- R é uma rede de Petri definida pela 4-tupla $\langle P, T, Pre, Pos \rangle$, onde:
 - $P = \{p_1, p_2, p_3, \dots, p_m\}$ é um conjunto finito de lugares.
 - $T = \{t_1, t_2, t_3, \dots, t_n\}$ é um conjunto finito de transições.
 - $P \cap T = \emptyset, P \cup T \neq \emptyset$.
 - $Pre: P \times T \rightarrow \mathbb{N}$ define os arcos de entrada das transições ($\mathbb{N}$ é o conjunto de números naturais).

- $\text{Pos}: T \times P \rightarrow \mathbb{N}$ define os arcos de saída das transições.
- $M_0: P \rightarrow \mathbb{N}$ é a marcação inicial da rede.

Pre e Pos podem ser representados na forma de matrizes, onde as linhas representam lugares e as colunas transições. O valor de um elemento da matriz indica o peso do arco ligando o correspondente lugar à correspondente transição. Um elemento igual a zero indica que não existe arco entre os correspondentes lugar e transição. Um exemplo é apresentado na Fig. 2.1.

Fig. 2.1. Exemplo de rede de Petri, com correspondente representação matricial.

A evolução dinâmica da rede de Petri, isto é, a modificação da marcação da rede, ocorre através do disparo de transições. Uma transição t_i está habilitada para disparo quando todos os lugares à sua entrada (lugares p_j , onde $\text{Pre}(p_j, t_i) > 0$) possuem um número de marcas $M(p_j) \geq \text{Pre}(p_j, t_i)$.

Quando uma transição t_i dispara, de cada lugar p_j de entrada da transição, removem-se $\text{Pre}(p_j, t_i)$ marcas, e para cada lugar p_j de saída da transição adicionam-se $\text{Pos}(p_j, t_i)$ marcas.

A matriz de incidência (W) de uma rede de Petri representa o balanço das alterações realizadas na marcação da rede após um disparo. Ela é definida como:

$$W = \text{Post} - \text{Pre}$$

Na forma matricial, uma sequência de disparo de transições é dada por:

$$M = M_0 + W \cdot s$$

Na equação acima M é a nova marcação e s é o vetor de disparo, onde o valor de $s[i]$ representa o número de disparos da transição t_i .

As tentativas de utilização das redes de Petri em problemas práticos reais mostraram duas desvantagens principais. Em primeiro lugar, não existe o conceito de

dados e os modelos tornam-se excessivamente grandes porque toda a manipulação de dados tem que ser representada através da estrutura da rede (isto é, através de lugares e transições). Em segundo lugar, não existe noção de hierarquia e, portanto, não é possível construir um modelo de grande porte através de um conjunto separado de sub-modelos com interfaces bem definidas.

Para resolver estes problemas, foram propostas as redes de Petri de alto nível, onde procura-se incorporar estruturas de dados e decomposição hierárquica ao modelo original das redes de Petri. Entre as redes de Petri de alto nível encontram-se as redes de Petri Coloridas (Jensen, 1997) e as redes Predicado-Transição (Genrich, 1987).

No caso das redes de Petri Coloridas, o poder de descrição é aumentado através da associação de ‘cores’ às marcas. A cada lugar associa-se um conjunto de cores correspondente às marcas que podem pertencer a este lugar. A cada transição associa-se um conjunto de cores que correspondem às diferentes formas de disparar a transição. Os números inteiros da matriz de incidência ($W(p_j, t_i)$) de uma rede de Petri ordinária são substituídos por matrizes que definem para cada possível cor (forma de disparo) da transição t_i , as cores das marcas a serem retiradas ou adicionadas ao lugar p_j . Para as redes de Petri Coloridas, assim como para as redes de Petri ordinárias, as transições são consideradas como regras de um sistema de lógica proposicional (sem variáveis).

No caso das redes Predicado-Transição, é introduzida a noção de variável. A cada transição são associadas condições suplementares de disparo, que são escritas como fórmulas lógicas utilizando variáveis. As transições tornam-se portanto regras de um sistema de lógica de primeira ordem (com variáveis) (Cardoso; Valette, 1997).

A introdução da noção explícita de variável justifica a escolha das redes Predicado-Transição para a proposta de uma rede para modelagem de Sistemas Híbridos (redes Predicado-Transição Diferenciais). Assim, apresenta-se a seguir, uma versão simplificada da definição apresentada em Genrich (1987), onde se procura evidenciar os pontos que serviram de base para a proposta das redes Predicado-Transição Diferenciais.

⇒ **Definição** (Genrich, 1987 apud Champagnat, 1998) – Uma *rede Predicado-Transição marcada* é uma 3-tupla $N_{PT} = \langle R, A, M_0 \rangle$, onde:

- R é uma rede de Petri definida pela 4-tupla $\langle P, T, Pre, Pos \rangle$.
- A é a inscrição da N_{PT} , $A = \langle X, A_x, A_c, A_a \rangle$:
 - X é um conjunto de variáveis formais.
 - A_x associa a cada arco um vetor de variáveis formais de X (por simplificação considera-se peso unitário associado aos arcos).
 - A_c associa a cada transição uma condição envolvendo as variáveis pertencentes aos vetores A_x associados aos arcos de entrada da transição.
 - A_a associa a cada transição uma ação definindo os valores das variáveis pertencentes aos vetores A_x associados aos arcos de saída da transição em função dos valores das variáveis pertencentes aos vetores A_x associadas aos arcos de entrada da transição.
- M_0 é a marcação inicial da rede. Cada marca corresponde a um vetor de variáveis semelhante aos vetores associados aos arcos de saída do lugar, cujo valor deve ser definido para o instante inicial.

Nas redes Predicado-Transição, as marcas passam a ser individualizadas. Assim, uma transição está habilitada para o disparo com um determinado conjunto de marcas se, quando se atribui aos vetores dos arcos de entrada da transição os valores das variáveis destas marcas, a condição associada a transição está satisfeita. Similarmente, a ação associada a transição define o valor associado às variáveis dos vetores dos arcos de saída da transição, que são os valores atribuídos às variáveis das marcas geradas pelo disparo. Quando nenhuma ação é definida, supõem-se que o valor da variável não é alterado.

Um exemplo de disparo em uma rede Predicado-Transição é apresentado na Fig. 2.2. Nesta figura, as variáveis são $X = \{r, q, v, d\}$, os vetores associados aos arcos são $A_x(p_1, t_1) = \langle v \rangle$, $A_x(p_2, t_1) = \langle r, q \rangle$, $A_x(t_1, p_3) = \langle d, q \rangle$. Neste caso, a transição t_1 está habilitada para o disparo apenas com a marca $\langle 5 \rangle$ de p_1 . No caso da marca $\langle 3 \rangle$ a condição de disparo não é satisfeita.

Fig. 2.2. Exemplo de disparo em uma rede Predicado-Transição.

Buscando uma solução para a modelagem de sistemas híbridos que fosse resultado do acoplamento de um formalismo discreto a um formalismo contínuo, foram propostas as redes Predicado-Transição Diferenciais (redes PTD) (Champagnat, 1998). Ao contrário das redes Predicado-Transição, onde as variáveis associadas às marcas só têm seu valor alterado no momento do disparo da transição, nas redes PTD as variáveis podem ser modificadas continuamente.

As redes PTD são baseadas no seguinte princípio. A rede de Petri representa as diferentes configurações do sistema. Cada configuração é associada a um conjunto de equações que descreve a evolução das variáveis contínuas. Assim, acoplam-se sistemas de equações aos lugares da rede de Petri. Quando uma marca é adicionada ao lugar, ‘ativa-se’ o correspondente sistema de equações, que irá determinar a evolução das variáveis associadas a marca enquanto esta permanecer no lugar. Além disso, funções de habilitação são associadas às transições, habilitando-as de acordo com os valores das variáveis contínuas. Através das funções de junção, o disparo de transições modifica discretamente o valor das variáveis contínuas.

⇒ **Definição** (Champagnat, 1998) – Uma *rede Predicado-Transição Diferencial marcada* é uma 3-tupla $N_{PTD} = \langle R, A, M_0 \rangle$, onde:

- R é uma rede de Petri definida pela 4-tupla $\langle P, T, Pre, Pos \rangle$.
- A é a inscrição da N_{PTD} , $A = \langle X, A_p, A_c, A_a, A_f \rangle$:
 - X é um conjunto de variáveis formais, cujo valor é um número real.
 - A_p associa a cada lugar um vetor X_{p_i} de variáveis pertencentes a X .

- A_c associa a cada transição uma função de habilitação e_i , onde $e_i(X_{input_i}(\theta_i)) = 0$ (X_{input_i} é a união dos vetores X_{pi} dos lugares de entrada da transição t_i e θ_i é o instante de disparo da transição t_i).
- A_a associa a cada transição t_i uma função de junção j_i , onde $X_{output_i}(\theta_i^+) = j_i(X_{input_i}(\theta_i^-))$ (X_{output_i} é a união dos vetores X_{pi} dos lugares de saída da transição t_i e θ_i^+ , θ_i^- são os instantes imediatamente após e antes do disparo da transição t_i).
- A_F associa a cada lugar p_i um sistema de equações diferenciais algébricas F_i cujas variáveis são X_{pi} , suas derivadas no tempo e o tempo (θ):

$$F_i(\dot{X}_{pi}, X_{pi}, \theta) = \begin{bmatrix} f_{i1}(\dot{X}_{pi}, X_{pi}, \theta) = 0 \\ \vdots \\ f_{in}(\dot{X}_{pi}, X_{pi}, \theta) = 0 \end{bmatrix}$$

- M_0 é a marcação inicial da rede. Cada marca corresponde a um vetor de variáveis que é uma instância do vetor (X_{pi}) associado ao lugar onde a marca se encontra. O valor das variáveis de cada marca deve ser definido para o instante inicial.

No caso das redes PTD, a evolução dinâmica da rede é definida não só pelo disparo de transições, mas também pela evolução contínua das variáveis associadas às marcas. Esta evolução é determinada pelo conjunto de equações associado ao lugar onde a marca se encontra. Uma vez que uma transição está habilitada, ela dispara imediatamente. Um exemplo de disparo de transição em uma rede PTD é apresentado na Fig. 2.3.

Fig. 2.3. Exemplo de disparo de transição em uma rede PTD.

Como a rede Predicado-Transição, a rede PTD permite que uma variável seja ‘compartilhada’ entre duas marcas. Neste caso, a variável é ‘duplicada’ para uma

segunda marca através do disparo de uma transição. Isto significa que o sistema de equações associado ao lugar onde a marca se encontra pode conter esta variável. A Fig. 2.4 apresenta um exemplo de variável compartilhada. Neste caso a transição t_1 copia a variável d para p_3 e p_4 .

Fig. 2.4. Exemplo compartilhamento de variável em uma rede PTD.

O compartilhamento de variáveis evidencia a necessidade de introdução de conceitos adicionais, pois dois lugares diferentes poderiam atribuir valores para a mesma variável, tornando a resolução da rede indefinida. Um exemplo seria se o sistema de equações de p_3 fosse substituído por ' $F_3: \dot{d} + 3 = 0$ '.

Este problema leva à necessidade de dividir o vetor de variáveis associado a um lugar (e a correspondente instância na marca) em variáveis externas, internas e de saída. As variáveis internas e de saída são variáveis cujos valores podem ser modificados pelo sistema de equações daquele lugar. As variáveis externas são variáveis cujo valor é utilizado para resolução do sistema de equações, mas não pode ser modificado por ele. Uma variável compartilhada passa então a ser vista como variável de saída no lugar onde ela é calculada e variável externa nos demais lugares. Variáveis internas por sua vez não podem ser compartilhadas.

Uma terceira implicação do compartilhamento de variáveis é que se cria uma relação 'invisível' entre as marcas. Quando existe mais de uma instância de cada vetor de variáveis (mais de uma marca em um mesmo lugar), gera-se a necessidade de identificar-se de modo individual cada marca.

Outro ponto é quando se deseja comparar variáveis de duas marcas que estão no mesmo lugar e, por exemplo, selecionar a marca com a variável de menor valor. Neste caso a transição teria que conter na sua estrutura a identificação individual das marcas em questão, o que não é possível, de acordo com a definição apresentada.

Uma última observação relacionada às redes PTD é a modularidade, isto é, a possibilidade de decomposição de uma rede em uma série de sub-redes, de forma a viabilizar a modelagem de sistemas complexos, de grande porte. Este problema é discutido em Champagnat (1998), onde algumas possibilidades de decomposição são analisadas.

A busca de solução para estes problemas e a necessidade de formalizar uma estrutura modular com interfaces bem definidas induzem a introdução dos conceitos de orientação a objetos para as redes PTD, que é a contribuição deste trabalho, no que se refere à definição de um formalismo para modelagem de sistemas híbridos.

De uma forma geral, existem diversas formas de se fazer a associação entre os conceitos de orientação a objetos e redes de Petri. Algumas opções são brevemente ilustradas a seguir na Seção 2.3.

2.3. Redes de Petri e Orientação a Objetos

De acordo com Bastide (1995), os trabalhos presentes na literatura que utilizam o conceito de objeto para construção de modelos em redes de Petri podem ser divididos em dois grupos:

- a) “*Objetos dentro de redes de Petri*”. Neste caso as marcas da rede de Petri são objetos, ou seja, são instâncias de classes descritas em alguma linguagem de programação orientada a objetos (ex.: C++). O disparo de transições corresponde à ‘movimentação de objetos’ e, eventualmente, realiza a chamada de métodos destes objetos, alterando o valor dos seus atributos. Através do disparo de transições, pode-se também criar e/ou destruir objetos. Um exemplo deste tipo de abordagem é a HyNet (*Hybrid High Level Petri Net*) (Wieting, 1996), que foi desenvolvida a partir de uma classe especial de redes de Petri de alto nível chamada Thorns (*Timed Hierarchical Object-Related Nets*) (Schof; Sonnenschein; Wieting, 1995).
- b) “*Redes de Petri dentro de objetos*”. Neste caso utiliza-se a rede de Petri para modelar o comportamento interno dos objetos. A marcação da rede representa o estado do objeto e as transições são interpretadas como a execução de um método por este objeto. Esta rede é mantida escondida ou protegida (conceito de encapsulamento). As transições (ou lugares) deixadas visíveis correspondem

aos serviços oferecidos a outros objetos. Geralmente existe um modo de construir um modelo global do sistema através da união das redes dos objetos. Esta rede global modela a disponibilidade de métodos, as seqüências potenciais de execução de métodos e as possibilidades de execução paralela. Um exemplo deste tipo de rede para sistemas híbridos é proposto por Drath (1998), que utiliza redes de Petri Híbridas (Alla; David, 1998). Outros exemplos para sistemas a eventos discretos são G-CPN (*G-Coloured Petri Net*), baseada na fusão de redes de Petri Coloridas com *G-nets* (Perkusich, A.; Perkusch, M. L. B.; Chang, 1996), e OOPN (*Object-Oriented Petri Net*) (Wang, 1996).

Uma terceira abordagem consiste em misturar as duas anteriores, criando uma estrutura hierárquica dentro da rede. Este é o caso das OPN (*Object Petri Nets*) onde se busca uma integração completa dos conceitos de orientação a objetos, incluindo herança, polimorfismo, etc. (Valk, 1998); (Lakos, 1996). Nestes casos, tem-se uma rede chamada de *rede de sistema*, cujas marcas são objetos que ‘contém’ uma rede chamada de *rede objeto*. Uma marca da rede de sistema pode possuir como atributo, por exemplo, a marcação de um determinado lugar de sua rede objeto. Uma rede objeto, por sua vez, pode ser a rede do sistema para suas marcas e assim sucessivamente, gerando uma estrutura hierárquica (Valk, 1998).

A análise dos trabalhos citados anteriormente, resultou nas seguintes conclusões:

- É desejável que seja possível a construção de um modelo global do sistema, que é resultado da interação entre os modelos dos diversos objetos.
- O conceito de ‘encapsulamento’ deve ser conservado quando são definidos os mecanismos através dos quais objetos podem interagir.
- A incorporação de novos e complexos mecanismos e regras pode comprometer uma das principais vantagens das redes de Petri, que é a visualização do comportamento do sistema através da representação gráfica.
- A possibilidade de instanciação dinâmica (isto é, durante a ‘execução’ da rede) é desejável, mas não essencial para o caso de Sistemas de Controle.

Estas conclusões fundamentaram a proposta, apresentada a seguir, da aplicação dos conceitos de orientação a objetos para as redes PTD. A rede resultante é chamada de rede PTD-OO.

2.4. Aplicação dos conceitos de orientação a objetos para as redes PTD.

Segundo os princípios da orientação a objetos, um sistema é formado por um conjunto de objetos que interagem entre si e estão organizados em classes. Os conceitos de classe e de objeto podem ser considerados os pilares da orientação a objetos. Assim, inicia-se definindo como são modeladas as classes e os objetos, de acordo com a abordagem proposta.

2.4.1. Modelagem de Classes e Objetos

De acordo com Booch; Rumbaugh; Jacobson (1998), “uma classe é a descrição de um conjunto de objetos que compartilham dos mesmos atributos, operações, relações e semânticas”, isto é, compartilham do mesmo comportamento e da mesma estrutura de dados. Baseando-se nesta definição, a abordagem proposta neste trabalho associa a cada classe uma sub-rede PTD-OO (definida na sequência), que modela os possíveis comportamentos para os objetos daquela classe. Além disso, num determinado instante, o estado dos objetos pertencentes uma classe é representado pela marcação da sub-rede desta classe.

Desta forma, um sistema pode ser modelado por uma composição de sub-redes PTD-OO marcadas que interagem entre si através de suas interfaces. Esta composição de sub-redes PTD-OO marcadas forma uma rede PTD-OO marcada.

⇒ **Definição 1:** Uma *rede PTD-OO marcada* é formada por um conjunto de sub-redes PTD-OO marcadas: $N_{PTD-OO} = \{N_{PTD-OO_1}, N_{PTD-OO_2}, \dots, N_{PTD-OO_C}\}$.

Observa-se que o índice ‘C’ indica o número de classes que representam o sistema modelado.

➤ *Exemplo:* Para ilustrar os conceitos apresentados, utiliza-se como exemplo o sistema da Fig. 2.5, onde dois produtos P_1 e P_2 são misturados em um tanque Tq_1 . A admissão de P_1 e P_2 é determinada através do posicionamento das válvulas V_1 e V_2 , respectivamente, que podem assumir dois estados distintos: aberta ou

fechada. Um controlador L_1 impõe a seguinte seqüência de operações: encher Tq_1 com os produtos P_1 e P_2 , misturar P_1 e P_2 , e esvaziar Tq_1 . Para este exemplo, uma possível modelagem em redes PTD-OO é através da definição de 3 classes¹: C_1 - *Válvula*, C_2 - *Tanque* e C_3 - *Controlador*.

Fig. 2.5. Exemplo a ser modelado em redes PTD-OO.

A definição de uma sub-rede PTD-OO é baseada na definição de rede PTD apresentada na seção anterior. Neste caso, o conjunto de variáveis X_i associado a cada sub-rede N_{PTD-OO_i} do sistema representa os atributos daquela classe.

⇒ **Definição 2:** Cada sub-rede PTD-OO marcada é formada por uma 4-tupla $N_{PTD-OO_i} = \langle C_i, R_i, A_i, M_{0_i} \rangle$, onde:

- C_i é o nome da classe representada pela sub-rede.
- R_i é uma rede de Petri definida pela 4-tupla $\langle P_i, T_i, Pre_i, Pos_i \rangle$, onde os arcos têm peso unitário:
 - $P_i = \{p_{1_i}, p_{2_i}, p_{3_i}, \dots, p_{m_i}\}$ é um conjunto finito de lugares.
 - $T_i = \{t_{1_i}, t_{2_i}, t_{3_i}, \dots, t_{n_i}\}$ é um conjunto finito de transições.
 - $P_i \cap T_i = \emptyset, P_i \cup T_i \neq \emptyset$.
 - $Pre_i: P_i \times T_i \rightarrow (0, 1)$.
 - $Pos_i: P_i \times T_i \rightarrow (0, 1)$.
- A_i é a inscrição da N_{PTD-OO_i} , $A_i = \langle X_i, A_{pi}, A_{ei}, A_{ji}, A_{Fi} \rangle$:
 - X_i é um conjunto de variáveis formais (detalhado na Definição 5).
 - A_{pi} associa a cada lugar p_{k_i} um vetor X_{pk_i} de variáveis pertencentes a X_i (detalhado na Definição 4).

¹ Adota-se a seguinte convenção neste trabalho: nomes de classes são escritos em *itálico*, enquanto nomes de objetos são escritos sublinhados.

- A_{ci} associa a cada transição t_{k_i} uma função de habilitação e_{k_i} que é uma função booleana que tem como parâmetros de entrada as variáveis de X_i .
- A_{ji} associa a cada transição t_{k_i} uma função de junção j_{k_i} onde $X_i(\theta^+) = j_{k_i}(X_i(\theta^-))$ (θ^+ , θ^- são os instantes imediatamente após e antes do disparo da transição t_{k_i}).
- A_{Fi} associa a cada lugar p_{k_i} um sistema de equações diferenciais algébricas F_{k_i} que é um conjunto de equações cujas variáveis são X_{pk_i} , e cujos parâmetros de entrada são X_i :

$$F_{j_i}(\dot{X}_{pk_i}, X_i) = \begin{bmatrix} f_{j_i1}(\dot{X}_{pk_i}, X_i) = 0 \\ \vdots \\ f_{j_in}(\dot{X}_{pk_i}, X_i) = 0 \end{bmatrix}$$

- M_{0_i} é a marcação inicial da rede (detalhada na Definição 3).

➤ *Exemplo:* A Fig. 2.6, a Fig. 2.7 e a Fig. 2.8 apresentam possíveis modelos para as classes do sistema da Fig. 2.5. As definições das demais características das redes, como vetores de variáveis, marcação inicial, entre outras, são apresentadas a seguir. Nestes modelos, a variável q indica o fluxo de saída de uma válvula, Vol , Vol_{P1} , Vol_{P2} o volume total, do produto P_1 e do produto P_2 no tanque, M a quantidade de mistura a ser produzida, $K_{\theta M}$, o tempo total de mistura, θ_M tempo decorrido desde o início da mistura e pc a porcentagem de P_1 no tanque. Os índices $li.Cj$ e as variáveis l_1 , l_2 , l_3 referem-se a interface da classe e são explicados adiante. A interface discreta das classes é apresentada na Seção 2.4.3.

Fig. 2.6. Modelo da Classe 1 - Válvula.

Fig. 2.7. Modelo da Classe 2 - Tanque.

Fig. 2.8. Modelo da Classe 3 - Controlador.

Uma vez definido que o comportamento de uma classe é modelado por uma sub-rede PTD-OO, o passo seguinte é definir o que representa o estado de um objeto do sistema em um determinado instante.

Inicialmente, adotou-se que um objeto seria representado por uma marca (na sub-rede de sua classe), à qual estaria associada uma instância do conjunto de variáveis X daquela sub-rede. No entanto, esta definição elimina a possibilidade de representação de paralelismo no comportamento interno do objeto. Assim, esta definição foi flexibilizada para que o estado de um objeto pudesse ser representado por uma ou mais marcas na sub-rede de sua classe e por uma instanciação do conjunto de variáveis X de sua sub-rede:

⇒ **Definição 3:** A marcação de uma sub-rede PTD-OO é formada por um conjunto de marcações, cada qual representando o estado de um objeto $M_i = \{M_{1,i}, M_{2,i}, \dots, M_{O,i}\}$, onde:

- $M_{j,i}$ é formada por uma 3-tupla $M_{j,i} = \langle O_{j,i}, X_{j,i}, m_{j,i} \rangle$, onde:
 - $O_{j,i}$ é o nome do objeto (da sub-rede 'i') cujo estado é representado pela marcação $M_{j,i}$.
 - $X_{j,i}$ é uma instância do vetor X_i desta sub-rede.

- $m_{j,i}: P \rightarrow (0,1)$ indica as marcas que representam o estado do objeto na sub-rede de sua classe.²

Observa-se que a definição acima impõe como restrição que cada lugar pode conter apenas uma marca de cada objeto.

➤ *Exemplo:* O sistema da Fig. 2.5 é composto pelos objetos $\underline{V}_1$ e $\underline{V}_2$ da *Classe 1 – Válvula*, $\underline{Tq}_1$ da *Classe 2 – Tanque* e $\underline{L}_1$ da *Classe 3 - Controlador*. Uma possível marcação para o sistema é apresentada na Fig. 2.9. Para facilitar a compreensão desta e das demais marcações de redes PTD-OO presentes neste texto, os valores de algumas variáveis são apresentados como ‘*ind*’, de *indefinido*. Isto significa que não há interesse em se definir o valor de tais variáveis. Neste caso, o conteúdo da cada variável permanece o último valor que lhe foi atribuído. Considerando a interpretação da marcação, este valor desatualizado pode ser inconsistente, e é portanto omitido.

$$\begin{aligned}
 M_{1,1} & \begin{cases} \text{Nome do Objeto: } O_{1,1} = \underline{V}_1 \\ \text{Instância das Variáveis: } X_{1,1}: q=0; \\ \text{Marcação da rede de Petri: } m_{1,1} = \{1,0\}; \end{cases} \\
 M_{2,1} & \begin{cases} \text{Nome do Objeto: } O_{2,1} = \underline{V}_2 \\ \text{Instância das Variáveis: } X_{2,1}: q=10; \\ \text{Marcação da rede de Petri: } m_{2,1} = \{0,1\}; \end{cases} \\
 M_{1,2} & \begin{cases} \text{Nome do Objeto: } O_{1,2} = \underline{Tq}_1 \\ \text{Instância das Variáveis: } X_{1,2}: \text{Vol}=20; l_1 = 'V_1'; l_2 = 'V_2'; q_{l1,C1}=0; q_{l2,C1}=10; \\ \text{Marcação da rede de Petri: } m_{1,2} = \{1,0,0\}; \end{cases} \\
 M_{1,3} & \begin{cases} \text{Nome do Objeto: } O_{1,3} = \underline{L}_1 \\ \text{Instância das Variáveis: } X_{1,3}: M=40; K_{\theta M} = 10; \theta_M = \text{ind}; pc=0.3; \text{Vol}_{P1} = \text{ind}; \\ \text{Vol}_{P2} = \text{ind}; l_1 = 'Tq_1'; l_2 = 'V_1'; l_3 = 'V_2'; \text{Vol}_{l1,C2}=20; q_{l1,C1}=\text{ind}; q_{l2,C1}=10; \\ \text{Marcação da rede de Petri: } m_{1,2} = \{0,0,0,0,1,1,0,0,0\}; \end{cases}
 \end{aligned}$$

Fig. 2.9. Possível marcação para os objetos do sistema da Fig. 2.5.

Quanto ao conjunto de variáveis X_{pk_i} associado a cada lugar ‘k’ de uma sub-rede ‘i’, este deve respeitar a seguinte restrição, para que apenas um lugar defina o valor da variável em cada instante:

² Neste texto, o número de marcas dos lugares da rede de um objeto será indicado das seguintes formas:

- Especificando o número de marcas de todos os lugares da rede: $m_{1,3} = \{0,0,0,0,1,1,0,0,0\}$
- Indicando apenas os lugares que possuem uma marca: $m_{1,3} = \{p_{5,3}, p_{6,3}\}$
- Indicando o número de marcas de um lugar específico: $p_{4,3,1} = 1; p_{5,3,1} = 1;$

⇒ **Definição 4:** Se entre as marcações alcançáveis por um objeto 'j', existe uma marcação $m_{j,i}$ tal que $m_{j,i} \supset \{p_{a_i}, p_{b_i}\}$, então $X_{p_{a_i}} \cap X_{p_{b_i}} = \emptyset$.

➤ *Exemplo:* As possíveis marcações alcançáveis $m_{j,i}$ para os objetos do exemplo da Fig. 2.5 são ilustradas na Fig. 2.10. Considerando a restrição imposta pela Definição 4, os vetores X_p são apresentados na Fig. 2.11. Um exemplo de vetores X_p inconsistentes e que desrespeitam a Definição 4 é apresentado na Fig. 2.12.

Fig. 2.10. Marcações alcançáveis pelos objetos das classes do exemplo da Fig. 2.5.

Fig. 2.11. Vetores X_p para as classes do sistema da Fig. 2.5.

Fig. 2.12. Exemplo de vetores X_p inconsistentes.

A cada variável do conjunto de variáveis X_i está associado um *tipo*. O conceito de tipo de variável está relacionado ao conceito de tipo de dado das linguagens de programação (Cantú, 1996). O tipo define os valores que um atributo pode assumir e as operações que podem ser realizadas com ele. Neste trabalho, serão considerados apenas 4 tipos, no entanto outros tipos podem ser introduzidos. Para atributos numéricos, os tipos considerados são: ‘booleano’, ‘inteiro’, ‘real’. Além destes, considera-se ainda que os atributos podem pertencer ao tipo ‘nome_de_objeto’. Este tipo foi adicionado para permitir a inclusão, no conjunto de atributos de um objeto, do nome dos objetos com os quais ele pode interagir. Estes atributos são chamados de variáveis de interface. Por uma questão de facilidade de compreensão dos modelos, estipulou-se que, neste trabalho, as variáveis de interface são nomeadas como $l_1, l_2, l_3, l_4, l_5 \dots$. A utilização destas variáveis será explicada mais adiante.

➤ *Exemplo:* A Fig. 2.13 define os tipos das variáveis de cada classe do sistema da Fig. 2.5.

Classe 1: $X_1 = \{q: real\};$

Classe 2: $X_2 = \{Vol: real, l_1: nome_de_objeto, l_2: nome_de_objeto, q_{l1.C1}: real, q_{l2.C1}: real\};$

Classe 3: $X_3 = \{M: real, K_{\theta M}: real, \theta_M: real, pc: real, Vol_{P1}: real, Vol_{P2}: real, l_1: nome_de_objeto, l_2: nome_de_objeto, l_3: nome_de_objeto, Vol_{l1.C2}: real, q_{l2.C1}: real, q_{l3.C1}: real\};$

Fig. 2.13. Tipos de variáveis para as classes do sistema da Fig. 2.5.

O conjunto de atributos de uma classe é formado por variáveis internas (X_{int_i}), por variáveis compartilhadas (X_{comp_i}) e por variáveis externas (X_{ext_i}). O valor de uma instância de uma variável interna é acessível somente ao próprio objeto. Quando uma variável é do tipo compartilhada, outros objetos (da mesma ou de outras classes) podem ter acesso ao valor de uma instância daquela variável. Este acesso restringe-se

à leitura, isto é, o valor da variável não pode ser alterado por outros objetos. Da mesma forma que um objeto de uma classe ‘compartilha’ o valor de suas variáveis, ele também pode ter acesso ao valor de variáveis externas, isto é de variáveis que outros objetos do sistema compartilham. Define-se então que:

⇒ **Definição 5:** O conjunto de variáveis de uma classe é dado por $X_i = X_{int_i} \cup X_{comp_i} \cup X_{ext_i}$, onde $X_{int_i} \cap X_{comp_i} = \emptyset$, $X_{int_i} \cap X_{ext_i} = \emptyset$ e $X_{ext_i} \cap X_{comp_i} = \emptyset$.

➤ *Exemplo:* A Fig. 2.14 define os conjuntos X_{int_i} , X_{comp_i} e X_{ext_i} para cada classe do sistema da Fig. 2.5.

Classe 1: $X_{int_1} = \emptyset$; $X_{comp_1} = \{q\}$; $X_{ext_1} = \emptyset$;

Classe 2: $X_{int_2} = \{l_1, l_2\}$; $X_{comp_2} = \{Vol\}$; $X_{ext_2} = \{q_{l1.C1}, q_{l2.C1}\}$;

Classe 3: $X_{int_3} = \{M, K_{\theta M}, \theta_M, pc, Vol_{P1}, Vol_{P2}, l_1, l_2, l_3\}$; $X_{comp_3} = \emptyset$; $X_{ext_3} = \{Vol_{l1.C2}, q_{l2.C1}, q_{l3.C1}\}$;

Fig. 2.14. Tipos de variáveis para as classes do sistema da Fig. 2.5.

O conjunto de variáveis externas (X_{ext_i}) é composto por variáveis pertencentes à outras classes ($X_{ext_c_i}$) e variáveis cujos valores são definidos por elementos exteriores ($X_{ext_ext_i}$) ao sistema (este assunto é tratado em maiores detalhes na Seção 2.4.3):

⇒ **Definição 6:** $X_{ext_i} = X_{ext_c_i} \cup X_{ext_ext_i}$, onde $X_{ext_c_i} \cap X_{ext_ext_i} = \emptyset$.

➤ *Exemplo:* No exemplo da Fig. 2.14 todas as variáveis de X_{ext_i} pertencem a $X_{ext_c_i}$.

Quando uma classe C_i contém no seu conjunto de variáveis externas ($X_{ext_c_i}$) uma variável qualquer ‘n’ que pertence ao conjunto de variáveis compartilhadas (X_{comp_j}) de uma outra classe C_j significa que cada objeto de C_i vai ‘ler’ o valor de uma instância de ‘n’, isto é, o valor da variável ‘n’ de um determinado objeto que é a instância de C_j . É portanto necessário definir, para cada objeto de C_i , qual é o objeto de C_j que ele deve considerar quando for ‘ler’ o valor de ‘n’. O nome do objeto de C_j a ser considerado é então armazenado em uma variável de interface ‘l’ de C_i . Define-se então:

⇒ **Definição 7:** O conjunto de variáveis externas $X_{\text{ext_c_i}}$ de uma classe C_i é um multi-set do conjunto $\{X_{\text{comp_1}} \cup X_{\text{comp_2}} \cup \dots \cup X_{\text{comp_C}}\}$ de todas as variáveis compartilhadas das classes que compõem o sistema, onde:

- Cada elemento de $X_{\text{ext_c_i}}$ está associado uma classe C_j à qual pertence a variável externa.
- Cada elemento de $X_{\text{ext_c_i}}$ está associado uma variável de interface l_z , do conjunto de variáveis X_i .
- Uma variável de $X_{\text{ext_c_i}}$ é nomeada como ' $n_{l_z.C_j}$ ', onde ' n ' é o nome da variável na sua classe de origem (C_j), l_z é a variável de interface (da classe C_i) que contém o nome do objeto da classe C_j ao qual a variável ' n ' pertence.

➤ *Exemplo:* A Fig. 2.15 apresenta as associações das variáveis $X_{\text{ext_c_i}}$ para cada classe do sistema da Fig. 2.5. Considerando os objetos $\underline{V}_1$, $\underline{V}_2$, $\underline{Tq}_1$ e $\underline{L}_1$ e a marcação apresentada na Fig. 2.9, a Fig. 2.16 ilustra o compartilhamento de variáveis entre os objetos.

- Classe 1: não contém variáveis externas
- Classe 2: $q_{l_1.C_1}$ está associada a classe C_1 e à variável l_1 ;
 $q_{l_2.C_1}$ está associada a classe C_1 e à variável l_2 ;
- Classe 3: $Vol_{l_1.C_2}$ está associada a classe C_2 e à variável l_1 ;
 $q_{l_2.C_1}$ está associada a classe C_1 e à variável l_2 ;
 $q_{l_3.C_1}$ está associada a classe C_1 e à variável l_3 ;

Fig. 2.15. Associações das variáveis externas das classes do sistema da Fig. 2.5.

Fig. 2.16. Compartilhamento de variáveis para a marcação definida em Fig. 2.9.

2.4.2. Comunicação entre as sub-redes

A comunicação entre objetos em um sistema orientado a objetos baseia-se no conceito de ‘encapsulamento’. Segundo este conceito, um objeto é formado por uma estrutura interna (chamada de implementação) e por uma interface, que restringe a interação entre este objeto e os demais objetos do sistema. A estrutura interna é escondida a fim de garantir a independência da visão externa (chamada de visão abstrata) que se tem do objeto em relação à sua estrutura interna. O encapsulamento considera que alguns detalhes de um objeto são inacessíveis, o que permite reduzir o risco de corrupção involuntária do sistema. Desta forma, para que seja estabelecida uma comunicação entre dois objetos, não é necessário conhecer a sua implementação, mas apenas a interface dos dois objetos.

De acordo com (Booch; Rumbaugh; Jacobson, 1998), uma interface é uma coleção de operações³ que especifica os serviços disponibilizados por uma classe e as formas de interação de um objeto desta classe com outros objetos do sistema.

Nas redes PTD-OO, consideram-se duas formas de comunicação entre sub-redes. A primeira delas, já apresentada anteriormente, é através do compartilhamento de variáveis contínuas. Este tipo de compartilhamento é chamado de ‘contínuo’ porque um objeto tem que atualizar continuamente o valor das variáveis $X_{ext_c_i}$, de acordo com seu valor no objeto de origem. Além da comunicação contínua, dois objetos podem também se comunicar através da *chamada de métodos*, que é modelada através da *fusão dinâmica de transições*.

Desta forma, adota-se a seguinte definição para interface fornecida por uma classe em uma rede PTD-OO:

⇒ **Definição 8:** A interface fornecida por uma classe C_i às demais classes é composta por:

- Um conjunto de variáveis compartilhadas X_{comp_i} (Definição 5).

³ A UML (Booch; Rumbaugh; Jacobson, 1998) faz a seguinte distinção entre operação e método: “Uma operação especifica um serviço que pode ser requerido por qualquer objeto da classe para alterar seu comportamento; um método é uma implementação de uma operação.”

- Um conjunto de transições T_{f_i} , onde $T_{f_i} \subset T_i$ – cada transição t_{w_i} pertencente a T_{f_i} representa uma operação disponibilizada pela classe C_i , que pode ser chamada por objetos de outras classes.

➤ *Exemplo:* A Fig. 2.17 define a interface fornecida pelas classes do sistema da Fig. 2.5:

Classe 1: $X_{comp_1} = \{q\}$; $T_{f_1} = \{t_{1_1}; t_{2_1}\}$;
 t_{1_1} – ‘Abrir válvula’
 t_{2_1} – ‘Fechar válvula’

Classe 2: $X_{comp_2} = \{Vol\}$; $T_{f_2} = \{t_{1_2}; t_{2_2}; t_{4_2}; t_{5_2}\}$;
 t_{1_2} – ‘Iniciar mistura’
 t_{2_2} – ‘Finalizar mistura’
 t_{4_2} – ‘Esvaziar’
 t_{5_2} – ‘Finalizar mistura e esvaziar’

Classe 3: $X_{comp_3} = \emptyset$; $T_{f_3} = \emptyset$;

Fig. 2.17. Interface fornecida pelas classes do sistema da Fig. 2.5 às demais classes.

Além da interface *fornecida* por uma classe, no contexto deste trabalho, é importante definir a interface *utilizada* pela classe, isto é, quais são as operações e as variáveis de outros objetos que os objetos daquela classe pode vir a utilizar. Define-se então a interface utilizada por uma classe como sendo:

⇒ **Definição 9:** A interface *utilizada* por uma classe C_i é composta por:

- Um conjunto de variáveis externas $X_{ext_c_i}$ (Definições 5, 6 e 7).
- Um conjunto de transições T_{u_i} , onde $T_{u_i} \subset T_i$ e $T_{u_i} \cap T_{f_i} = \emptyset$ - cada transição t_{x_i} pertencente a T_{u_i} representa uma operação chamada pela classe C_i .

Como para o caso das variáveis externas, para cada transição de T_{u_i} é preciso definir qual a classe que contém a operação a ser chamada (classe C_j) e qual é o objeto desta classe que deve ser considerado quando um objeto da classe C_i for realizar a chamada de operação.

⇒ **Definição 10:** O conjunto de transições T_{u_i} de uma classe C_i é um multi-set do conjunto $\{T_{f_1} \cup T_{f_2} \cup \dots \cup T_{f_c}\}$ de todas as operações disponibilizadas pelas classes que compõem o sistema, onde:

- Cada transição t_{x_i} de T_{u_i} está associada a uma transição t_{w_j} de T_{f_j} da classe C_j . Esta associação indica que a transição t_{x_i} ‘chama’ o método associado a t_{w_j} .
- Cada transição t_{x_i} de T_{u_i} está associada a uma variável de interface l_z , do conjunto de variáveis X_i .
- A inscrição $t_{x_i} \rightarrow t_{w_j.l_z}$ representa estas associações e indica que para um objeto da classe C_i a transição t_{x_i} chama o método associado a t_{w_j} para o objeto de C_j cujo nome está armazenado na variável l_z do objeto de C_i .

➤ *Exemplo:* A Fig. 2.18 define a interface utilizada pelas classes do sistema da Fig. 2.5:

Classe 1: $X_{ext_c_1} = \emptyset$; $T_{u_1} = \emptyset$;
 Classe 2: $X_{ext_c_2} = \{q_{l1.C1}, q_{l2.C1}\}$; $T_{u_2} = \emptyset$;
 Classe 3: $X_{ext_c_3} = \{Vol_{l1.C2}, q_{l2.C1}, q_{l3.C1}\}$; $T_{u_3} = \{t_{2_3}; t_{3_3}; t_{4_3}; t_{5_3}; t_{6_3}\}$;
 $t_{2_3} \rightarrow t_{1_1.l2}$ – Chamada do método ‘Abrir válvula’
 $t_{3_3} \rightarrow t_{1_1.l3}$ – Chamada do método ‘Abrir válvula’
 $t_{4_3} \rightarrow t_{2_1.l2}$ – Chamada do método ‘Fechar válvula’
 $t_{5_3} \rightarrow t_{2_1.l3}$ – Chamada do método ‘Fechar válvula’
 $t_{6_3} \rightarrow t_{1_2.l1}$ – Chamada do método ‘Iniciar mistura’
 $t_{7_3} \rightarrow t_{5_2.l1}$ – Chamada do método ‘Finalizar mistura e esvaziar’

Fig. 2.18. Interface utilizada pelas classes do sistema da Fig. 2.5.

Para facilitar a compreensão visual dos modelos, estipula-se que as transições pertencentes a T_f (operações disponibilizadas pela classe) são representadas por retângulos vazios e as transições pertencentes a T_u (operações utilizadas pela classe) são representadas por retângulos cheios. A Fig. 2.19, a Fig. 2.20 e a Fig. 2.21 apresentam os modelos em redes PTD-OO das classes da Fig. 2.6, da Fig. 2.7 e da Fig. 2.8, considerando agora esta notação para diferenciar as transições pertencentes a T_u e T_f . Ainda, para facilitar a visualização, foram excluídos das figuras abaixo os elementos das redes não utilizados pela classe (definidos anteriormente como $\emptyset$).

Fig. 2.19. Modelo da Classe 1 - Válvula.

Fig. 2.20. Modelo da Classe 2 - Tanque.

Fig. 2.21. Modelo da Classe 3 - Controlador.

Do ponto de vista dinâmico, a execução de uma chamada de método é realizada através da *fusão* das duas transições envolvidas: a que representa a chamada do método (t_{x_i} pertencente a T_{u_i} de uma classe C_i) e a que representa o fornecimento do método (t_{w_j} pertencente a T_{f_j} de uma segunda classe C_j). Esta *fusão de transições* está habilitada quando ambas as transições estão habilitadas nas redes de suas respectivas classes. Além disso é necessário que o valor da variável de interface I_z do objeto que está habilitando a transição t_{x_i} da chamada de método corresponda ao nome do objeto que está habilitando a transição t_{w_j} .

- *Exemplo:* Admita-se a hipótese em que o modelo do sistema da Fig. 2.5 esteja no estado apresentado pela Fig. 2.22, onde as duas válvulas (objetos $\underline{V}_1$ e $\underline{V}_2$) se encontrem fechadas e o controlador (objeto $\underline{L}_1$) indique que o tanque já foi enchido com o produto P_2 , mas deve ainda receber o produto P_1 . Neste caso, observa-se que a fusão das transições $t_{2,3}$ e $t_{1,1}$ está habilitada para o disparo considerando as marcas dos objetos $\underline{L}_1$ e $\underline{V}_1$, pois $l_2 = O_{1,1} = \underline{V}_1$. No entanto o mesmo não pode ser dito para o disparo considerando as marcas dos objetos $\underline{L}_1$ e $\underline{V}_2$, pois $l_2 \neq O_{2,1}$.

Fig. 2.22. Exemplo de chamada de método.

Uma vez habilitada a fusão de transições, ambas disparam como se fossem uma única transição.

- *Exemplo:* A Fig. 2.23 apresenta a rede da Fig. 2.22 após o disparo das transições $t_{2,3}$ e $t_{1,1}$, considerando os objetos $\underline{L}_1$ e $\underline{V}_1$.

Fig. 2.23. Rede da Fig. 2.22 após a fusão e o disparo das transições $t_{2,3}$ e $t_{1,1}$.

De acordo com o apresentado anteriormente, um objeto pode ter acesso ao valor de uma variável de um outro objeto através do compartilhamento de variáveis. Neste caso, a comunicação é contínua no tempo, isto é, o valor da variável é constantemente atualizado. No entanto, no caso em que a variável externa é utilizada na função de junção de um objeto, não existe necessidade de atualização contínua do valor da variável, é necessário apenas conhecer o seu valor no instante de disparo da transição à qual a função de junção está associada.

Para evitar um desnecessário compartilhamento contínuo de variáveis, possibilita-se a passagem de valores através da chamada de métodos, como ocorre nas linguagens de programação (Cantú, 1996). Desta forma, quando o Objeto 1 chama um método do Objeto 2, o Objeto 1 pode informar ao Objeto 2 valores que são utilizados como entrada na função de junção da transição (do Objeto 2)

correspondente ao método chamado. Os valores transmitidos são calculados com base nos valores das variáveis do Objeto 1 pertencentes a X_{comp} . O número e o tipo dos valores a serem informados é indicado na definição da ‘assinatura’ do método. Define-se, então:

⇒ **Definição 11:** Para cada transição $t_{w,j}$ do conjunto de transições $T_{f,j}$ de uma classe C_j é definida uma ‘assinatura’ $S_{w,j}$, composta por uma lista de n variáveis pertencentes a X_j cujos valores devem ser recebidos pelos objetos da classe C_j quando o método associado a $t_{w,j}$ é chamado.

⇒ **Definição 12:** Para cada transição $t_{x,i}$ do conjunto de transições $T_{u,i}$ de uma classe C_i é definido um conjunto de valores (fixos ou resultado da combinação matemática dos valores das variáveis desta classe) que deve ser transmitido quando esta transição chama o método da correspondente transição $t_{w,j}$. O número e os tipos dos valores transmitidos devem corresponder àqueles da ‘assinatura’ $S_{w,j}$, definida para a transição $t_{w,j}$ na classe C_j .

➤ **Exemplo:** A Fig. 2.24 apresenta um exemplo de passagem de valores através da chamada de métodos. Neste caso, quando o ‘Método 1’ é chamado, o Objeto 1 deve receber dois valores do tipo ‘real’, que são armazenados nas variáveis x e z . O ‘Método 1’ então utiliza estes valores para calcular o valor da variável y . O estado da rede após o disparo é apresentado na Fig. 2.25.

Fig. 2.24. Exemplo de passagem de valores através da chamada de métodos.

Fig. 2.25. Rede da Fig. 2.24 após o disparo das transições t_{1_1} e t_{1_2} .

2.4.3. Interface com Elementos Externos

As redes de Petri, da forma como foram inicialmente propostas, e, conseqüentemente, também as redes Predicado-Transição e as redes PTD não consideram a possibilidade de elementos exteriores ao sistema interferirem no comportamento do sistema. Qualquer elemento que interfira no comportamento do sistema deve ter seu próprio comportamento incluído no modelo em redes de Petri – em outras palavras, ele é parte do sistema modelado.

Entretanto, para a implementação prática dos sinais de controle de um sistema, é necessário explicitar interferências de elementos externos, cujo comportamento não é conhecido e, portanto, não pode ser incluído no modelo. Neste sentido, algumas extensões de redes de Petri, como por exemplo o MFG (Miyagi, 1988), definiram formas de comunicação com o ambiente exterior.

Para as redes PTD-OO, a interface com o ambiente exterior é definida de forma semelhante à interface com outros objetos:

$\Rightarrow$ **Definição 12:** A interface com o ambiente exterior de uma classe C_i é composta por:

- Um conjunto de variáveis externas $X_{\text{ext_ext}_i}$ (Definições 5, 6 e 7).

- Um conjunto de transições $T_{f_ext_i}$, onde $T_{f_ext_i} \subset T_i$ – cada transição t_{h_i} pertencente a $T_{f_ext_i}$ representa uma operação disponibilizada pela classe C_i , que pode ser chamada por elementos exteriores ao sistema.
- Um conjunto de transições $T_{u_ext_i}$, onde $T_{u_ext_i} \subset T_i$ e $T_{u_ext_i} \cap T_{f_ext_i} = \emptyset$ – cada transição t_{y_i} pertencente a $T_{u_ext_i}$ representa uma operação de elemento exterior ao sistema que é chamada pela classe C_i .

➤ *Exemplo:* A Fig. 2.26 define a interface fornecida pelas classes do sistema da Fig. 2.5 a elementos exteriores ao sistema modelado. A associação de um método a transição t_{1_3} indica que a produção de um lote só é iniciada quando um elemento externo ao sistema faz uma solicitação.

Classe 1: $X_{ext_ext_1} = \emptyset$; $T_{f_ext_1} = \emptyset$; $T_{u_ext_1} = \emptyset$;
 Classe 2: $X_{ext_ext_2} = \emptyset$; $T_{f_ext_2} = \emptyset$; $T_{u_ext_2} = \emptyset$;
 Classe 3: $X_{ext_ext_2} = \emptyset$; $T_{f_ext_3} = \{t_{1_3}\}$; $T_{u_ext_3} = \emptyset$;
 t_{1_3} – ‘Iniciar produção’

Fig. 2.26. Interface fornecida pelas classes do sistema da Fig. 2.5 à elementos externos.

A representação gráfica das transições $T_{u_ext_i}$ e $T_{f_ext_i}$ é semelhante à das transições T_{u_i} e T_{f_i} .

Observa-se que, para a execução da rede, deve-se especificar um comportamento para estes elementos externos. O mesmo não é imposto para a análise, que pode ser realizada considerando todos um conjunto de possíveis interações com elementos externos.

2.4.4. Desdobramento da rede PTD-OO

A fusão de transições apresentada na seção anterior é considerada dinâmica porque um método oferecido por uma classe pode ser chamado por objetos de diferentes classes, o que significa que a transição associada àquele método poderá ser fundida com diferentes transições de diferentes classes. Um exemplo é a transição t_{1_1} da Fig. 2.19, que pode ser fundida com ambas as transições t_{2_3} e t_{3_3} da Fig. 2.21. O fato da fusão de transição ser dinâmica significa que a estrutura da rede de Petri que representa o comportamento discreto do sistema também o é, o que é uma grande desvantagem, do ponto de vista da análise do modelo, porque as

técnicas e os métodos definidos para as redes de Petri ordinárias não podem ser aplicados.

Uma forma de contornar este problema é através do desdobramento da rede PTD-OO, que consiste na construção de um modelo global do sistema, de estrutura fixa. O desdobramento da rede é realizado de acordo com a marcação inicial do sistema. Duas marcações iniciais diferentes podem levar a duas redes PTD-OO desdobradas diferentes, não apenas do ponto de vista da marcação mas também da estrutura.

Dada uma marcação inicial, o desdobramento só é possível se o número de objetos de cada classe for conhecido e constante. Isto implica que a rede de cada classe deve ser limitada (isto é, o número máximo de marcas na rede durante a evolução do sistema é limitado).

O desdobramento da rede é realizado nas seguintes etapas:

⇒ **Etapa 1** - A rede de cada classe C_i é copiada o número de vezes dos objetos instanciados daquela classe na marcação inicial. O estado de cada objeto é representado em uma rede diferente. Para cada objeto $O_{m,i}$ as transições e os lugares são renomeadas de $t_{k,i}$ e $p_{k,i}$ para $t_{k,i.O_m}$ e $p_{k,i.O_m}$.

➤ *Exemplo:* Considera-se o sistema da Fig. 2.5 e a marcação apresentada na Fig. 2.9. Neste caso, a única classe que possui mais de um objeto instanciado é C_1 – *Válvula*, que possui dois objetos ($\underline{V}_1$ e $\underline{V}_2$). A rede desta classe é então copiada e cada objeto é representado em uma rede diferente (Fig. 2.27 e Fig. 2.28). Para os demais objetos realiza-se apenas a renomeação dos lugares e transições.

Fig. 2.27. Etapa 1 do desdobramento da rede para os objetos $O_{1,1}$ e $O_{2,1}$ do sistema da Fig. 2.5.

Fig. 2.28. Etapa 1 do desdobramento da rede para os objetos $O_{1.2}$ e $O_{1.3}$ do sistema da Fig. 2.5.

⇒ **Etapa 2** - Na rede de cada objeto, cada transição correspondente a uma chamada de método ($t_{x_i} \subset T_{u_i}$) é copiada o número de vezes dos objetos da classe que fornece o método por ela chamado. As transições são renomeadas de $t_{x_i.O_m}$ para $t_{x_i.O_m/w_j.O_n}$, onde $t_{w_j.O_n}$ é a transição do objeto $O_{n,j}$ que fornece o método chamado por $t_{x_i.O_m}$. A cada transição $t_{x_i.O_m/w_j.O_n}$ é associada a função de habilitação $l_z = O_{n,j}$, onde l_z é a variável de interface do objeto $O_{m,i}$ associada a chamada de método da transição $t_{x_i.O_m}$.

➤ *Exemplo:* Para o exemplo da Fig. 2.28, a Fig. 2.29 apresenta a nova rede para o objeto L_1 (único objeto que possui transições correspondentes a chamadas de método).

Fig. 2.29. Etapa 2 do desdobramento da rede do sistema da Fig. 2.5.

⇒ **Etapa 3** - Na rede de cada objeto, cada transição correspondente a um método fornecido ($t_{w,j} \subset T_{f,j}$) é copiada o número de vezes das transições dos objetos chamam este método. As transições são renomeadas de $t_{w,j,On}$ para $t_{w,j,On/x_i,On}$, onde $t_{x_i,Om}$ é a transição do objeto $O_{m,i}$ que eventualmente chama o método fornecido por $t_{w,j,On}$. Os métodos que não são chamados por nenhuma classe do sistema podem ser eliminados. O modelo resultante desta etapa possui uma estrutura estática. Para obter o modelo global do sistema, basta fundir as transições correspondentes: $t_{w,j,On/x_i,On}$ (da rede do objeto $O_{n,j}$) com $t_{x_i,Om/w_j,On}$ (da rede do objeto $O_{m,i}$).

➤ **Exemplo:** Considerando o sistema da Fig. 2.5 e a marcação apresentada na Fig. 2.9, as únicas transições duplicadas são $t_{1,1.01}$, $t_{1,1.02}$, $t_{2,1.01}$ e $t_{2,1.02}$, pois são chamadas por duas transições de $O_{1.3}$. O modelo resultante é apresentado na Fig. 2.31.

Fig. 2.30. Etapa 3 do desdobramento da rede para os objetos $O_{1.1}$ e $O_{2.1}$ do sistema da Fig. 2.5.

Fig. 2.31. Etapa 3 do desdobramento da rede para o objetos $O_{1,2}$ do sistema da Fig. 2.5.

⇒ **Etapa 4** – Esta última etapa consiste na simplificação do modelo resultante da Etapa 2 para os casos em que, de acordo com a estrutura da classe, as variáveis de interface são constantes durante a evolução do sistema. Se a variável l_z associada a uma chamada de método é sempre constante, significa que a transição $t_{x_i.Om/w_j.On}$ a ser habilitada será sempre a mesma, e portanto as demais transições (referentes a outros objetos da classe C_z) podem ser excluídas do modelo. Além disso, as variáveis de interface podem ser eliminadas, o que significa que o comportamento do sistema do ponto de vista puramente discreto passa a ser representado por uma rede de Petri ordinária.

➤ *Exemplo:* Para o exemplo da Fig. 2.29, de acordo com a rede desta classe, as variáveis de interface l_1 , l_2 e l_3 são sempre constantes (não existe nenhuma função de junção que as altere). O valor de l_2 determina qual das transições $t_{2_3.O1/1_1.O1}$ ou $t_{2_3.O1/1_1.O2}$, e $t_{4_3.O1/2_1.O1}$ ou $t_{4_3.1/2_1.O2}$ serão habilitadas. Semelhantemente l_3 determina a habilitação de $t_{3_3.O1/1_1.O1}$ ou $t_{3_3.O1/1_1.O2}$, e de $t_{5_3.O1/2_1.O1}$ ou $t_{5_3.O1/2_1.O2}$. Uma vez que, para $\underline{l}_1$, $l_2=\underline{V}_1$ ($O_{1,1}$) e $l_3=\underline{V}_2$ ($O_{2,1}$), as únicas transições que poderão ser disparadas são $t_{2_3.O1/1_1.O1}$, $t_{3_3.O1/1_1.O2}$, $t_{4_3.O1/2_1.O1}$ e $t_{5_3.O1/2_1.O2}$. Sendo assim, as demais transições podem ser eliminadas do modelo, resultando na rede da Fig. 2.32.

Fig. 2.32. Etapa 4 do desdobramento da rede do sistema da Fig. 2.5.

Nos casos em que todas as variáveis de interface associadas às chamadas de métodos são constantes, a dinâmica do sistema do ponto de vista discreto pode ser representada pela rede de Petri ordinária correspondente à rede PTD-OO desdobrada. Esta característica é particularmente importante, pois viabiliza a utilização do procedimento proposto no Capítulo 4 para análise. Se, ao contrário, uma ou mais variáveis de interface não são constantes, apesar de ser possível o desdobramento da rede, a representação da dinâmica do ponto de vista discreto não pode ser representada por uma rede de Petri ordinária. Isto acontece porque devem ser mantidos os nomes dos objetos, as variáveis de interfaces não-constantes e as funções de habilitação que utilizam tais variáveis.

2.5. Observações

Neste capítulo, o formalismo proposto por Champagnat (1998) para as redes PTD foi modificado através da incorporação dos conceitos de orientação a objeto, resultando nas redes PTD-OO. O objetivo principal desta incorporação foi a modelagem segundo uma estrutura modular para sistemas complexos. Desta forma, até mesmo um modelo de grande porte (com um grande número de lugares, transições e/ou sistemas de equação) pode ser mais facilmente construído, compreendido e analisado.

Em relação às redes PTD, não foram propostas alterações na dinâmica da rede. Nas redes PTD-OO, assim como nas redes PTD, a ocorrência de eventos discretos tem prioridade sobre a evolução do tempo e a ocorrência de eventos internos tem a mesma prioridade que a ocorrência de chamada de métodos.

Entre as vantagens resultantes das modificações introduzidas está a possibilidade de desdobramento da rede quando o número de objetos é limitado. Neste caso, o modelo final é uma rede 1-limitada (isto é, uma rede onde a marcação de cada lugar é sempre igual ou inferior a um) com uma estrutura estática, o que é particularmente importante do ponto de vista da análise, como será ilustrado no Capítulo 4, pois todas as técnicas desenvolvidas para análise de modelos em redes de Petri podem ser utilizadas diretamente.

Observa-se, no entanto, que a definição de um número limitado de objetos não é uma imposição para utilização do formalismo, mas apenas uma recomendação. É deixada ao usuário a opção de construir modelos onde o número de objetos de uma determinada classe é indeterminado, bastando para tanto que a rede não seja limitada e que a criação de um novo objeto seja requerida por um outro objeto. Neste caso, não é possível aplicar a abordagem proposta no Capítulo 4 para análise, mas, ainda assim, é possível analisar o modelo através de técnicas de simulação.

Outra vantagem do formalismo proposto em relação as redes PTD concerne a modelagem de Sistemas Produtivos. Nas redes PTD-OO, todos os componentes do sistema (correspondentes a objetos) têm uma identidade definida. Toda ‘ordem’, emitida por um objeto que faz parte do Sistema de Controle, tem especificado o receptor desta ordem (um objeto do Objeto de Controle), o que facilita a conversão do modelo do Sistema de Controle num programa de controle (2ª Fase do processo de desenvolvimento de um Sistema de Controle, Fig. 1.5 da Seção 1.1.2). Além disso, a organização do modelo em classes e objetos é fundamental para a implementação estruturada do *software* de controle/supervisão.

3 DESENVOLVIMENTO DE SISTEMAS SUPERVISÓRIOS HÍBRIDOS

O desenvolvimento de Sistemas Supervisórios Híbridos pode ser considerado, em parte, como uma atividade da Engenharia de *Software*, uma vez que, conforme apresentado na Seção 1.1, os Sistemas Supervisórios são uma classe especial de Sistemas de Informação. No entanto, conceitos, técnicas, métodos e ferramentas definidos genericamente para auxiliar o desenvolvimento de Sistemas de Informação devem ser adaptados para atender às necessidades particulares dos Sistemas Supervisórios Híbridos, que incluem tópicos específicos da área de Engenharia de Controle, como a necessidade de compreensão e modelagem do Objeto de Controle segundo formalismos apropriados, e a problemática de como definir, a partir deste modelo, um Sistema de Controle que imponha um determinado comportamento ao Objeto de Controle.

Na Engenharia de *Software*, um dos modelos mais difundidos para o processo de desenvolvimento de Sistemas de Informação é o modelo incremental, que tem como um de seus principais exemplos o *Rational Unified Process* (RUP) (Jacobson; Booch; Rumbaugh, 1999). De acordo com o modelo incremental, o desenvolvimento do sistema é realizado em ciclos, ao final de cada um dos quais uma versão do produto é produzida. Além disso, cada ciclo deve gerar também um conjunto de modelos que auxiliam e documentam o processo de desenvolvimento.

As principais etapas abordadas em cada ciclo são: definição de requisitos, análise⁴ de requisitos, projeto (*design*), implementação e testes. Estas etapas podem

⁴ Especificamente nesta seção, o termo ‘análise’ refere-se a análise dos requisitos, diferentemente do restante do texto, onde se refere a análise do modelo construído em redes PTD-OO.

ser abordados simultaneamente, em maior ou menor intensidade, no decorrer de um ciclo, conforme ilustra a Fig. 3.1, onde a área sob as curvas representa a intensidade de trabalho envolvida na respectiva etapa.

Fig. 3.1. Etapas abordadas no decorrer de um ciclo (Jacobson; Booch; Rumbaugh, 1999).

Conforme apresentado na Seção 1.1.2, considera-se neste trabalho que o processo de desenvolvimento de um Sistema Supervisório Híbrido é composto por duas fases principais. Na 1ª Fase, obtém-se um *modelo para validação* do Sistema Supervisório e seu Objeto de Controle em um formalismo (neste caso redes PTD-OO), que é então devidamente validado. Em seguida, na 2ª Fase, este modelo é detalhado e implementado em alguma linguagem de programação.

No caso da adoção de um modelo incremental, como o RUP, para o desenvolvimento de Sistemas Supervisórios Híbridos, ambas as fases devem estar presente em cada ciclo. A relação entre estas fases e as diferentes etapas da Engenharia de *Software* a serem abordadas em um ciclo é apresentada na Fig. 3.2.

Cada etapa a ser abordada corresponde à produção e ao detalhamento de um conjunto de modelos, que podem ser representados por diagramas da *Unified Modeling Language* (UML) (Booch; Rumbaugh; Jacobson, 1999).

Fig. 3.2. A modelagem em redes PTD-OO e as etapas da Engenharia de *Software*.

Neste contexto, o objetivo deste capítulo é propor um procedimento para construção do modelo de um Sistema Supervisório Híbrido e seu respectivo Objeto de Controle de acordo com o formalismo apresentado no Capítulo 2. Este procedimento tem como ponto de partida os objetivos do Sistema Supervisório e a especificação do Objeto de Controle a ser supervisionado. Ele define um conjunto de modelos a serem construídos, baseados nos diagramas da UML, que visam auxiliar e documentar, de forma gradual e sistemática, a obtenção do modelo em redes PTD-OO para 1ª Fase do processo de desenvolvimento do Sistema Supervisório (Fig. 3.2), enfocando diferentes aspectos relacionados ao comportamento dinâmico do sistema e à sua organização em classes e objetos.

Este procedimento é detalhado na Seção 3.1. A Seção 3.3 trata de um aspecto particular desta abordagem que é a utilização de relações de composição/decomposição e especialização/generalização na construção do modelo em redes PTD-OO. A Seção 3.4 trata de alguns aspectos relacionados a modelagem do Sistema de Controle Local e explora a interação entre o projeto deste sistema e o projeto do Sistema Supervisório, visando otimizar o desempenho do Sistema Produtivo. A Seção 3.5 encerra o capítulo apresentando alguns comentários sobre o que foi proposto.

3.1. A Modelagem em Redes PTD-OO e os Diagramas da UML

Para cada ciclo do desenvolvimento de um Sistema Supervisório Híbrido, a 1ª Fase pode ser organizada em um conjunto de **atividades**⁵ onde são especificados, entre outras coisas, os diagramas UML a serem construídos.

Entre as linguagens definidas para modelagem de sistemas orientados a objetos, a UML foi escolhida por ter demonstrado ser, de fato, um padrão para representação deste tipo de sistema. Ela é o resultado da união dos esforços de muitos especialistas em orientação a objeto, dos quais destacam-se Grady Booch (*Método Booch*), Jim Rumbaugh (*Object Modeling Technique* (OMT)), Ivar Jacobson (*Object-Oriented Software Engineering* (OOSE)) e David Harel (*Statecharts*).

De uma forma geral, pode-se descrever a UML como uma linguagem que, a partir de alguns elementos básicos e dos tipos de relação entre estes elementos, define uma série de diagramas que têm como finalidade a representação de diferentes aspectos de um mesmo sistema. Este texto não pretende apresentar uma revisão bibliográfica sobre os diagramas da UML, tema para o qual cita-se como referência Booch; Rumbaugh; Jacobson (1999).

Observa-se que, de acordo com a necessidade, são propostas algumas alterações para os diagramas da UML, visando uma melhor representação de aspectos relacionados à dinâmica contínua do sistema modelado.

As **atividades** que compõem o procedimento proposto são apresentadas na Fig. 3.3. É importante salientar que apesar das **atividades** da Fig. 3.3 serem representadas como uma sequência, elas constituem na verdade um processo iterativo, onde a realização de uma **atividade** leva à revisão das **atividades** anteriores.

⁵ Neste trabalho, o termo ‘atividade’ é utilizado em três diferentes situações, diferenciadas entre si pela formatação do termo:

- Para se referir a uma **atividade** do procedimento proposto para modelagem do Sistema Supervisório e seu Objeto de Controle.
- Para se referir a uma atividade do Production Flow Schema (PFS) (detalhado na Seção 3.1.1).
- Para se referir a uma *atividade* do Diagrama de *Atividades* (detalhado na Seção 3.1.3).

O processo inicia-se com a definição do sistema a ser supervisionado (Objeto de Controle), para o qual é construído um modelo em *Production Flow Schema* (PFS) com foco nos fluxos de materiais. O passo seguinte é a definição das funções do sistema supervisor, através da construção dos *Diagramas de Casos de Uso* (Use Case Diagrams da UML).

Posteriormente, cada Caso de Uso é detalhado em um *Diagrama de Atividades* (UML). Paralelamente, definem-se as classes e os objetos que irão compor o Sistema Supervisor e seu Objeto de Controle. Constroem-se então os *Diagramas de Seqüência* (UML) e/ou de *Colaboração* (UML), onde evidenciam-se as comunicação entre os objetos para cada Caso de Uso. A partir destes diagramas, definem-se os conjuntos de atributos e métodos das classes, que são então modeladas em redes PTD-OO e organizadas em um *Diagrama de Classes* (UML). Define-se também um conjunto de estados iniciais para os objetos. Verifica-se então a coerência entre os modelos em redes PTD-OO das classes e os diagramas construídos.

Fig. 3.3. **Atividades** para modelagem do Sistema Supervisor e seu Objeto de Controle.

Para melhor explicar e ilustrar estas **atividades**, apresenta-se a seguir sua aplicação para um exemplo.

- *Exemplo:* O sistema a ser supervisionado consiste em uma linha de produção de dois produtos (P_1 e P_2), que são resultado da mistura de um produto base (B) com um corante (C_1 ou C_2). Para produção de P_1 mistura-se B e C_1 , e para produção de P_2 mistura-se B e C_2 . Um esquema das instalações é apresentado na Fig. 3.4. Para este exemplo, os modelos obtidos em cada **atividade** são apresentados na sequência.

Fig. 3.4. Exemplo de sistema a ser supervisionado.

3.1.1. Atividade 1 – Modelagem dos Fluxo de Materiais

A **Atividade 1** consiste em definir as fronteiras do Objeto de Controle do Sistema Supervisório a ser projetado através da modelagem dos fluxos de materiais no sistema.

Este modelo é construído em PFS (*Production Flow Schema*), o qual está baseado no conceito de refinamento sucessivo, onde os elementos de um modelo inicial são substituídos por modelos PFS de maior complexidade. Uma introdução ao PFS e ao processo de refinamento sucessivo pode ser encontrada em (Miyagi, 1988). Em (Villani, 2000) propõe-se sua utilização para Sistemas Híbridos, já que, até então, sua aplicação era restrita a Sistemas a Eventos Discretos. Neste caso,

diferentemente do PFS original, os arcos podem indicar fluxos de materiais tanto discretos como contínuos.

➤ *Exemplo:* Para o sistema da Fig. 3.4, o PFS do fluxo de material através do sistema é apresentado na Fig. 3.5.

Fig. 3.5. PFS para o exemplo da Fig. 3.4.

Além de proporcionar uma visão geral do processamento de materiais no sistema, esta modelagem é particularmente importante na medida que evidencia possíveis dependências em ciclo entre as entradas e saídas das diversas etapas de um processo, correspondentes às atividades do PFS. Um exemplo de dependência em ciclo é ‘a Etapa 1 recebe como entrada um produto que é a saída de uma Etapa 2, que por sua vez recebe como entrada um produto que é a saída da Etapa 1’. Este tipo de dependência entre etapas de um processo pode resultar no compartilhamento de variáveis contínuas em ciclos fechados.

3.1.2. *Atividade 2 – Definição dos Casos de Uso*

A **Atividade 2** consiste na construção dos Diagramas de Casos de Uso, que apresentam uma visão da funcionalidade do sistema (Sistema Supervisório + Objeto de Controle), identificando quais são os Casos de Uso e, para cada caso, quais são os *atores* (elementos externos: usuários, sistemas de controle de nível superior) que interagem com o sistema.

➤ *Exemplo:* Para o sistema da Fig. 3.4, uma funcionalidade do sistema supervisório é o gerenciamento da produção de P_1 e P_2 a partir de uma ordem de produção emitida por um técnico. Neste caso, o Diagrama de Caso de Uso é apresentado na Fig. 3.6.

Fig. 3.6. Diagrama de Caso de Uso para o exemplo da Fig. 3.4.

Observa-se que no exemplo apresentado, o Objeto de Controle é considerado como parte do sistema cuja funcionalidade está sendo definida, não como uma entidade externa ou um ator. O principal motivo que leva a esta especificação é que o objetivo final da modelagem não é apenas a obtenção de um modelo do Sistema Supervisório, mas também do Objeto de Controle.

3.1.3. *Atividade 3 – Construção dos Diagramas de Atividades*

A **Atividade 3** consiste em construir os Diagramas de *Atividades* de cada Caso de Uso. Estes diagramas mostram as seqüências de *atividades* realizadas pelo sistema entre o começo e o final de um Caso de Uso, ilustrando casos de paralelismo, sincronismo e concorrência. Este trabalho introduz o símbolo para indicar uma *atividade* contínua.

➤ *Exemplo:* Para o sistema da Fig. 3.4, detalha-se na Fig. 3.7 o Caso de Uso ‘Produzir P₁’.

3.1.4. *Atividade 4 – Definição de Classes e Objetos*

A **Atividade 4** consiste em definir um conjunto de objetos para compor o modelo do Sistema Supervisório e o Objeto de Controle. Estes objetos são então organizados em classes.

Fig. 3.7. Diagrama de Atividades para o Caso de Uso 'Produzir P_1 '.

De uma forma genérica, no Objeto de Controle, os principais candidatos a objetos são as entidades, os recursos e os equipamentos do sistema. No caso do Sistema Supervisório, são candidatos objetos relacionados às entidades, aos recursos ou aos equipamentos do Objeto de Controle com os quais o Sistema Supervisório interage (estes objetos são responsáveis não apenas pela interface como também por armazenar as informações necessárias sobre o seu correspondente no Objeto de Controle). Ainda para o Sistema Supervisório, considera-se como candidatos os objetos relacionados à funcionalidade do sistema, quando esta envolve mais de um sub-sistema ou entidade ou equipamento. Exemplos são objetos responsáveis pela execução de planos de produção, supervisão de processos, etc.

Além disso, observa-se que a definição dos objetos que compõem o sistema deve ser realizada considerando que cada objeto deve ter uma forte coesão interna e uma fraca conexão com os demais objetos (Paludetto, 1991). Com base nesta

premissa, apresenta-se um conjunto de 3 Regras de Decomposição a serem aplicadas na sequência, que restringem o tipo de interação entre os objetos. Inicia-se a definição do conjunto de objetos considerando a restrição imposta pela 1ª Regra. Se os objetos resultantes forem demasiadamente complexos, dificultando a sua modelagem, utiliza-se a 2ª Regra. Caso a complexidade de algum objeto ainda persista elevada, utiliza-se a 3ª Regra.

A seguir apresentam-se as regras consideradas e a sua aplicação para o exemplo da Fig. 3.4.

⇒ **1ª Regra de Decomposição** – *Os objetos resultantes da decomposição podem ter apenas interações discretas entre eles (no modelo em redes PTD-OO não existe compartilhamento de variáveis contínuas).*

➤ *Exemplo:* Considerando o Objeto de Controle, todos os candidatos a objetos têm compartilhamento de variáveis contínuas, pois os equipamentos compartilham o fluxo de base ou corante e os controladores interagem de forma contínua com as válvulas e o tanque de mistura. Como o agrupamento de todos estes equipamentos em um único objeto resultaria em uma rede de elevada complexidade, deve-se aplicar a 2ª Regra de Decomposição. Para o Sistema Supervisório são candidatos a objetos responsáveis pela interface com o Objeto de Controle: Interface V_{T2-1} , Interface V_{T2-2} , Interface V_{T3-1} e Interface V_{T3-2} (válvulas acionadas diretamente pelo sistema supervisor) e Interface C_{M1} e Interface C_{M2} . Além disso, considerando-se as possíveis receitas, são candidatos a objetos: Receita P_1 (para produção de P_1) e Receita P_2 . Finalmente são também necessários objetos no Sistema Supervisório para executar as ordens de produção – considerando que existem duas ordem de produção diferentes, tem-se os objetos: Ordem de Produção 1 e Ordem de Produção 2.

⇒ **2ª Regra de Decomposição** – *Os objetos resultantes da decomposição podem ter interações contínuas mas obrigatoriamente restritas a um intervalo de tempo (o que acontece principalmente em processos por bateladas).*

- *Exemplo:* Aplicando a 2ª Regra de Decomposição para o Objeto de Controle, são definidos como candidatos a objetos: os controladores $\underline{C}_{M1}$ e $\underline{C}_{M2}$, os misturadores $\underline{M}_1$ e $\underline{M}_2$ e o tanque $\underline{T}_1$. Para os demais tanques, o volume depende do fluxo de saída de suas válvulas, recorre-se então à 3ª Regra de Decomposição.

⇒ **3ª Regra de Decomposição** – *Os objetos resultantes da decomposição podem ter interações contínuas não restritas a um intervalo de tempo, mas não podem ter compartilhamento de variáveis em ciclos fechados.*

A imposição da 3ª Regra como restrição mínima está relacionada com o conceito de independência do objeto. Quando existe compartilhamento de variáveis contínuas em ciclo fechado, decorre que as equações dos objetos envolvidos fazem parte de um único sistema de equações e não podem ser resolvidas de forma independente. Isto interfere diretamente no conceito de independência do objeto. Nestes casos, a evolução dos estados dos objetos está de tal forma interligada que não existe razão para a definição de dois objetos distintos. O compartilhamento de variáveis é discutido no Capítulo 4, onde se enfoca sua influência na análise do modelo em redes PTD-OO.

- *Exemplo:* Aplicando a 3ª Regra de Decomposição para o restante do Objeto de Controle, são definidos como candidatos a objetos: os tanques $\underline{T}_2$, $\underline{T}_3$, $\underline{M}_1$ e $\underline{M}_2$, e as válvulas $\underline{V}_{T2-1}$, $\underline{V}_{T2-2}$, $\underline{V}_{M1-1}$ e $\underline{V}_{M2-1}$.

Os candidatos a objetos são então organizados em classes e, em seguida, definem-se os métodos e atributos de cada classe.

- *Exemplo:* Para o exemplo da Fig. 3.4, considerando os candidatos a objetos previamente apresentados, são definidas as seguintes classes para o Objeto de Controle: C_1 – *Tanque* (objetos $\underline{T}_1$, $\underline{T}_2$ e $\underline{T}_3$), C_2 – *Válvula A* (objetos $\underline{V}_{T2-1}$, $\underline{V}_{T2-2}$, $\underline{V}_{T3-1}$, $\underline{V}_{T3-2}$, $\underline{V}_{M1-1}$ e $\underline{V}_{M2-1}$), C_3 – *Válvula B* (objetos $\underline{V}_{M1-2}$ e $\underline{V}_{M2-2}$), C_4 – *Misturador* (objetos $\underline{M}_1$ e $\underline{M}_2$), C_5 – *Controlador Misturador* (objetos $\underline{C}_{M1}$ e $\underline{C}_{M2}$). Para o Sistema Supervisório tem-se as seguintes classes: C_6 – *Interface* C_M

(objetos Interface C_{M1} e Interface C_{M2}), *C₇ – Interface Válvula A* (objetos Interface V_{T2-1}, Interface V_{T2-2}, Interface V_{T3-1} e Interface V_{T3-2}), *C₈ – Receita* (objetos Receita P₁ e Receita P₂), *C₉ – Ordem de Produção* (objetos Ordem de Produção 1 e Ordem de Produção 2).

3.1.5. *Atividade 5 – Construção dos Diagramas de Seqüência e Diagramas de Colaboração*

O Diagrama de *Atividades* anteriormente construído modela a dinâmica do sistema, sem, no entanto, indicar qual o objeto responsável por cada *atividade*. Assim, uma vez definido o conjunto de objetos que compõem o sistema, o passo seguinte é definir quais são as comunicações necessárias entre os objetos para realizar as *atividades* de um Caso de Uso. Neste caso, podem ser utilizados os Diagramas de Seqüência e/ou os Diagramas de Colaboração. O Diagrama de Seqüência enfatiza a ordem cronológica das chamadas de métodos, enquanto o Diagrama de Colaboração evidencia qual é o objeto responsável por enviar cada chamada de método. Observa-se contudo, que, em ambos os casos, um diagrama apresenta uma possível evolução do sistema, isto é, um *cenário*⁶, não explicitando paralelismo, sincronismo ou conflito.

De acordo com a notação UML, nestes diagramas utiliza-se o símbolo $\longrightarrow$ para indicar uma interação discreta síncrona. Para indicar uma interação contínua (que correspondem ao compartilhamento de variáveis contínuas entre os objeto), introduz-se o símbolo $---\longrightarrow$ e adiciona-se a letra I ou F à numeração. A letra I indica o início da interação contínua e a letra F o final. Esta notação é válida, seja para o Diagrama de Seqüência, seja para o Diagrama de Colaboração.

⁶ Nesta tese, o termo ‘cenário’ é utilizado no lugar do termo em inglês ‘scenario’ e indica ‘uma seqüência específica de ações que ilustram um comportamento’ (Booch, Rumbaugh; Jacobson, 2000), correspondendo portanto a uma visão *dinâmica* do mundo. Esta tradução é adotada para manter a conformidade com a bibliografia em português sobre orientação a objetos (ex.: tradução para o português do livro *The Unified Modelling Language user guide* (Booch, Rumbaugh; Jacobson, 1999)). Observa-se, no entanto, que este significado difere dos significados comumente atribuídos a ‘cenário’ na língua portuguesa, entre os quais se encontram por exemplo ‘paisagem’, ‘panorama’ e ‘decoração de teatro’, que estão associados a uma visão *estática* do mundo.

- *Exemplo:* Para o exemplo da Fig. 3.4, considerando os objetos e a seqüência de *atividades* previamente definida, é construído o Diagrama de Seqüência (Fig. 3.8) e o Diagrama de Colaboração (Fig. 3.9) para o Caso de Uso ‘Produzir P_1 ’. Nestas figuras considera-se apenas a produção de um lote de P_1 em M_1 .

Comunicações discretas

- 1: Ordem de Produção solicita produção de P_1 a Receita P_1
- 2: Receita P_1 solicita M_1 à Interface C_{M1}
- 3: Interface C_{M1} solicita M_1 ao controlador C_{M1}
- 4: Receita P_1 envia solicitação de abertura de V_{T2-1} à Interface V_{T2-1}
- 5: Interface V_{T2-1} abre V_{T2-1}
- 6: C_{M1} abre V_{M1-1}
- 7: C_{M1} abre V_{M1-2}
- 15: C_{M1} finaliza o carregamento de corrente fechando V_{M1-2}
- 16: C_{M1} informa fim de carregamento de corrente a Interface C_{M1}
- 17: Interface C_{M1} informa fim de carregamento de corrente a Receita P_1
- 18: Receita P_1 envia solicitação de fechamento de V_{T2-1} à Interface V_{T2-1}
- 19: Interface V_{T2-1} fecha V_{T2-1}
- 24: C_{M1} finaliza o carregamento de base fechando V_{M1-1}
- 28: C_{M1} inicia mistura
- 29: C_{M1} finaliza mistura e inicia a esvaziar
- 32: C_{M1} informa fim da produção do lote à Interface C_{M1}
- 33: Interface C_{M1} informa fim da produção do lote à Receita P_1

Comunicações contínuas

- 8: T_1 usa vazão de saída de V_{M1-1} p/ determinar seu volume
- 9: C_{M1} usa vazão de saída de V_{M1-1} p/ determinar volume de corrente
- 10: M_1 usa vazão de saída de V_{M1-1} p/ determinar seu volume
- 11: V_{M1-2} usa vazão de saída de V_{T2-1} p/ determinar sua vazão
- 12: T_2 usa vazão de saída de V_{T2-1} p/ determinar seu volume
- 13: C_{M1} usa vazão de saída de V_{M1-2} p/ determinar volume de base
- 14: M_2 usa vazão de saída de V_{M1-1} p/ determinar seu volume
- 30: C_{M1} usa volume de M_1 p/ determinar fim do esvaziamento

Fig. 3.8. Diagrama de Seqüência para o Caso de Uso ‘Produzir P_1 ’.

Fig. 3.9. Diagrama de Colaboração para o Caso de Uso 'Produzir P₁'.

A partir da construção destes diagramas, é identificado o conjunto de métodos e atributos necessários a cada classe.

➤ *Exemplo:* Para o exemplo da Fig. 3.4, são definidos os seguintes métodos e atributos (Fig. 3.10).

C₁ - Tanque Vol, I ₁ , I ₂ q _{I1.C2} , q _{I2.C2} , q _{In}	C₄ - Misturador I ₁ , I ₂ Vol q _{I1.C2} , q _{I2.C3} Iniciar mistura Finalizar mistura Esvaziar Finalizar mistura e esvaziar	C₅ - Controlador Misturador M, K _{BM} , θ _M , pc, Vol _{P1} , Vol _{P2} , I ₁ , I ₂ , I ₃ Vol _{I1.C4} , q _{I2.C2} , q _{I3.C3} Iniciar produção de lote Informar fim do carregamento de corante Finalizar produção de lote
C₂ - Válvula A q Informar fim de fluxo Abrir válvula Fechar válvula	C₇ - Interface Válvula A Abrir válvula Fechar válvula	C₆ - Interface C_M I ₁ Iniciar produção de lote Informar fim do carregamento de corante Finalizar produção de lote
C₃ - Válvula B I ₁ , I ₂ q q _{I1.C2} , q _{I2.C2} Informar fim de fluxo Abrir válvula Fechar válvula	C₉ - Ordem de Produção I ₁ , I ₂ N _{P1} , N _{P2} Receber ordem	C₈ - Receita N, I ₁ , I ₂ ; I ₃ , I ₄ Iniciar produção de P Finalizar produção de P

Fig. 3.10. Classes para o exemplo da Fig. 3.4.

Além disso, é possível também detalhar o Diagrama de *Atividades* que passa agora a incluir não apenas as *atividades* realizadas por equipamentos do sistema, mas também *atividades* referentes às comunicações entre os objetos, evidenciando casos de paralelismo, sincronismo e conflito no fluxo de controle.

- *Exemplo:* Para o exemplo da Fig. 3.4, o Diagrama de Atividades da Fig. 3.7 é detalhado na Fig. 3.11.

Fig. 3.11. Detalhamento do Diagrama de Atividades da Fig. 3.7.

3.1.6. Atividade 6 – Modelagem das Classes em Redes PTD-OO e Construção dos Diagramas de Classes

A modelagem das classes em redes PTD-OO é realizada de acordo com o definido no Capítulo 2.

O modelo das classes em redes PTD-OO deve ser consistente com os demais diagramas. Neste sentido, tem-se que:

- Cada atividade do modelo em PFS é realizada por um objeto de uma classe do Objeto de Controle. Estas atividades correspondem a lugares (no caso de atividades contínuas) ou transições (no caso de atividades discretas) dos modelos em redes PTD-OO das respectivas classes. Os fluxos de materiais discretos correspondem a chamada de métodos entre os modelos destas classes, enquanto os fluxos de materiais contínuos correspondem ao compartilhamento de variáveis contínuas.
- As *atividades* dos Diagramas de *Atividades* de um Caso de Uso correspondem a lugares (no caso de *atividades* contínuas) ou transições (no caso de *atividades* discretas) do modelo em redes PTD-OO das classes do Sistema Supervisório ou do Objeto de Controle.
- As comunicações entre objetos modeladas nos Diagramas de Sequência e de Colaboração correspondem a chamadas de métodos ou compartilhamento de variáveis entre as respectivas classes.

➤ *Exemplo:* Para o exemplo da Fig. 3.4, os modelos em redes PTD-OO são apresentados a seguir (Fig. 3.12, Fig. 3.13, Fig. 3.14, Fig. 3.15, Fig. 3.16, Fig. 3.17, Fig. 3.18, Fig. 3.19 e Fig. 3.20). Para facilitar a compreensão dos modelos, as redes são apresentadas com uma das possíveis marcações (do ponto de vista discreto) para um objeto daquela classe.

Fig. 3.12. Modelo em rede PTD-OO da classe $C_1 - \text{Tanque}$.

Fig. 3.13. Modelo em rede PTD-OO da classe C₂ – Válvula A. Fig. 3.14. Modelo em rede PTD-OO da classe C₃ – Válvula B. Fig. 3.15. Modelo em rede PTD-OO da classe C₄ – Misturador.

Fig. 3.16. Modelo em rede PTD-OO da classe C₅ – Controlador Misturador. Fig. 3.17. Modelo em rede PTD-OO da classe C₆ – Interface C_M.

Fig. 3.18. Modelo em rede PTD-OO da classe C_7 – Interface Válvula A. Fig. 3.19. Modelo em rede PTD-OO da classe C_8 – Receita. Fig. 3.20. Modelo em rede PTD-OO da classe C_9 – Ordem de Produção.

É importante salientar que, no que se refere à construção do Diagrama de Classes, seu objetivo é mostrar relações estruturais entre as classes. Destas, as relações mais importantes são de generalização/especificação e de decomposição/

composição. A utilização destas relações para construção do modelo em redes PTD-OO do Sistema Supervisório e seu Objeto de Controle é abordada na Seção 3.2.

A última parte da **Atividade 6** é a definição (parcial ou completa) do estado inicial do sistema, ou de um conjunto de estados iniciais. Esta definição visa impor restrições que garantam a coerência do modelo completo do sistema, isto é, da composição dos estados dos objetos.

Em cada possível estado inicial, deve-se especificar, para cada objeto, qual é a marcação inicial da rede PTD-OO do ponto de vista discreto ($m_{j,i}$ do objeto $O_{j,i}$). No que se refere às variáveis contínuas (instância $X_{j,i}$ de X_i para o objeto $O_{j,i}$), os valores iniciais das variáveis externas (X_{ext_i}) de cada objeto não são definidos, enquanto os valores das variáveis compartilhadas (X_{comp_i}) e internas (X_{int_i}) podem ou não serem definidos. Neste segundo caso o estado inicial do sistema está apenas parcialmente definido. Um valor inicial não definido é designado como *ind*, de indefinido.

➤ *Exemplo:* Para o exemplo da Fig. 3.4, apresenta-se uma possível definição do estado inicial do sistema. Um exemplo de coerência na composição dos objetos que este estado inicial deve garantir é que se o estado da válvula $\underline{V_{T2-1}}$ (do Objeto de Controle) é ‘Fechada’, seu fluxo de saída (q) deve ser zero e o respectivo objeto $\underline{Interface_V_{T2-1}}$ (do Sistema Supervisório) também deve estar no estado ‘Fechada’. Uma vez que o valor das variáveis externas é por definição *ind*, estas variáveis são omitidas dos vetores $X_{j,i}$ no estado inicial apresentado a seguir:

- $O_{1,1} = \underline{I_1}$; $X_{1,1} = \{\text{Vol} = \text{ind}, l_1 = \underline{V_{M1-1}}, l_2 = \underline{V_{M2-1}}\}$; $m_{1,1} = \{p_{1_1}\}$;
- $O_{2,1} = \underline{I_2}$; $X_{2,1} = \{\text{Vol} = \text{ind}, l_1 = \underline{V_{T2-1}}, l_2 = \underline{V_{T2-2}}\}$; $m_{2,1} = \{p_{1_1}\}$;
- $O_{3,1} = \underline{I_3}$; $X_{3,1} = \{\text{Vol} = \text{ind}, l_1 = \underline{V_{T3-1}}, l_2 = \underline{V_{T3-2}}\}$; $m_{3,1} = \{p_{1_1}\}$;
- $O_{1,2} = \underline{V_{T2-1}}$; $X_{1,2} = \{q = 0\}$; $m_{1,2} = \{p_{1_2}, p_{2_2}\}$;
- $O_{2,2} = \underline{V_{T2-2}}$; $X_{2,2} = \{q = 0\}$; $m_{2,2} = \{p_{1_2}, p_{2_2}\}$;
- $O_{3,2} = \underline{V_{T3-1}}$; $X_{3,2} = \{q = 0\}$; $m_{3,2} = \{p_{1_2}, p_{2_2}\}$;
- $O_{4,2} = \underline{V_{T3-2}}$; $X_{4,2} = \{q = 0\}$; $m_{4,2} = \{p_{1_2}, p_{2_2}\}$;
- $O_{5,2} = \underline{V_{M1-1}}$; $X_{5,2} = \{q = 0\}$; $m_{5,2} = \{p_{1_2}, p_{2_2}\}$;
- $O_{6,2} = \underline{V_{M2-1}}$; $X_{6,2} = \{q = 0\}$; $m_{6,2} = \{p_{1_2}, p_{2_2}\}$;
- $O_{1,3} = \underline{V_{M1-2}}$; $X_{1,3} = \{q = 0, l_1 = \underline{V_{T2-1}}, l_2 = \underline{V_{T3-1}}\}$; $m_{1,3} = \{p_{1_3}, p_{2_3}\}$;
- $O_{2,3} = \underline{V_{M2-2}}$; $X_{2,3} = \{q = 0, l_1 = \underline{V_{T2-2}}, l_2 = \underline{V_{T3-2}}\}$; $m_{2,3} = \{p_{1_3}, p_{2_3}\}$;

- $O_{1.4} = \underline{M_1}$; $X_{1.4} = \{Vol = 0, l_1 = \underline{V_{M1-1}}, l_2 = \underline{V_{M1-2}}\}$; $m_{1.4} = \{p_{1.4}\}$;
- $O_{2.4} = \underline{M_2}$; $X_{2.4} = \{Vol = 0, l_1 = \underline{V_{M2-1}}, l_2 = \underline{V_{M2-2}}\}$; $m_{2.4} = \{p_{1.4}\}$;
- $O_{1.5} = \underline{C_{M1}}$; $X_{1.5} = \{M = ind, K_M = ind, M = ind, pc = ind, Vol_{P1} = 0, Vol_{P2} = 0, l_1 = \underline{M_1}, l_1 = \underline{V_{M1-1}}, l_2 = \underline{V_{M1-2}}\}$; $m_{1.5} = \{p_{1.5}\}$;
- $O_{2.5} = \underline{C_{M2}}$; $X_{2.5} = \{M = ind, K_M = ind, M = ind, pc = ind, Vol_{P1} = 0, Vol_{P2} = 0, l_1 = \underline{M_1}, l_1 = \underline{V_{M2-1}}, l_2 = \underline{V_{M2-2}}\}$; $m_{2.5} = \{p_{1.5}\}$;
- $O_{1.6} = \underline{Interface C_{M1}}$; $X_{1.6} = \{l_1 = \underline{C_{M1}}\}$; $m_{1.6} = \{p_{1.6}\}$;
- $O_{2.6} = \underline{Interface C_{M2}}$; $X_{2.6} = \{l_1 = \underline{C_{M2}}\}$; $m_{2.6} = \{p_{1.6}\}$;
- $O_{1.7} = \underline{Interface V_{T2-1}}$; $X_{1.7} = \{l_1 = \underline{V_{T2-1}}\}$; $m_{1.7} = \{p_{1.7}\}$;
- $O_{2.7} = \underline{Interface V_{T2-2}}$; $X_{2.7} = \{l_1 = \underline{V_{T2-2}}\}$; $m_{2.7} = \{p_{1.7}\}$;
- $O_{3.7} = \underline{Interface V_{T3-1}}$; $X_{3.7} = \{l_1 = \underline{V_{T3-1}}\}$; $m_{3.7} = \{p_{1.7}\}$;
- $O_{4.7} = \underline{Interface V_{T3-2}}$; $X_{4.7} = \{l_1 = \underline{V_{T3-2}}\}$; $m_{4.7} = \{p_{1.7}\}$;
- $O_{1.8} = \underline{Receita P_1}$; $X_{1.8} = \{N = ind, l_1 = \underline{Interface C_{M1}}, l_2 = \underline{Interface C_{M2}}, l_3 = \underline{Interface V_{T2-1}}, l_4 = \underline{Interface V_{T2-2}}\}$; $m_{1.8} = \{p_{1.8}\}$;
- $O_{2.8} = \underline{Receita P_2}$; $X_{2.8} = \{N = ind, l_1 = \underline{Interface C_{M1}}, l_2 = \underline{Interface C_{M2}}, l_3 = \underline{Interface V_{T3-1}}, l_4 = \underline{Interface V_{T3-2}}\}$; $m_{2.8} = \{p_{1.8}\}$;
- $O_{1.9} = \underline{Ordem de Produção 1}$; $X_{1.9} = \{N_{P1} = 0, N_{P2} = 0, l_1 = \underline{Receita P_1}, l_2 = \underline{Receita P_2}\}$; $m_{1.9} = \{p_{1.9}\}$;
- $O_{2.9} = \underline{Ordem de Produção 2}$; $X_{2.9} = \{N_{P1} = 0, N_{P2} = 0, l_1 = \underline{Receita P_1}, l_2 = \underline{Receita P_2}\}$; $m_{2.9} = \{p_{1.9}\}$;

3.1.7. Atividade 7 – Verificação dos Modelos

Modelo em redes PTD-OO e Diagramas de Seqüência e/ou Colaboração

Conforme apresentado anteriormente, os modelos das classes e os Diagramas de Seqüência e Colaboração construídos devem ser consistentes. Para que esta consistência seja verificada, tem-se que:

- Cada comunicação discreta deve corresponder a uma chamada de método associada a uma transição.
- Cada comunicação contínua deve corresponder a uma variável contínua compartilhada.

➤ *Exemplo:* Para o exemplo da Fig. 3.4, a relação entre o Diagrama de Seqüência da Fig. 3.8 e as respectivas transições ou variáveis compartilhadas é apresentada na Fig. 3.21.

Fig. 3.21. Correspondência entre o Diagrama de Seqüência e o modelo em redes PTD-OO.

Modelo em redes PTD-OO e Diagrama de Atividades

Os Diagramas de *Atividades* construídos anteriormente são convertidos para um modelo em redes de Petri. O objetivo desta conversão é identificar quais são os lugares e transições nos modelos em redes PTD-OO das classes que executam as *atividades* do diagrama e, assim, verificar se ambos estão consistentes.

Para a conversão são consideradas as seguintes regras:

- Cada *atividade* discreta corresponde a uma transição. Entre duas *atividades* discretas subsequentes é inserido um lugar (Fig. 3.22).

Fig. 3.22. Conversão do Diagrama de Atividades para redes de Petri – atividades discretas.

- Cada *atividade* contínua corresponde a um lugar. Entre duas *atividades* contínuas é necessário inserir uma transição (Fig. 3.23).

Fig. 3.23. Conversão do Diagrama de *Atividades* para redes de Petri – *atividades* contínuas.

- Cada barra de sincronização corresponde a uma transição. Entre as transições correspondentes às *atividades* discretas anteriores à barra de sincronização e a transição correspondente a própria barra, são inseridos lugares. O mesmo é válido para as *atividades* discretas posteriores à barra de sincronização. Entre as *atividades* contínuas (correspondentes a lugares) e a barra de sincronização não é inserido nenhum elemento no modelo em redes de Petri (Fig. 3.24).

Fig. 3.24. Conversão do Diagrama de *Atividades* para redes de Petri – barras de sincronização.

- Uma *atividade* seguida por um losango de decisão com n saídas é representada por um lugar com n transições de saída. Quando, após o losango de decisão, tem-se uma *atividade* discreta, é inserido um lugar no modelo em redes de Petri entre a transição correspondente à saída do losango e a transição correspondente a *atividade* discreta. Quando, após o losango de decisão, tem-se uma *atividade* contínua, não são inseridos novos elementos no modelo em redes de Petri (Fig. 3.25).

Fig. 3.25. Conversão do Diagrama de *Atividades* para redes de Petri – losango de decisão.

- Uma vez construído o modelo em redes de Petri, este pode ser simplificado: uma sequência de transição e lugar (ou lugar e transição) pode ser eliminada nos casos em que estes elementos não correspondem a nenhuma *atividade* do Diagrama de *Atividades* e, além disso, enquadram-se em uma das seguintes situações:

- o Possuem apenas um arco de entrada e um de saída (Fig. 3.26).

Fig. 3.26. Conversão do Diagrama de *Atividades* para redes de Petri – simplificação (tipo 1).

- o O lugar possui um arco de entrada e um de saída, enquanto que a transição, um arco de entrada e vários de saída (Fig. 3.27).

Fig. 3.27. Conversão do Diagrama de *Atividades* para redes de Petri – simplificação (tipo 2).

- O lugar possui um arco de entrada e um de saída, enquanto que a transição, um arco de saída e vários de entrada (Fig. 3.28).

Fig. 3.28. Conversão do Diagrama de Atividades para redes de Petri – simplificação (tipo 3).

Uma vez construído o modelo em redes de Petri de um Diagrama de Atividades, deve-se estabelecer a relação entre os lugares e transições deste modelo e os lugares e transições do modelo em redes PTD-OO dos objetos. O modelo em redes de Petri de um Diagrama de Atividades é na verdade uma parte da rede global construída através do desdobramento da rede das classes. Um exemplo é apresentado a seguir.

- *Exemplo:* Para o exemplo da Fig. 3.4, apresenta-se na Fig. 3.29 a conversão do Diagrama de Atividades da Fig. 3.11.

3.2. Relações entre classes para redes PTD-OO

Em sistemas complexos, de grande porte, uma modelagem ‘plana’, onde todos os objetos e classes devem ser completamente identificados e todas as suas relações explicitadas, não é recomendada. Na prática, isto é muitas vezes inviável, devido ao número de variáveis envolvidas. Nestes casos, a modelagem deve ser feita de forma progressiva, segundo estratégias do tipo *bottom-up*, *top-down* ou ainda uma combinação de ambas. Em estratégias do tipo *bottom-up*, o sistema a ser modelado é dividido em partes que são modeladas separadamente e sucessivamente integradas até a obtenção do modelo completo do sistema. Na decomposição *top-down*, parte-se de uma descrição geral do sistema, que é decomposta e sucessivamente detalhada até a obtenção de um modelo com o nível de descrição necessário (Azzopardi; Holding, 1997).

Fig. 3.29. Conversão em redes de Petri do Diagrama de Atividades da Fig. 3.11.

Neste sentido, as relações entre classes propostas pela orientação a objetos são particularmente importantes. Destacam-se aqui dois tipos principais de relações: a *decomposição/composição* e a *generalização/especialização*.

3.2.1. Decomposição/Composição

A *decomposição/composição* estabelece uma relação do tipo “é parte de” entre as partes resultantes da decomposição (hierarquicamente inferiores) e o nível hierarquicamente superior (Booch, 1994). A relação de *agregação* é semelhante a

relação de decomposição/composição. Neste caso, no entanto, a ‘vida’ dos objetos que compõem cada uma das *partes* não está limitada à vida do *todo*. Além disso, um objeto pode participar de mais de uma relação de agregação, isto é, pode pertencer a mais de um todo.

Nos modelos em redes PTD-OO, ambas a composição e a agregação são realizadas através da fusão de transições correspondentes às chamadas de métodos entre as classes.

- *Exemplo:* Para o exemplo da Fig. 3.4, uma opção é definir uma classe responsável pelo fornecimento de corante (C_{10} - *Estação de Corante*). Esta classe é resultado da composição da classe C_1 - *Tanque* com a classe C_2 - *Válvula A*. Cada objeto de C_{10} contém um objeto de C_1 e dois objetos de C_2 . Esta relação é representada no Diagrama de Classes da Fig. 3.30. O modelo em redes PTD-OO da classe resultante é apresentada na Fig. 3.31.

Fig. 3.30. Diagrama de classes para a composição da classe C_{10} - *Estação de Corante*.

Fig. 3.31. Modelo em rede PTD-OO da classe C_{10} - *Estação de Corante*

Uma vez construído o modelo da classe resultante da composição, a rede resultante pode ser simplificada de forma a eliminar informações duplamente representadas.

Uma forma de determinar se duas informações, cada uma das quais representadas por um lugar (ou um conjunto de lugares), são equivalentes é verificar se correspondem a invariante de lugares. Outras regras para redução do modelo se encontram em Cardoso; Valette (1997). Observa-se que estas regras são aplicáveis desde que os elementos envolvidos não estejam relacionados com a dinâmica contínua da classe (com sistemas de equações, funções de habilitação e de junção). Um exemplo é apresentado a seguir.

- *Exemplo:* No modelo da Fig. 3.31 os lugares p_{7_10} e p_{12_10} não contém nenhuma informação relevante. Para cada um destes lugares, considerando a marcação inicial do sistema (1,0,0,0,0,0,1,0,1,0,0,1,0,0,1) tem-se os seguintes invariantes: ' $m(p_{7_10}) = m(p_{1_10}) + m(p_{2_10})$ ' e ' $m(p_{12_10}) = m(p_{1_10}) + m(p_{3_10})$ '. Ambos os lugares podem portanto serem eliminados sem interferir na dinâmica do restante da rede. Além disso, quando o tanque está vazio, ambas as válvulas ficam sem fluxo. Se não existe interesse na representação de forma distinta destes três estados, os lugares p_{4_10} , p_{5_10} e p_{6_10} também podem ser eliminados (invariante: ' $m(p_{4_10}) + m(p_{5_10}) + 2*m(p_{6_10}) = m(p_{8_10}) + m(p_{11_10}) + m(p_{13_10}) + m(p_{14_10})$ '). Uma vez eliminados p_{4_10} , p_{5_10} , p_{6_10} , p_{7_10} e p_{12_10} , as seqüências de lugar-transição p_{2_10} - t_{2_10} e p_{3_10} - t_{3_10} possuem apenas um arco de entrada e um de saída e não representam nenhuma atividade, podendo portanto ser eliminadas. A rede resultante é apresentada na Fig. 3.32.

Fig. 3.32. Simplificação do modelo da classe C_{10} – Estação de Corante

O inverso da relação de composição é a decomposição. C_{10} é resultado da *composição* de C_2 e C_1 . Similarmente, C_1 e C_2 podem ser vistos como resultado da decomposição de C_{10} . A decomposição de uma classe é realizada através da identificação de invariantes de lugares correspondentes a diferentes equipamentos. Um exemplo é apresentado a seguir.

➤ *Exemplo:* Partindo do modelo de C_{10} apresentado na Fig. 3.32, identificam-se os seguintes invariantes: ‘ $m(p_{9_10}) + m(p_{10_10}) + m(p_{11_10}) = 1$ ’ e ‘ $m(p_{14_10}) + m(p_{15_10}) + m(p_{16_10}) = 1$ ’, correspondentes aos estados das duas válvulas. Uma decomposição simples é conseguida simplesmente associando-se chamadas de métodos à t_{5_10} , t_{8_10} , t_{9_10} , t_{12_10} . Um posterior detalhamento é necessário se quisermos que t_{5_10} e t_{8_10} sejam associados a um único método e que o estado tanque vazio seja representado explicitamente. Neste caso, recaímos nos modelos das classes C_1 e C_2 representados na Fig. 3.12 e Fig. 3.13.

Além da obtenção de modelos com o nível necessário de detalhamento, o uso da relação de decomposição/composição também é particularmente interessante nos casos em que existe compartilhamento de variáveis contínuas em ciclos fechados

entre vários equipamentos. Nestes casos, a classe correspondente ao ciclo fechado pode ser definida como a composição de diversas classes intermediárias compartilhando variáveis entre si. Estas classes intermediárias são modeladas separadamente ou podem ser provenientes de uma bibliotecas de classes, evitando assim o problema de complexidade. Diversos exemplos são apresentados para os estudos de caso dos Capítulos 5, 6 e 7.

3.2.2. *Generalização/Especialização*

A *generalização/especialização*, também chamada de herança, corresponde a uma relações do tipo “*é um de*”. Ela evidencia uma estrutura e comportamentos em comum entre classes dentro do sistema (Booch, 1994). Na especialização, a ‘classe filha’ herda os métodos e atributos da ‘classe mãe’ e, além destes, possui novos métodos e atributos. Um dos principais objetivos da generalização/especialização é contribuir para a reutilização de códigos durante a programação. Neste sentido, quando uma ‘classe filha’ é criada, não é necessário copiar todos os métodos e atributos da ‘classe mãe’.

Apesar de algum autores, como Lakos (1995), definirem a aplicação do conceito de herança para redes de Petri como uma forma de reutilização de modelos, onde, de forma semelhante ao código na programação, o modelo da classe mãe não é copiado na definição do modelo da classe filha, acredita-se que tal conceito não se aplica a este trabalho.

A principal motivação para tanto é que, dentro do escopo deste trabalho, a compreensão do modelo através da visualização da marcação da rede de um objeto é particularmente importante, pois, conforme será apresentado no Capítulo 4, a análise dos modelos é realizada através de procedimentos não automáticos. Não existe interesse na apresentação do modelo da ‘classe filha’ sem o correspondente modelo da ‘classe mãe’ e, portanto, não existe sentido na definição da relação de herança com a finalidade de reutilização de modelos de redes PTD-OO.

No entanto, se considerarmos todo o processo de desenvolvimento de Sistemas Supervisórios Híbridos, a relação de generalização/especialização apresenta interesse para a 2ª Fase (Fig. 1.5 do Capítulo 1 e Fig. 3.2, deste capítulo) onde o modelo em redes PTD-OO é traduzido para uma linguagem de programação, possibilitando a

reutilização de código. Neste sentido, a identificação de estruturas e comportamentos em comum entre as classes pode ser considerada relevante.

Em redes PTD-OO considera-se que uma ‘classe filha’ é a especialização de uma ‘classe mãe’, quando a ‘classe filha’ contém todos os elementos da rede (lugares, transições, variáveis, funções de habilitação, etc.) da ‘classe mãe’ e, além destes, possui alguns elementos adicionais. Um exemplo é apresentado a seguir.

➤ *Exemplo:* Para o exemplo da Fig. 3.4 e para os modelos de classes apresentados na Seção 3.1.6, pode-se considerar as classes C_2 – Válvula A e C_3 – Válvula B, como especialização de uma única classe C_{11} – Válvula. Esta relação é apresentada no Diagrama de Classes da Fig. 3.33. O modelo da classe C_{11} é apresentado na Fig. 3.34. A classe C_2 (Fig. 3.13) possui como elemento adicional a função de junção associada a t_{3_2} . A classe C_3 (Fig. 3.14) possui como elementos adicionais as variáveis dos vetores X_{int_3} e X_{ext_3} e o sistema de equações associado a p_{5_3} .

Fig. 3.33. Diagrama de classes para a especialização da classe C_{11} – Válvula.

Fig. 3.34. Modelo da classe C_{11} , resultante da generalização das classes C_2 e C_3 .

3.3. (Sistema de Controle Local + Planta) x Planta Controlada

O nível de detalhamento e de precisão dos modelos do Objeto de Controle depende das funções associadas ao Sistema Supervisório. Um aspecto particularmente importante deste detalhamento é a distinção entre o modelo do

Sistema de Controle Local e o modelo da Planta (Fig. 1.6 do Capítulo 1). Neste caso, existem duas opções a serem adotadas: a modelagem do comportamento do Sistema de Controle Local separadamente do comportamento da Planta e a modelagem do comportamento da *Planta controlada*. A escolha de uma ou outra opção depende da especificação do Sistema de Controle Local em relação à precisão desejada para o modelo do Objeto de Controle. Um exemplo é apresentado a seguir.

- *Exemplo:* Para o exemplo da Fig. 3.4, o modelo da classe C_2 - *Válvula A* apresentado na Fig. 3.13 considera o fluxo de saída do tanque T_1 , quando a válvula está aberta, como sendo constante. Este modelo é na verdade o modelo da válvula controlada. A medida que o volume do tanque T_1 varia, a pressão na entrada da válvula varia e, para se manter o fluxo constante, deve-se variar a abertura da válvula, o que indica a existência de um Sistema de Controle Local. Um possível modelo onde o comportamento da válvula é apresentado separadamente do modelo do Sistema de Controle Local é ilustrado na Fig. 3.35. Neste caso, a classe C_{12} - *Válvula A (Modelo 2)* pode ser resultado da composição de duas classes distintas (*Controlador PID* e *Válvula Proporcional*) que compartilham variáveis em ciclo fechado. O fluxo de saída da válvula (q) é proporcional à posição da válvula (P) e ao fluxo máximo possível ($q_{\max}$), que é determinado em função do volume do tanque. K_p é a constante de proporcionalidade. P é determinada por um controlador local do tipo PID (constantes K_0 , K_1 , K_2 e K_3), em função do erro (E) de q em relação ao valor desejado ($q_{\text{teor}} = 10$). A utilização do modelo com fluxo de saída constante (Planta controlada - classe C_2) indica que o eventual erro (E) apresentado pela variável q em relação ao valor de referência ($q_{\text{teor}} = 10$) não foi considerado relevante durante o processo de modelagem.

Fig. 3.35. Modelo em rede PTD-OO da classe C₁₂ – Válvula A (Modelo 2).

3.4. Observações

Este capítulo apresentou um procedimento para obtenção do *modelo para validação* do Sistema Supervisório e seu Objeto de Controle. O procedimento proposto está dividido em **atividades**, onde cada **atividade** corresponde à construção de um conjunto de diagramas cuja finalidade é auxiliar e documentar a obtenção de um *modelo para validação* consistente com os requisitos do Sistema Supervisório. As **atividades** propostas são:

- **Atividade 1** – Modelagem do Fluxo de Materiais (em PFS): define as fronteiras do Objeto de Controle e auxilia, durante a **Atividade 4**, na identificação das interações entre possíveis candidatos a objetos.
- **Atividade 2** – Definição dos Casos de Uso: representa em Diagramas de Casos de Usos as funcionalidades do Sistema Supervisório e quais os elementos externos que interagem com o Sistema Produtivo em cada Caso de Uso.
- **Atividade 3** – Construção dos Diagramas de *Atividades*: detalha os Casos de Uso da **Atividade 2**.
- **Atividade 4** – Definição de Classes e Objetos: especifica um conjunto de classes e objetos que realizem as *atividades* descritas dos diagramas da **Atividade 3**, baseando-se nas possíveis interações entre os candidatos a objetos.

- **Atividade 5** – Construção dos Diagramas de Seqüência e/ou de Colaboração: representam as interações entre os objetos definidos na **Atividade 4** para cada Caso de Uso definido na **Atividade 2**.
- **Atividade 6** – Modelagem das Classes em redes PTD-OO e Construção dos Diagramas de Classes: utiliza as informações presentes nos diagramas das **Atividades 1, 3 e 5** para obtenção de um modelo em redes PTD-OO para cada classe definida na **Atividade 4**. Observa-se que o modelo gerado nesta **atividade** é o *modelo para validação* do Sistema Supervisório e de seu Objeto de Controle.
- **Atividade 7** – Verificação dos Modelos: verifica se os modelos em redes PTD-OO (**Atividade 6**) e os modelos das **Atividades 3 e 5** são efetivamente consistentes.

A utilização do PFS e dos Diagramas da UML visa auxiliar na modelagem em redes PTD-OO de Sistemas Produtivos onde os processos e os recursos utilizados apresentam uma elevada complexidade. Neste sentido, o PFS e os diagramas da UML permitem, através de suas visões complementares, o enfoque de diferentes aspectos do comportamento e da estrutura do sistema, induzindo assim a uma modelagem gradual. Por outro lado, os modelos em redes PTD-OO são eficazes como ‘elo’ de ligação entre os diferentes diagramas, garantindo sua consistência. Estas vantagens da utilização em conjunto de modelos baseados em redes de Petri e UML já haviam sido identificada em diversos trabalhos para o caso de Sistemas a Eventos Discretos, como por exemplo em Baresi; Pezzè (2001), Delatour (2003), Elkoutbi; Keller (2000) e Giese; Graf; Wirtz (1999).

No que se refere à natureza híbrida do modelo construído, a UML e as redes PTD-OO complementam-se. Enquanto as redes PTD-OO explicitam os estados de um objeto associados a uma dinâmica contínua, a UML, através dos Diagramas de Colaboração, possibilita a representação, de uma forma explícita, da interação contínua entre os objetos. A utilização destes diagramas é também explorada no Capítulo 4, para análise do modelo.

Uma outra vantagem é que, sendo a UML uma linguagem bastante conhecida, não apenas no meio acadêmico mas também na indústria, a sua utilização facilita e

auxilia na comunicação entre pessoas de diferentes áreas que estejam relacionadas ao Sistema Supervisório.

Este capítulo tratou ainda de alguns aspectos relacionados à definição de relações estruturais entre classes, considerando em especial as relações de composição/decomposição e generalização/especialização. Enquanto a primeira é particularmente importante para a construção do modelo em redes PTD-OO de forma progressiva, utilizando estratégias do tipo *bottom-up* e *top-down*, a segunda é importante para a 2ª Fase do desenvolvimento de Sistemas Supervisórios Híbridos (Fig. 1.5 do Capítulo 1). Neste sentido, observa-se que a aplicação do conceito de generalização/especialização às redes PTD-OO, definida na Seção 3.3.2 pode ser revista de acordo com o procedimento estabelecido para tradução dos modelos para uma linguagem de programação. No entanto, a revisão deste conceito não altera os modelos das classes que compõem o sistema (a menos do Diagrama de Classes), nem os resultados obtidos na análise dos modelos.

Finalmente, no que se refere à modelagem do Sistema de Controle Local separadamente da Planta, esta é particularmente interessante para os casos em que o Sistema de Controle Local pode ser projetado simultaneamente e de forma interativa com o Sistema Supervisório.

Nestes casos, uma vez construído um modelo do Sistema Supervisório, dos Sistemas de Controle Local e da Planta, pode-se utilizar este modelo para detectar eventos do sistema que interfiram no desempenho dos Sistemas de Controle Local (especialmente nos controladores contínuos), causando perturbações nas variáveis controladas. Estes eventos podem ser discretos ou corresponderem a ultrapassagem de limites (*thresholds*) por variáveis contínuas.

Nos casos em que os eventos correspondentes às perturbações podem ser previstos e monitorados pelo Sistema Supervisório, é possível que o Sistema Supervisório interfira no Sistema de Controle Local (por exemplo através do chaveamento de controladores, ou da troca de parâmetros), melhorando assim seu desempenho quando da ocorrência destes eventos (que deixam de ser perturbações *não previstas*). Desta forma, a integração dos diversos componentes da Planta e do

Sistema de Controle Local proporcionada pelo Sistema Supervisório é fundamental para a otimização do sistema.

4 ANÁLISE DE SISTEMAS HÍBRIDOS

Na literatura científica, o termo ‘análise’ vem sendo utilizado com significados distintos e em referência a diferentes aspectos do sistema. No contexto deste capítulo, este termo refere-se particularmente a análise do comportamento de um sistema através de seu modelo.

No âmbito de Sistemas a Eventos Discretos, costuma-se distinguir duas formas de se estudar o comportamento de um modelo: simulação e análise formal. Considerando o escopo deste trabalho, esta dicotomia é adotada também para os Sistemas Híbridos.

Entre estas duas formas de análise, a simulação mostra uma das possíveis soluções para a evolução do sistema sob certas condições e durante um intervalo de tempo limitado. Se a condição inicial não é completamente conhecida, se o comportamento do sistema depende de interações com o ambiente exterior, ou ainda se o objetivo da análise não se restringe a um intervalo de tempo limitado então a simulação nem sempre é efetiva para garantir o comportamento desejado do sistema.

Por outro lado, a chamada análise formal consiste na verificação (prova) de propriedades do modelo. Diferentemente da simulação, estas propriedades não estão necessariamente restritas a um intervalo de tempo específico ou a uma determinada interação com o ambiente exterior. Assim sendo, se os requisitos referentes ao comportamento de um sistema são traduzidos em propriedades do modelo, então ao contrário da simulação, a verificação destas propriedades garante a ausência de erros sob as mais diferentes circunstâncias nas quais o sistema possa vir operar.

Neste sentido, este trabalho considera em particular o problema de verificação de propriedades em um modelo híbrido. O objetivo desta análise é validar o Sistema

Supervisório através da verificação de propriedades do modelo construído em redes PTD-OO (do Sistema Supervisório e seu Objeto de Controle).

Este capítulo inicia-se com uma discussão dos principais problemas relacionados a verificação de propriedades em Sistemas Híbridos e apresenta uma breve revisão sobre os trabalhos desenvolvidos nesta área (Seção 4.2). Com base nesta revisão bibliográfica são identificadas as principais características desejadas num procedimento de análise de redes PTD-OO. Entre estas características se encontra a necessidade de decomposição do problema de análise, o que levou a utilização neste trabalho da associação entre redes de Petri e lógica linear, proposta por Girault; Pradin-Chezalviel; Valette (1997) e apresentada na Seção 4.3. Tendo como base esta associação, a Seção 4.4 introduz então uma nova abordagem para verificação de propriedades de modelos construídos em redes PTD-OO. Finalmente, alguns comentários finais são apresentados na Seção 4.5.

4.1. Verificação de Propriedades em Sistemas Híbridos

De acordo com Antsaklis; Koutsoukos (1998) as técnicas de verificação de propriedades para Sistemas Híbridos não sofreram o mesmo desenvolvimento das técnicas de modelagem. Enquanto inúmeras soluções foram propostas para a modelagem de Sistemas Híbridos com as mais variadas características, o mesmo não ocorreu para análise.

Em geral, as abordagens para verificação de propriedades podem ser classificadas em dois grupos. A prova de propriedades através da enumeração dos estados atingíveis por um modelo é conhecido como '*model checking*' (verificação do modelo). Uma alternativa a este tipo de abordagem é a análise formal através de prova de teoremas, também conhecida como '*theorem proving*' e consiste em inferir ou contradizer uma propriedade através de regras lógicas da matemática (Clarke; Wing, 1996). A vantagem deste último tipo de abordagem é que ele não se restringe a sistemas com um número de estados finitos. Por outro lado, são poucos os tipos de propriedades que podem ser verificados, de forma automática, por abordagens deste tipo.

O principal problema relacionado às abordagens do tipo *model checking* para Sistemas Híbridos é a não-decidibilidade, isto é, a não garantia de que o

comportamento do sistema possa ser descrito por um número finito estados (ou regiões de estados). Este problema foi inicialmente considerado para modelos de Sistemas a Eventos Discretos com relógios de tempo-denso (isto é, onde o tempo é uma variável contínua representada por um número real). Em Alur; Dill (1994) foi mostrado que para autômatos temporizados (*timed automata*) as propriedades ainda são decidíveis. No mesmo trabalho, o “grafo de regiões” foi introduzido como uma ferramenta de análise associando estados discretos com intervalos para as variáveis contínuas representando os relógios do modelo. Os estados acessíveis são, então, representados por um número finito de regiões, permitindo a validação de propriedades. Por outro lado, neste mesmo trabalho, foi também provado que, se variáveis contínuas com diferentes taxas de crescimento (diferentes derivadas) são introduzidas no modelo, então o número de regiões pode se tornar infinito. De forma semelhante, a decidibilidade dos Sistemas Híbridos não pode ser garantida, pois, de uma forma geral, as derivadas das variáveis contínuas não apenas variam entre si em um determinado instante como também podem variar ao longo do tempo.

Uma vez que não existe garantia da decidibilidade do modelo, o desenvolvimento de um procedimento automático para a verificação do sistema baseado na enumeração dos possíveis estados atingíveis não tem garantia de convergência, isto é, não existe garantia de que uma propriedade possa ser provada com um número finito de passos. Além da não garantia de convergência, este tipo de abordagem está sujeito às limitações computacionais.

Estes problemas são evidenciados pelos trabalhos desenvolvidos nesta área, onde buscam-se soluções senão para todos os casos, ao menos para algumas classes de modelos. Na sua maioria, estes trabalhos se referem à análise de sistemas modelados usando *autômatos híbridos*. Alguns exemplos são Alur et al (1995), Gueguen; Zaytoon (2001), que tratam da análise de autômatos lineares através do cálculo do espaço de estados atingíveis.

Apesar destas limitações, alguns destes métodos foram implementados em ferramentas computacionais, entre as quais se destacam UPPAAL (Pettersson; Larsen, 2000) (apenas para autômatos temporizados), HyTech (Henzinger et al, 1997) (apenas para autômatos híbridos lineares), CheckMate (Silva et al, 2000) e Verdict (Stursberg et al, 1998). Silva et al (2001) apresenta uma comparação entre

estas ferramentas usando como exemplo um sistema relativamente simples de um reator químico por bateladas. A conclusão obtida pelo trabalho é que a complexidade computacional restringe a aplicação das atuais ferramentas disponíveis para sistemas relativamente pequenos e simples.

Considerando os problemas apresentados, e as soluções encontradas na literatura, neste capítulo é descrita a proposta de um novo procedimento para verificação de propriedades em redes PTD-OO. Este procedimento explora a decomposição do modelo em objetos para decompor um problema de análise que envolveria a rede global do sistema, em uma série de problemas mais simples, envolvendo apenas sub-redes de um ou poucos objetos. Neste sentido, a verificação de uma propriedade é realizada através da busca de cenários representando as possíveis evoluções do sistema, onde apenas os eventos e estados relacionados à propriedade são considerados. Este enfoque *dirigido* aos aspectos relevantes para as propriedades é conseguido através da utilização da lógica linear como formalismo de base para a análise da parte discreta. Sendo assim, apresenta-se na Seção 4.3 uma introdução sobre a associação entre a lógica linear e as redes de Petri, e como esta associação é utilizada para verificar a alcançabilidade de marcações e para busca de cenários em modelos de redes de Petri.

4.2. Redes de Petri e Lógica Linear

4.2.1. Lógica Linear x Lógica Clássica

A idéia de definir uma associação entre a lógica e as redes de Petri para a análise da alcançabilidade foi inicialmente estudada considerando a lógica clássica. No entanto, a lógica clássica apresenta algumas propriedades que a tornam incompatível para tal associação, sendo uma delas a **monotonicidade**. Na lógica clássica, se uma proposição é verdadeira, ela permanece verdadeira qualquer que seja o uso que se faça dela. No entanto, para os problemas representados por redes de Petri, é necessário caracterizar os recursos que são consumidos, alocados ou liberados dinamicamente, sendo assim, qualquer proposição associada ao seu estado terá sua veracidade alterada de acordo com a evolução do sistema. Um outro

problema refere-se a necessidade de contabilizar os recursos. Se cada recurso é associado a uma proposição ‘P’, segundo a lógica clássica, ‘P AND P’ é igual a ‘P’, o que equivale a dizer que dispor de dois ou mais recursos é o mesmo que dispor de um único recurso.

Em função destas características, no lugar da lógica clássica optou-se pela lógica linear, proposta por Girard (1987), onde as proposições não são mais ‘verdades eternas’ e podem tanto serem ‘consumidas’ por raciocínios, como serem ‘contadas’, como se fossem recursos. Basicamente, a lógica linear difere da lógica clássica pelo abandono de duas regras: a regra de contração e a regra de enfraquecimento, o que resultou na redefinição de 3 conectores: ‘AND’, ‘OR’ e ‘IMPLY’.

As deduções no âmbito da lógica linear são baseadas na prova de *seqüentes*. Um seqüente é formado por: uma lista de premissas (que são hipóteses), o meta-conector ‘|—’ e uma lista de conclusões. Os elementos de cada uma das listas de um seqüente são separados pelo meta-conector ‘,’. De modo intuitivo um seqüente representa um teorema. Por exemplo, ‘ $X_1, X_2 \text{ |— } Y_1, Y_2$ ’ significa que ‘a partir das hipóteses X_1 e X_2 pode-se deduzir as conclusões Y_1 ou Y_2 ’ (o meta-conector ‘,’ portanto não tem o mesmo significado à esquerda ou à direita de ‘|—’).

A prova de um seqüente é feita usando uma abordagem sintática, isto é, verificando que um seqüente está corretamente escrito (sintaticamente correto). A prova consiste na aplicação de um conjunto de regras até se obter apenas seqüentes axiomas (isto é, seqüentes que são verdadeiros por definição). Cada regra é composta de duas partes: a parte inferior e a parte superior (Fig. 4.1). A parte inferior é constituída por um único seqüente (Seqüente 1), enquanto a parte superior pode ser constituída por um ou dois seqüentes (apenas o Seqüente 2 ou os Seqüentes 2 e 3). Uma regra se interpreta da seguinte forma: para provar o seqüente da parte inferior é suficiente provar os seqüentes da parte superior.

Fig. 4.1. Representação gráfica de uma regra.

Neste trabalho são consideradas as regras apresentadas na Fig. 4.2. Nestas regras tem-se que:

- A, B e C são proposições atômicas da lógica linear.
- F, G e H são fórmulas. Uma fórmula é constituída de uma ou mais proposições atômicas separadas por conectores. Neste trabalho considera-se apenas os seguintes conectores $\otimes$ (conjunção multiplicativa), $\wp$ (disjunção multiplicativa) e $\multimap$ (implicação). Exemplos de fórmulas são ' $F = A \otimes B$ ', ' $G = A \otimes B \multimap C$ '.
- $\Gamma, \Gamma_1, \Gamma_2, \Delta, \Delta_1$ e Δ_2 são blocos de fórmulas. Cada bloco é composto por uma lista (eventualmente vazia) de fórmulas separadas pelo meta-conector ','. Um exemplo de bloco de fórmula é ' $\Gamma = F, G$ '.

$\frac{\Gamma_1, F, G, \Gamma_2 \vdash \Delta}{\Gamma_1, G, F, \Gamma_2 \vdash \Delta} \text{ Exchange L}$	$\frac{\Gamma, F, G \vdash \Delta}{\Gamma, F \otimes G \vdash \Delta} \otimes L$	$\frac{\Gamma, F \vdash G, \Delta}{\Gamma \vdash F \multimap G, \Delta} \multimap R$
$\frac{\Delta \vdash \Gamma_1, F, G, \Gamma_2}{\Delta \vdash \Gamma_1, G, F, \Gamma_2} \text{ Exchange R}$	$\frac{\Gamma \vdash F, G, \Delta}{\Gamma \vdash F \wp G, \Delta} \wp R$	$\frac{\Gamma_1 \vdash F, \Delta_1 \quad \Gamma_2, G \vdash \Delta_2}{\Gamma_1, \Gamma_2, F \multimap G \vdash \Delta_1, \Delta_2} \multimap L$
$\frac{\Gamma_1 \vdash F, \Delta_1 \quad \Gamma_2 \vdash G, \Delta_2}{\Gamma_1, \Gamma_2 \vdash F \otimes G, \Delta_1, \Delta_2} \otimes R$	$\frac{}{A \vdash A} \text{ Identidade}$	$\frac{\Gamma_1 \vdash F \quad \Gamma_2, F \vdash \Delta}{\Gamma_1, \Gamma_2 \vdash \Delta} \text{ Cut}$
$\frac{\Gamma_1, F \vdash \Delta_1 \quad \Gamma_2, G \vdash \Delta_2}{\Gamma_1, \Gamma_2, F \wp G \vdash \Delta_1, \Delta_2} \wp L$		

Fig. 4.2. Regras da lógica linear.

A regra 'Identidade' é verdadeira por definição. A regra 'Cut' especifica a possibilidade de utilizar um lema intermediário para fazer uma prova. Este lema é representado pela fórmula 'F'. O seqüente a direita da regra (' $\Gamma_1 \vdash F$ ') representa a prova do lema, enquanto que o seqüente à esquerda (' $\Gamma_2, F \vdash \Delta$ ') representa a utilização do lema na prova.

As regras 'Exchange L' e 'Exchange R' representam a propriedade de comutação na lógica linear. Para não sobrecarregar a prova dos seqüentes em geral estas regras são omitidas.

A utilização das regras, assim como a sua interpretação no contexto de redes de Petri é apresentada a seguir.

4.2.2. Alcançabilidade em Redes de Petri x Prova de Seqüentes em

Lógica Linear

Inicialmente, foi proposta Gunter; Gehlot (1989 apud Girault; Pradin-Chezalviel; Valette, 1997) uma abordagem onde associava-se um seqüente axioma a cada transição (elemento da rede de Petri). Posteriormente, Girault; Pradin-Chezalviel; Valette (1997) propôs uma segunda abordagem, onde cada ‘disparo de transição’ é associado a uma proposição implicativa. Entre as vantagens desta segunda abordagem encontra-se o fato de que a prova é realizada apenas usando os axiomas propostos pela lógica linear, enquanto que na primeira abordagem a extensão de axiomas leva a utilização da regra ‘Cut’ (Fig. 4.2) para a prova do seqüente. Isto significa que a prova é realizada por partes. Do bloco de fórmulas Γ_1 prova-se a formula intermediária F . Então, a partir de Γ_2 e F , prova-se o bloco final Δ . No entanto a fórmula F não existia no seqüente original, ela é um estado intermediário da prova introduzido de modo intuitivo, o que pode tornar a prova do seqüente não trivial. Além disso, na segunda abordagem a noção de marcação (da rede de Petri) é explícita, e a prova de um seqüente evidencia relações de paralelismo e ordem parcial dos eventos. Esta é, portanto, a abordagem considerada neste trabalho.

A alcançabilidade de marcações de uma rede de Petri pode ser feita no âmbito da lógica linear de duas formas (Khalfaoui, 2003): a partir da marcação inicial, evolui-se através dos estados do sistema disparando-se as transições até chegar a marcação final (raciocínio para frente), ou a partir da marcação final retrocede-se nos estados do sistema, disparando-se as transições no sentido contrário até chegar-se a marcação inicial (raciocínio para trás). Estes dois raciocínios são ilustrados a seguir e não podem ser combinados dentro da prova de um único seqüente a menos da utilização da regra ‘Cut’.

Raciocínio para frente

Segundo a abordagem de raciocínio para frente, a prova da alcançabilidade entre as marcações de uma rede de Petri é realizada considerando que:

- Um átomo ‘p’ é associado a cada lugar ‘p’ da rede de Petri.

- Um monômio usando o conector $\otimes$ é associado a toda marcação que é pré-condição ou pós-condição de uma transição.
- Uma fórmula implicativa é definida para cada transição 't' da rede de Petri:

$$t: \otimes p_i (i \in \text{Pre}(p_i, t)) \multimap \otimes p_j (j \in \text{Post}(p_j, t))$$

- *Exemplo:* A Fig. 4.3 apresenta um exemplo de rede de Petri e a respectiva representação de suas transições como fórmulas implicativas da lógica linear.

Fig. 4.3. Exemplo de rede de Petri e respectiva definição das transições usando lógica linear (Raciocínio para frente).

A prova de alcançabilidade entre marcações de uma rede de Petri é realizada através da prova do seqüente do tipo ' $M_0, t_1, t_2, \dots, t_n \vdash M_f$ ', onde M_0 é a marcação inicial, M_f é a marcação final e $t_1, t_2, \dots, t_n$ é um conjunto de disparos de transições que devem levar de M_0 a M_f . A prova do seqüente é realizada através da construção de sua *árvore de prova*, isto é, através da aplicação sucessiva das regras ' $\otimes L$ ', ' $\otimes R$ ' e ' $\multimap L$ ', até a obtenção apenas de seqüentes identidade (' $A \vdash A$ '), que são verdadeiros por definição. Observa-se que as árvores de prova são lidas de baixo para cima. A seguir apresenta-se um exemplo.

- *Exemplo:* A Fig. 4.4 apresenta a árvore de prova para verificar a alcançabilidade entre as marcações $\{p_1, p_4\}$ e $\{p_2, p_5\}$ através do disparo das transições t_1 e t_2 usando o raciocínio para frente. Partindo do seqüente inicial, inicia-se a prova pela aplicação da regra ' $\otimes L$ ', que indica que, se o seqüente é verdadeiro quando p_1 e p_4 estão presentes simultaneamente na rede definindo a marcação ' $p_1 \otimes p_4$ ', também o será quando p_1 e p_4 forem *consumidos* de forma independente, resultando em ' p_1, p_4 '. Em seguida aplica-se a regra ' $\multimap L$ ', correspondente ao disparo da transição t_1 , pois leva a marcação ' $p_4, p_2 \otimes p_3$ '. Sucessivamente, a segunda aplicação da regra ' $\otimes L$ ' transforma ' $p_2 \otimes p_3$ ' em ' p_2, p_3 ' e a segunda aplicação da regra ' $\multimap L$ ' corresponde ao disparo de t_2 . A última regra utilizada na prova do seqüente é a ' $\otimes R$ ' que indica que se dois seqüentes são verdadeiros

de forma independente um do outro, também o serão em conjunto. Uma vez obtidos apenas seqüentes identidade, a prova está concluída pois estes são verdadeiros por definição, o que garante a veracidade do seqüente inicial.

Fig. 4.4. Exemplo de prova usando o raciocínio para frente.

Raciocínio para trás

No raciocínio para trás, o conector $\otimes$ é substituído pelo conector $\wp$ e a realização da prova corresponde a disparar as transições no sentido contrário, isto é, a partir da marcação após o disparo tem-se a marcação antes do disparo. Segundo esta abordagem, a prova da alcançabilidade entre marcações de uma rede de Petri é realizada considerando que:

- Um átomo ‘p’ é associado a cada lugar ‘p’ da rede de Petri.
- Um monômio usando o conector $\wp$ é associado a toda marcação que é pré-condição ou pós-condição de uma transição.
- Uma fórmula implicativa é definida para cada transição ‘t’ da rede de Petri:

$$t: \wp p_i (i \in \text{Pre}(p_i, t)) \multimap \wp p_j (j \in \text{Post}(p_j, t))$$

➤ *Exemplo:* A Fig. 4.5 apresenta a representação das transições da rede de Petri da Fig. 4.3 considerando o raciocínio para trás.

Fig. 4.5. Definição das transições usando lógica linear e o raciocínio para trás.

A prova de alcançabilidade entre marcações de uma rede de Petri é realizada de forma semelhante ao raciocínio para frente. No entanto, utilizam-se as regras ‘ $\wp R$ ’, ‘ $\wp L$ ’ e ‘ $\multimap L$ ’.

➤ *Exemplo:* A Fig. 4.4 apresenta a árvore de prova para o mesmo problema apresentado na Fig. 4.3 mas agora usando o raciocínio para trás. Neste caso, partindo do seqüente inicial, inicia-se a prova pela aplicação da regra ‘ $\wp R$ ’, que equivale a regra ‘ $\otimes L$ ’ do raciocínio para frente, pois os dois conectores se comportam de forma semelhante em lados opostos do seqüente. A aplicação da regra ‘ $\wp R$ ’ indica que as marcas em p_2 e p_5 não precisam ser *produzidas* simultaneamente. Similarmente, a regra ‘ $\wp L$ ’ equivale a regra ‘ $\otimes R$ ’.

Fig. 4.6. Exemplo de prova usando o raciocínio para trás.

4.2.3. Lógica linear para a busca de cenários em redes de Petri

Na seção anterior foi apresentado como utilizar a lógica linear para provar a alcançabilidade entre marcações uma vez que o conjunto de transições a serem disparados é conhecido – o que corresponde à prova da veracidade (ou falsidade) de um cenário já definido, onde o estado inicial, o estado final e o conjunto de eventos do cenário são todos conhecidos.

No entanto, em muitos problemas, estes dados são apenas parcialmente conhecidos. Um exemplo é quando o conjunto de eventos que levam da marcação inicial à final está apenas parcialmente definido (conhece-se apenas alguns eventos que fazem parte do cenário, mas não *todos* os eventos) ou simplesmente não está definido. Outro exemplo é quando a marcação inicial ou final está parcialmente

definida, o que significa que apenas a marcação de alguns lugares é conhecida, correspondendo, por exemplo, ao estado de alguns equipamentos. Nestes casos, o que se deseja é especificar o conjunto de cenários possíveis (se existente) que ‘encaixam’ nesta definição parcial, estabelecendo uma relação de causalidade entre M_0 e M_f .

Em Khalfaoui et al (2001) foi proposta a utilização da lógica linear para determinação de cenários parcialmente definidos. Neste caso, o seqüente correspondente a prova é escrito na seguinte forma:

- Raciocínio para frente: $\Gamma_0, M_0, !t_1, \dots, !t_n \multimap M_f \otimes \Gamma_f$
- Raciocínio para trás: $\Gamma_0 \wp M_0, !t_1, \dots, !t_n \multimap M_f, \Gamma_f$

Nestes seqüentes, tem-se que:

- $!t_i$ representa um número de disparos desconhecido da transição t_i , o que indica que os cenários que levam de M_0 a M_f podem ter de zero a infinitos disparos de t_i .
- Γ_0 representa um conjunto desconhecido de marcas necessário para alcançar M_f a partir de M_0 . As marcas são unidas por ‘,’ no primeiro caso, e por ‘ $\wp$ ’ no segundo caso.
- Γ_f representa um conjunto desconhecido de marcas, adicional a M_f e gerado a partir de Γ_0 e M_0 . As marcas são unidas por ‘ $\otimes$ ’ no primeiro caso, e por ‘,’ no segundo caso.

A determinação dos possíveis cenários é realizada através da construção da árvore de prova. Neste caso, no entanto, sempre que duas transições estão habilitadas, duas possíveis árvores são geradas, correspondendo a dois possíveis cenários. No raciocínio para frente, a prova é finalizada quando a marcação M_f é alcançada. No raciocínio para trás, a prova é finalizada quando M_0 é alcançado. Um exemplo é apresentado a seguir.

- *Exemplo:* Considera-se a rede da Fig. 4.7 onde a marcação inicial e a marcação final são parcialmente conhecidas: $M_0 = p_2$ e $M_f = p_6$, e onde o conjunto de disparos de transições é desconhecido. Deseja-se determinar quais os possíveis cenários que estabelecem uma relação de causalidade entre M_0 a M_f .

Fig. 4.7. Exemplo.

- *Exemplo – Raciocínio para frente:* O seqüente a ser analisado é: ' $\Gamma_0, p_2, !t_1, \dots, !t_5 \mid - p_6 \otimes \Gamma_f$ '. A construção das árvores correspondentes aos possíveis cenários é apresentada na Fig. 4.8. Neste caso, a partir da marcação inicial parcial p_2 , duas transições podem ser disparadas (t_2 e t_1), levando a dois possíveis cenários. No caso de t_1 , observa-se que a pré-condição é ' $p_1 \otimes p_2$ ', portanto o cenário só é possível se Γ_0 conter p_1 - o que indicado pela substituição de Γ_0 por ' Γ_0, p_1 '. Para cada cenário, uma vez que a marcação do lado esquerdo do seqüente contém a marcação final especificada (p_6), a solução final é obtida fazendo com que ' $\Gamma_0^i = \emptyset$ ' e que Γ_f contenha as demais marcas presentes do lado esquerdo do seqüente além da marcação final.

Fig. 4.8. Busca de cenários - exemplo de raciocínio para frente.

- *Exemplo – Raciocínio para trás:* O seqüente a ser analisado é: ' $\Gamma_0 \wp p_2, !t_1, \dots, !t_5 \mid - p_5, \Gamma_f$ '. A construção das árvores correspondentes aos possíveis cenários é apresentada na Fig. 4.9. Neste caso, a partir da marcação final parcial p_6 , a transição t_4 é disparada, resultando na marcação parcial p_5 . Duas transições

podem então ser disparadas (t_2 ou t_3), levando a dois possíveis cenários. No caso de t_3 , observa-se que a pós-condição é ' $p_4 \not\wp p_5$ ', portanto o cenário só é possível se Γ_f conter p_4 . Semelhantemente ao raciocínio para frente, Γ_f é substituído por ' Γ_f, p_4 '. Uma vez que a marcação do lado direito do seqüente contém a marcação inicial especificada (p_2), a solução final é obtida fazendo com que ' $\Gamma_f^i = \emptyset$ ' e que Γ_0 contenha as demais marcas presentes do lado direito do seqüente além da marcação inicial.

Fig. 4.9. Busca de cenários - exemplo de raciocínio para trás.

Uma vez apresentada a associação entre lógica linear e redes de Petri, a próxima seção discute suas principais vantagens, em particular para modelos construídos utilizando os conceitos da orientação a objetos, como é o caso das redes PTD-OO.

4.2.4. A lógica linear e a Orientação a Objeto

A introdução dos conceitos de orientação a objetos na construção dos modelos em redes PTD-OO garante modularidade com interfaces bem definidas. Sendo assim, a utilização da lógica linear como formalismo para verificação de propriedades em redes de Petri apresenta duas características que a tornam particularmente interessante para análise da parte discreta das redes PTD-OO: ela permite um enfoque local do problema e explora a ordem parcial entre os eventos.

O enfoque local significa que uma propriedade pode ser verificada considerando apenas uma parte do sistema, independentemente dos disparos e da evolução da marcação no restante da rede. Assim, a evolução interna de um objeto

(entre duas interações com outros objetos) é representada de forma completamente independente da evolução interna de outros objetos. Da mesma forma, a evolução de um conjunto de objetos pode ser representada de forma independente da evolução dos demais objetos do sistema.

- *Exemplo:* Considera-se o seqüente ‘ $p_{1_1.O1}, p_{2_1.O1}, t_{1_1.O1}, t_{2_1.O1}, t_{3_1.O1} \mid \text{---} p_{5_1.O1} \otimes p_{6_1.O1}$ ’, que representa a alcançabilidade entre dois estados do objeto $O_{1,1}$ e onde nenhuma das transições $t_{1_1.O1}, t_{2_1.O1}, t_{3_1.O1}$ pertence a interface do objeto. Se este seqüente é verdadeiro, então também é verdadeiro o seqüente ‘ $\Gamma_A, p_{1_1.O1}, p_{2_1.O1}, t_{1_1.O1}, t_{2_1.O1}, t_{3_1.O1} \mid \text{---} p_{5_1.O1} \otimes p_{6_1.O1} \otimes \Gamma_B$ ’, onde Γ_A e Γ_B correspondem a um conjunto de qualquer proposição (que podem representar marcas e eventos em outros objetos do sistema). Além disso, se é verificada a veracidade de um segundo seqüente, ‘ $p_{7_2.O1}, t_{4_2.O1}, t_{5_2.O1} \mid \text{---} p_{9_2.O1}$ ’, representando a evolução interna de um segundo objeto $O_{1,2}$, que acontece paralelamente a evolução de $O_{1,1}$, então os seqüentes podem ser combinados através da regra ‘ $\otimes R$ ’, que indica que a prova dos dois seqüentes de forma independente equívale a prova do seqüente global (Fig. 4.10):

$$\frac{p_{1_1.O1}, p_{2_1.O1}, t_{1_1.O1}, t_{2_1.O1}, t_{3_1.O1} \mid \text{---} p_{5_1.O1} \otimes p_{6_1.O1} \quad p_{7_2.O1}, t_{4_2.O1}, t_{5_2.O1} \mid \text{---} p_{9_2.O1}}{p_{1_1.O1}, p_{2_1.O1}, p_{7_2.O1}, t_{1_1.O1}, t_{2_1.O1}, t_{3_1.O1}, t_{4_2.O1}, t_{5_2.O1} \mid \text{---} p_{5_1.O1} \otimes p_{6_1.O1} \otimes p_{9_2.O1}} \otimes R$$

Fig. 4.10. O enfoque local da lógica linear.

Por outro lado, se utilizarmos por exemplo como método de análise a construção do ‘grafo de marcações alcançáveis’ (Cardoso & Valette, 1997) do sistema, a combinação da evolução de dois objetos não é o resultado direto da simples associação de dois grafos e sim uma composição mostrando os possíveis estados do sistema de um ponto de vista global.

- *Exemplo:* A Fig. 4.11 apresenta os grafos de marcações alcançáveis equivalentes a análise de $O_{1,1}$, de $O_{1,2}$, e dos dois objetos em conjunto. Neste caso, de 7 estados locais, passa-se a ter 20 estados globais.

Fig. 4.11. Análise através da construção do grafo de marcações alcançáveis.

Outra importante característica da utilização da lógica linear para análise de redes de Petri é que os cenários representando as possíveis evolução do sistema são definidos tendo como base a ordem parcial de disparos, isto é, na relação de causalidade entre os eventos, e não a seqüência temporal das ocorrências. Cada cenário equívale a uma ordem parcial de disparos, e a prova de um seqüente corresponde então a verificação do cenário.

- *Exemplo:* Considera-se os objetos $O_{1.3}$ e $O_{1.4}$ da Fig. 4.12, cujos comportamentos entre as chamadas de métodos são independentes. Para a evolução do sistema do estado inicial $\{p_{1.3.O1}, p_{1.4.O1}\}$ ao estado final $\{p_{5.3.O1}, p_{5.4.O1}\}$, apenas uma árvore de prova deve ser construída, correspondente a prova do seqüente ' $p_{1.3.O1}, p_{1.4.O1}, t_{1.3.O1/1.4.O1}, t_{2.3.O1}, t_{3.3.O1}, t_{4.3.O1}, t_{2.4.O1}, t_{3.4.O1}, t_{4.4.O1}, t_{5.3.O1/5.4.O1} \vdash p_{6.3.O1} \otimes p_{6.4.O1}$ '. Esta árvore de prova equívale a uma única ordem parcial de eventos (e portanto um único cenário), representada na Fig. 4.13. Esta ordem parcial indica, por exemplo, que o disparo de $t_{2.3.O1}$ deve ocorrer entre o disparo de $t_{1.3.O1/1.4.O1}$ e de $t_{5.3.O1/5.4.O1}$, mas não define sua ocorrência em relação ao disparo das transições $t_{2.4.O1}$, $t_{3.4.O1}$ e $t_{4.4.O1}$. São apenas consideradas as relações de causalidade entre os eventos. No entanto, se construirmos o grafo de marcações alcançáveis, além do excessivo número de estados, encontraremos 20 seqüências de disparos, isto é 20 cenários possíveis, sendo que a análise de todos estes 20 cenários não trará nenhuma informação não representada pelo cenário associado à única ordem parcial do sistema.

Fig. 4.12. Rede PTD-OO dos objetos $O_{1,3}$ e $O_{1,4}$. Fig. 4.13. Ordem parcial de disparos para os objetos $O_{1,3}$ e $O_{1,4}$.

A seguir apresenta-se como a equivalência entre redes de Petri e lógica linear, e o procedimento descrito na seção 4.2.3 são utilizados para análise da parte discreta das redes PTD-OO.

4.3. O Procedimento Proposto para Análise das redes PTD-OO

4.3.1. Principais características

Decomposição do Processo de Análise

De acordo com o apresentado anteriormente, uma das principais características do procedimento proposto é a decomposição do processo de análise. Para determinar os possíveis cenários para a evolução do sistema considera-se de forma isolada a evolução de cada objeto. As possíveis comunicações entre o objeto em análise e os demais objetos do sistema geram *obrigações de análise* para outros objetos. Uma obrigação de análise indica que a veracidade da propriedade verificada em um determinado objeto depende do comportamento dos outros objetos com os quais ele interage. Estes objetos serão portanto analisados e poderão resultar em novas obrigações de análise. O processo continua até que todas as obrigações de análise tenham sido realizadas (Fig. 4.14).

Fig. 4.14. Decomposição da análise de um modelo.

Introdução de Hipóteses

Durante a análise de um objeto, podem ser introduzidas *hipóteses* sobre o comportamento do objeto e sobre a interação deste com outros objetos. Cada hipótese é uma suposição considerada provável de ser verdadeira pela pessoa que está fazendo a análise do modelo, e que facilita a verificação da propriedade. As hipóteses são ‘criadas’ pela pessoa que está fazendo a análise tendo como base seu conhecimento do sistema modelado (isto é, da interpretação do modelo). Hipóteses são obrigações de análise e, para que a propriedade seja considerada verdadeira, todas as hipóteses também devem ser verificadas.

Uma hipótese corresponde a um lema intermediário em uma prova matemática. Ela não é necessária para a prova, mas permite a decomposição e a simplificação da prova. Um exemplo de hipótese seria a utilização da regra ‘Cut’ da lógica linear para provar a alcançabilidade entre as marcações. Esta regra impõe uma marcação intermediária entre a marcação inicial e a final. Neste caso, a hipótese seria ‘a partir da marcação inicial uma determinada marcação intermediária deve ser atingida’, prova-se então que a partir desta marcação intermediária a marcação final é atingida. Para que a propriedade de alcançabilidade seja efetivamente verdadeira, deve-se provar a hipótese feita, isto é, que a partir da marcação inicial a marcação intermediária é efetivamente atingida.

Utilização da Lógica Linear

Um aspecto importante da abordagem proposta, é que a análise da parte discreta é realizada separadamente da parte contínua. A associação entre redes de

Petri e lógica linear apresentada na Seção 4.3 é utilizada para a parte discreta. Observa-se no entanto, que tal associação não considera qualquer mecanismo de identificação das marcas. Duas marcas em um determinado lugar são representadas por duas proposições idênticas, que podem ser indistintamente consumidas. É necessário portanto que a análise seja feita sobre o modelo desdobrado da rede PTD-OO (Seção 2.5.3), onde o estado de cada objeto de uma classe é representado em uma rede distinta, o que restringe a aplicação desta abordagem para modelos onde o estado inicial do sistema é definido (ao menos do ponto de vista discreto) e onde o número de objetos instanciados de cada classe é fixo.

4.3.2. *Visão geral do procedimento de análise*

O procedimento para validação do Sistema Supervisório através da análise da rede PTD-OO pode ser organizado em uma seqüência de **passos**, conforme apresentado na Fig. 4.15.

A análise se inicia com o estabelecimento de um conjunto de propriedades a serem verificadas que garantam os requisitos do sistema. Em particular, este trabalho considera dois tipos de propriedades: *propriedades de alcançabilidade* e *propriedades de segurança*. As propriedades de alcançabilidade garantem que, em determinadas circunstâncias, um estado sempre é atingido, enquanto que as propriedades de segurança garantem que estados considerados impróprios ou proibidos nunca são atingidos, independente do que aconteça no sistema.

A definição de uma propriedade é composta de duas partes: o *enunciado* (**Etapa 1**) e as eventuais *restrições* (**Etapa 2**). Para propriedades de alcançabilidade são propostos dois possíveis enunciados (PA1 e PA2) enquanto para as propriedades de segurança é proposto apenas um enunciado (PS1). As restrições delimitam os casos onde espera-se que a propriedade seja verdadeira. Elas são imposições sobre o estado ou a ocorrência de eventos nos objetos. Neste trabalho são considerados 9 possíveis tipos de restrições (R1 a R9).

Fig. 4.15. **Etapas** da Validação de um Sistema Supervisório Híbrido.

Uma vez definido o conjunto de propriedades, a **Etapa 3** consiste na construção dos *Diagramas de Colaboração Estáticos*, onde ilustra-se todas as interações entre objetos, e portanto, as possíveis seqüências de análise dos objetos na verificação de uma propriedade.

Para cada propriedade definida, a verificação inicia-se pela análise do 1º objeto (**Etapa 4**). Conforme apresentado anteriormente, a análise deste objeto pode resultar na obrigação de análise de outros objetos e assim sucessivamente – esta é a **Etapa 5**. Em ambas as **Etapas 4 e 5**, a análise de um objeto é dividida em 3 partes principais:

- **Etapa 4.1/5.1 – Parte discreta – Busca de cenários:** usando o procedimento da Seção 4.3.3, determina-se um conjunto de cenários relativos a evolução daquele objeto nas condições definidas pela propriedade. Durante esta busca,

desconsidera-se a interação do objeto analisado com outros objetos (as transição da interface são consideradas como transições internas).

- **Etapa 4.2/5.2 – *Elaboração de hipóteses***: são feitas hipóteses sobre a interação do objeto analisado com outros objetos e/ou sobre o comportamento interno do objeto. Estas hipóteses visam restringir o conjunto de cenários anteriormente definidos, os intervalos possíveis para as datas de disparo das transições destes cenários ou o comportamento das variáveis contínuas.
- **Etapa 4.3/5.3 – *Parte contínua – Evolução de Variáveis Contínuas e Datas de Disparos***: a análise do objeto é finalizada pela determinação de intervalos para as datas de disparos das transições e pela determinação do comportamento das variáveis contínuas tendo em vista as funções de junção, de habilitação e os sistemas de equações do objeto.

A análise de todos os objetos para os quais são geradas obrigações de análise resulta em um conjunto de cenários que respeitam ou não a propriedade estabelecida. No primeiro caso a propriedade é verdadeira se as hipóteses realizadas também são verdadeiras. No segundo caso, nenhuma conclusão é obtida: a propriedade pode ser falsa ou as hipóteses realizadas podem impõem restrições desnecessárias que impossibilitam a verificação da propriedade.

No caso dos cenários satisfazerem a propriedade, a **Etapa 6** consiste na construção de um seqüente global para cada cenário. Este seqüente resulta da composição dos seqüentes das **Etapas 4.1 e 5.1**. Construindo sua árvore de prova é verificada, através da lógica linear, a consistência da composição das análises de cada objeto. Observa-se que esta **etapa** é realizada apenas para as propriedades de alcançabilidade.

Finalmente, a **Etapa 7** consiste na verificação das hipóteses realizadas.

Apesar de a seqüência de **etapas** ser a mesma para ambas as propriedades de alcançabilidade e de segurança, o detalhamento de cada **etapa** é diferente. Assim, apresenta-se na Seção 4.3.3 o detalhamento do procedimento para propriedades de alcançabilidade, enquanto que a Seção 4.3.4 trata de propriedades de segurança.

Para ilustrar o procedimento de análise utiliza-se como exemplo o sistema para embalagem de um determinado produto, apresentado a seguir.

➤ *Exemplo:* A Fig. 4.16 apresenta o sistema para embalagem de um determinado produto, que é despejado em bandejas de 4 copos. O sistema é composto por duas máquinas: M_1 , responsável por posicionar adequadamente a bandeja, e M_2 , responsável por despejar o produto. O modelo do sistema é composto por 2 objetos: $O_{1.1} - \underline{M_1}$ e $O_{1.2} - \underline{M_2}$. As variáveis V_R e V_C (de $O_{1.2}$) indicam o volume do reservatório de produto em $\underline{M_2}$ e de produto no copo, respectivamente. A vazão de produto que chega ao reservatório é dado pela variável externa q . A variável N (de $O_{1.1}$) indica o número de copos enchedos na bandeja. O estado inicial do sistema é:

- $O_{1.1} = \underline{M_1}$; $X_{1.1} = \{N = 0, \theta_{aux} = 0, l_1 = \underline{M_2}\}$; $m_{1.1} = \{p_{1_1}\}$;
- $O_{1.2} = \underline{M_2}$; $X_{1.2} = \{V_R = ind, V_C = 0\}$; $m_{1.2} = \{p_{1_2}\}$;

Fig. 4.16. Sistema de embalagem e respectivo modelo em redes PTD-OO.

4.3.3. Propriedade de Alcançabilidade

4.3.3.1. Etapa 1 - Definição do enunciado da propriedade

As propriedades de alcançabilidade consideradas neste trabalho são definidas através dos seguintes enunciados:

- PA1) Dado a ocorrência de um evento e_0 , um segundo evento e_f deve ocorrer em um intervalo de tempo $\Delta\theta_{\max}$ (exemplos: **Propriedades 2** do Estudo de Caso 1 (Capítulo 5) e **Propriedade 1** do Estudo de Caso 3 (Capítulo 7)).
- PA2) Dado a ocorrência de um evento e_0 , um segundo evento e_i deve ocorrer em um intervalo de tempo $\Delta\theta_{\max}$, resultando em um estado que é mantido até a ocorrência de um terceiro evento e_f (exemplos: **Propriedades 1** do Estudo de Caso 1 (Capítulo 5)).

Os eventos e_0 , e_i e e_f podem ser definidos da seguinte forma:

- Como o disparo de uma transição interna $t_{x,y.Ow}$ ou de uma transição de interface $t_{x,y.Ow/z_u.Ov}$ de um objeto $O_{w,y}$ (exemplo: e_0 para a **Propriedade 1** do Estudo de Caso 1 (Capítulo 5)).
- Como o alcance de um estado que é definido através da especificação parcial ou completa da marcação $m_{w,y}$ de um objeto $O_{w,y}$.
- Como o alcance de um estado que é definido em função do valor das variáveis $X_{w,y}$ de um objeto $O_{w,y}$.

Observa-se que a propriedade de alcançabilidade não impõe que e_0 ocorra quando o sistema está no estado inicial ($\theta(e_0) \geq 0$). O estado do sistema no instante de ocorrência de e_0 não é conhecido, ele pode estar em qualquer estado alcançável a partir do conjunto de estados iniciais definidos e onde o evento e_0 está habilitado.

➤ *Exemplo:* Para o sistema da Fig. 4.16, um exemplo de propriedade de alcançabilidade a ser verificada é:

- **Propriedade 1** (correspondente a PA1) – Após a emissão de uma solicitação de enchimento de bandeja, a máquina M_1 deve atingir o estado ‘Em repouso’ em 20 segundos:

- O evento e_0 corresponde a emissão de uma solicitação de enchimento de bandeja: $e_0 = \text{disparo de } t_{1_1.O1}$.
- O evento e_f ocorre quando $\underline{M}_1$ atinge o estado ‘Em repouso’: $e_f = \text{alcance da marcação } m_{1.1} = \{p_{1_1.O1}\}$.
- O intervalo de tempo considerado é $\Delta\theta = 20$ segundos.

4.3.3.2. ***Etapa 2 - Definição do conjunto de restrições da propriedade***

Conforme apresentado anteriormente, a definição das propriedades pode conter *restrições*, que delimitam os casos onde espera-se que a propriedade seja verdadeira. Tendo como base os estudos de caso (apresentados no Capítulo 5, 6 e 7), neste trabalho foram especificados os seguintes tipos de restrições:

- Um determinado evento ocorre em um determinado intervalo de tempo:
 - R1) uma transição interna $t_{a_b.Oc}$ ou de uma transição de interface $t_{a_b.Oc/d_e.Of}$ de um objeto $O_{c.b}$ dispara em $\theta_g \leq \theta \leq \theta_h$.
- Um determinado evento não ocorre durante um determinado intervalo de tempo:
 - R2) uma transição interna $t_{a_b.Oc}$ ou de uma transição de interface $t_{a_b.Oc/d_e.Of}$ de um objeto $O_{c.b}$ não dispara em $\theta_g \leq \theta \leq \theta_h$.
 - R3) um estado definido através da especificação parcial ou completa da marcação $m_{c.b}$ de um objeto $O_{c.b}$ não é alcançado em $\theta_g \leq \theta \leq \theta_h$.
 - R4) uma função booleana que tem como parâmetros de entrada as variáveis $X_{c.b}$ de um objeto $O_{c.b}$ é verdadeira em $\theta_g \leq \theta \leq \theta_h$.
- Um objeto $O_{c.b}$ se encontra em um determinado estado durante um determinado intervalo de tempo:
 - R5) a marcação $m_{c.b}$ de $O_{c.b}$ é parcialmente ou completamente especificada para $\theta_g \leq \theta \leq \theta_h$.
 - R6) o valor de uma variável de $X_{c.b}$ de $O_{c.b}$ é especificado para $\theta_g \leq \theta \leq \theta_h$.
 - R7) o valor de uma variável de $X_{c.b}$ de $O_{c.b}$ pertence a uma faixa de valores durante $\theta_g \leq \theta \leq \theta_h$.
- A evolução de uma objeto $O_{c.b}$ do ponto de vista contínuo obedece a determinadas restrições durante um intervalo de tempo:
 - R8) o valor de uma variável de $X_{c.b}$ de $O_{c.b}$ pertence a um conjunto de valores durante $\theta_g \leq \theta \leq \theta_h$.

R9) a evolução dinâmica de uma variável de $X_{c,b}$ de $O_{c,b}$ obedece uma determinada função durante $\theta_g \leq \theta \leq \theta_h$.

Observa-se que os limites do intervalo de tempo considerado (θ_g e θ_h) podem ser definidos de forma absoluta, como por exemplo $\theta_g=0$ (neste caso a restrição é válida a partir do estado inicial), ou em relação a ocorrência de um evento, por exemplo o disparo de uma transição $t_{i,j,Ok}$ ($\theta_g=\theta_{i,j,Ok}$).

➤ *Exemplo:* Para a **Propriedade 1** do exemplo da Fig. 4.16 considera-se a seguinte restrição:

- Restrição 1A⁷ (correspondente a R2) – O processo de enchimento não é interrompido por falta de produto em M_2 :
 - $t_{3_2,01}$ ($= t_{a_b,0c}$) não dispara em $0(=\theta_g) \leq \theta \leq \infty(=\theta_h)$.

4.3.3.3. **Etapa 3** – Construção dos Diagramas de Colaboração Estáticos

Após a definição do conjunto de propriedades a serem verificadas, a **etapa** seguinte é a construção dos *Diagramas de Colaboração Estáticos*. Diferentemente dos Diagramas de Colaboração construídos durante modelagem (Capítulo 3), onde se modelava a sequência de interações entre os objetos para um cenário específico, o objetivo dos Diagramas de Colaboração Estáticos é ilustrar todas as possíveis interações entre objetos – sem especificar nenhuma ordem cronológica, indicando assim todas as possíveis interações entre objetos que resultaram em obrigações de provas durante a verificação de uma propriedade.

➤ *Exemplo:* Para o sistema da Fig. 4.16 tem-se o seguinte Diagrama de Colaboração Estático (Fig. 4.17):

⁷ Adota-se como padrão a utilização de números inteiros na nomenclatura das propriedades (ex.: Propriedade 1, Propriedade 2). Para as restrições utilizam-se letras maiúsculas, precedidas do número inteiro da correspondente propriedade (ex. Restrição 1A, Restrição 1B, Restrição 2A).

Fig. 4.17. Diagrama de Colaboração Estático para o exemplo da Fig. 4.16.

Uma vez definida a propriedade e construído o Diagrama de Colaboração Estático, as próximas **etapas (Etapas 4 a 6)** consistem então em determinar quais são os possíveis cenários a partir da ocorrência do evento e_0 e se todos estes cenários resultam na ocorrência de e_f , respeitando a propriedade estabelecida.

Inicialmente, nas **Etapas 4 e 5**, os objetos são analisados isoladamente. Determina-se, usando o raciocínio para frente, os possíveis cenários referentes ao comportamento do objeto no intervalo de tempo definido pela propriedade. Em seguida, na **Etapa 6**, usando as informações obtidas na primeira parte, verifica-se a coerência, do ponto de vista discreto, da composição dos cenários locais através da construção da árvore de provas de um seqüente global, envolvendo os estados e os disparos de transições de todos os objetos anteriormente analisados.

4.3.3.4. **Etapa 4** – Análise do 1º Objeto

O primeiro objeto a ser analisado é aquele onde ocorre o evento e_0 , isto é, cuja rede contém a transição, a marcação ou as variáveis relacionadas a e_0 .

4.3.3.5. **Etapa 4.1** – Parte Discreta – Busca de Cenários

O objetivo da busca de cenários é determinar, do ponto de vista discreto, o que pode acontecer no 1º objeto após a ocorrência do evento e_0 . Cada possível evolução, isto é, cada possível seqüência de disparo de transições corresponde a um possível cenário.

A busca de cenários é realizada usando o *raciocínio para frente* (Seção 4.2.3). As transições da interface são consideradas como transições internas. Se estivermos analisando um objeto $O_{w,y}$, uma transição da interface $t_{x,y.Ow/z_u.Ov}$ (cuja fórmula implicativa na lógica linear inclui as pré e pós condições de $O_{w,y}$ e de $O_{v,u}$) é

substituída durante a busca de cenários por uma transição chamada de $t_{x,y.Ow}$ cuja fórmula contém apenas as pré e pós condições do objeto $O_{w,y}$.

A definição dos seqüentes para a busca de cenários depende se, além do evento e_0 , e_i e/ou e_f também ocorrem no mesmo objeto que e_0 (genericamente chamado de $O_{w,y}$).

Tem-se os seguintes casos, ilustrados na Fig. 4.17:

- Caso 1 - apenas e_0 ocorre em $O_{w,y}$ – é realizada apenas uma busca:
 - o *Busca 1*: Evolução a partir de e_0 ;
- Caso 2 - e_0 e e_i ocorrem em $O_{w,y}$ – são realizadas duas buscas (neste caso o conjunto de cenários resultantes são as possíveis combinações entre os resultados das duas buscas):
 - o *Busca 1*: Evolução a partir de e_0 até e_i ;
 - o *Busca 2*: Evolução a partir de e_i ;
- Caso 3 - e_0 e e_f ocorrem em $O_{w,y}$ – é realizada apenas uma busca:
 - o *Busca 1*: Evolução a partir de e_0 até e_f ;
- Caso 4 - e_0 , e_i e e_f ocorrem em $O_{w,y}$ – são realizadas duas buscas (neste caso o conjunto de cenários resultantes são as possíveis combinações entre os resultados das duas buscas):
 - o *Busca 1*: Evolução a partir de e_0 até e_i ;
 - o *Busca 2*: Evolução a partir de e_i até e_f ;

Fig. 4.18. Busca de cenários no 1º objeto para propriedades de alcançabilidade.

Nos Casos 2 e 4, os cenários possíveis para o comportamento do objeto a partir de e_0 são resultados da combinação das seqüências de disparo obtida para as *Buscas 1* e 2. Por exemplo, no Caso 4 se existem duas possíveis seqüências que a partir de e_0 resultam em e_i , e três possíveis seqüências que a partir de e_i resultam em e_f , como resultado poderão ser definidos até 6 cenários.

O seqüente para cada busca é composta por: $\Gamma_0, M_0, !t_{1,y.Ow}, \dots, !t_{n,y.Ow}, t_{i,y.Ow} \vdash M_f \otimes \Gamma_f$. As marcações M_0 , M_f , o disparo $t_{i,y.Ow}$ e as transições do conjunto de disparos ' $!t_{1,y.Ow}, \dots, !t_{n,y.Ow}$ ' são definidas pelas seguintes regras:

- Regra 1 - Quando e_0 corresponde ao alcance de uma marcação $m_{w,y}$, no seqüente da Busca 1 tem-se $M_0 = m_{w,y}$.
- Regra 2 - Quando e_0 corresponde ao disparo de uma transição $t_{x,y.Ow}$ (ou $t_{x,y.Ow/z_u.Ov}$), no seqüente da *Busca 1* tem-se $M_0 = \text{pós-condição de } t_{x,y.Ow}$.
- Regra 3 - Quando e_0 corresponde a uma função booleana das variáveis $X_{w,y}$, nenhuma informação é fornecida sobre o estado do objeto do ponto de vista discreto. A *Busca 1* é decomposta em ' n ' buscas, onde n é o número de marcações alcançáveis por aquele objeto. Em cada busca, M_0 corresponde a uma marcação diferente e $\Gamma_0 = \emptyset$.
- Regra 4 - Quando e_i corresponde ao alcance de uma marcação $m_{w,y}$, no seqüente da Busca 1 (Casos 2 e 4) tem-se $M_f = m_{w,y}$ e o disparo de $t_{i,y.Ow}$ é excluído.
- Regra 5 - Quando e_i corresponde ao disparo de uma transição $t_{x,y.Ow}$ (ou $t_{x,y.Ow/z_u.Ov}$), no seqüente da *Busca 1* (Casos 2 e 4) tem-se $t_{i,y.Ow} = t_{x,y.Ow}$ e $M_f = \emptyset$.
- Regra 6 - Quando e_f corresponde ao alcance de uma marcação $m_{w,y}$, no seqüente da *Busca 1* (Caso 3) ou da *Busca 2* (Caso 4) tem-se $M_f = m_{w,y}$ e o disparo de $t_{i,y.Ow}$ é excluído.
- Regra 7 - Quando e_f corresponde ao disparo de uma transição $t_{x,y.Ow}$ (ou $t_{x,y.Ow/z_u.Ov}$), no seqüente da *Busca 1* (Caso 3) ou da *Busca 2* (Caso 4) tem-se $t_{i,y.Ow} = t_{x,y.Ow}$ e $M_f = \emptyset$.
- Regra 8 - O conjunto de disparo ' $!t_{1,y.Ow}, \dots, !t_{n,y.Ow}$ ' contém todas as transições do objeto $O_{w,y}$ com exceção de $t_{i,y.Ow}$ e de eventuais restrições presentes na definição da propriedade a ser verificada.

Para a *Busca 1* do Caso 1 e para a *Busca 2* do Caso 2, a busca de cenários é realizada até que os cenários gerados:

- a) resultem em marcações já anteriormente alcançadas, o que indica que os cenários para a evolução do objeto são uma combinação das seqüências de disparos definidas;
- b) atinjam um estado onde nenhum disparo está habilitado;
- c) atinjam um número máximo de eventos arbitrariamente definido. Quando esta opção é adotada, está se supondo que este número de eventos é suficiente para verificar a propriedade (isto é, para que o evento e_f ocorra). Caso isto não seja verdade, o objeto em questão deve ser novamente analisado, de forma a incluir um maior número de eventos nos cenários.

Para os demais casos, a busca de cenários é realizada até que os cenários gerados:

- a) resultem em marcações já anteriormente alcançadas, o que indica que qualquer cenário para a evolução do objeto é uma combinação das seqüências de disparos definidas;
- b) resultem no disparo de $t_{i_y.Ow}$ ou atinjam a marcação M_f ;
- c) até que nenhum evento esteja habilitado, o que indica que neste cenário o evento e_f não ocorre. Para que a propriedade seja verdadeira, deve-se então provar que este cenário é impossível.

➤ *Exemplo:* Para a **Propriedade 1** do sistema da Fig. 4.16 (Caso 3), o primeiro objeto a ser analisado é $O_{1.1}$. A análise da parte discreta deste objeto consiste em determinar os possíveis cenários a partir da solicitação de enchimento da bandeja até que o sistema entre em repouso (*Busca 1*).

- *Busca 1 – Especificação do seqüente* - $\Gamma_0, M_0, !t_{1_y.Ow}, \dots, !t_{n_y.Ow}, t_{i_y.Ow} \vdash M_f \otimes \Gamma_f$:
 - De acordo com a Regra 2: M_0 = pós-condição de $t_{1_1.O1} = p_{2_1.O1}$.
 - De acordo com a Regra 6: $t_{i_y.Ow}$ é excluído e $M_f = p_{1_1.O1}$.
 - De acordo com a Regra 8: $!t_{1_y.Ow}, \dots, !t_{n_y.Ow} = !t_{1_1.O1}, !t_{2_1.O1}, !t_{3_1.O1}, !t_{4_1.O1}, !t_{5_1.O1}, !t_{6_1.O1}$.

Fig. 4.19. Ordem de disparos dos **Cenários 1 a 4** para $O_{1.1}$ - Propriedade 1.

4.3.3.6. *Etapa 4.2 – Elaboração de Hipóteses*

As hipóteses são definidas da mesma forma que as restrições. Observa-se, no entanto, que diferentemente das restrições, as hipóteses devem ser provadas para que a propriedade em questão possa ser considerada verdadeira. Tendo como base os estudos de caso (apresentados no Capítulo 5, 6 e 7), neste trabalho foram especificados 9 tipos de restrições (H1 a H9), correspondentes aos 9 tipos de restrições (R1 a R9).

➤ *Exemplo:* Para a análise de $O_{1.1}$ no caso da **Propriedade 1** do sistema da Fig. 4.16, é feita a seguinte hipótese (a enumeração das hipóteses é feita da mesma forma que a enumeração das restrições):

- Hipótese 1A (correspondente a H1) – Quando solicitado por M_1 , a máquina M_2 sempre está imediatamente disponível para iniciar o enchimento de um copo: $t_{3_1.O1/1_2.O2}$ ($= t_{a_b.Oc/d_e.Of}$) dispara no instante de habilitação de $t_{3_1.O1/1_2.O2}$ em $O_{1.1}$.

4.3.3.7. *Etapa 4.3 – Parte Contínua – Evolução de variáveis contínuas e datas de disparos*

A análise da parte contínua consiste em determinar para cada cenário a data de disparo das transições em relação a ocorrência do evento e_0 , o valor das variáveis contínuas, e a viabilidade do cenário em situações de conflito. As datas de disparo das transições e os valores das variáveis contínuas estão intrinsecamente relacionados: a habilitação de transições pode depender do valor das variáveis contínuas, e por sua vez, o valor das variáveis pode depender do tempo de permanência em um determinado estado.

Uma vez que as redes PTD-OO não restringem o tipo de sistemas de equações diferenciais ou o tipo de expressão das funções de junção e habilitação, o estabelecimento de um procedimento analítico para sua resolução não é viável. Além disso, em muitos casos, os dados necessários para determinar as datas de disparo e os valores das variáveis para um determinado cenário não são completamente conhecidos. Deve-se, então, a partir das informações disponíveis, estabelecer um conjunto de expressões que restrinjam os possíveis valores destas variáveis.

Algumas situações são discutidas a seguir:

- O objeto não possui nenhuma função de habilitação, não compartilha nenhuma variável e os eventos e_0 , e_i e e_f não estão relacionados ao valor de suas eventuais variáveis. Neste caso a eventual evolução de suas variáveis não influenciará na verificação da propriedade e , portanto, não precisa ser determinada.
- O cenário considerado inclui sistemas de equações, funções de junção ou funções de habilitação que utilizam variáveis externas. Neste caso duas abordagens podem ser adotadas:
 - a) É feita uma hipótese sobre o comportamento desta variável ou sobre seus possíveis valores.
 - b) Suspende-se a análise do objeto em questão e analisa-se o objeto de onde provém a variável externa, de forma a estabelecer o seu comportamento. Em seguida retoma-se a análise do primeiro objeto.
- O cenário considerado inclui disparos de transições de interface. Duas abordagens podem ser adotadas:
 - a) É feita uma hipótese restringindo a data de disparo da transição.

- b) Nenhum hipótese é feita e deve-se então analisar o outro objeto envolvido no disparo da transição, a menos que a propriedade seja comprovada verdadeira para qualquer comportamento deste objeto.

A análise da parte contínua pode resultar em cenários impossíveis. Um exemplo é quando a função de habilitação de uma das transições do cenários não se torna nunca verdadeira. Neste caso, ou o objeto terá atingido um estado de ‘deadlock’ e a propriedade não será verdadeira, ou ocorre o disparo de alguma outra transição, correspondente a um dos demais cenários definidos, e a propriedade será verdadeira se este segundo cenário for verdadeiro.

➤ *Exemplo:* Apresenta-se a seguir a análise da parte contínua de $O_{1,1}$ no caso da **Propriedade 1** do sistema da Fig. 4.16. Esta análise resulta que o único cenário possível é o **Cenário 4**, todos os demais são impossíveis, pois a condição para que a bandeja seja retirada (disparo de $t_{5,1.O1}$) é que exatamente 4 copos estejam cheios ($e_{5,1.O1}$).

- **Cenário 1:**

- $\theta_{2,1.O1} = \theta_{1,1.O1} + 2$ (resultado de $j_{1,1}$, $F_{2,1}$ e $e_{2,1}$); $N=1$ (resultado de $j_{2,1}$);
- $\theta_{3,1.O1/1,2.O1} = \theta_{2,1.O1}$ (resultado da Hipótese 1A);
- $\theta_{4,1.O1/4,2.O1} \geq \theta_{3,1.O1/1,2.O1}$;
- $e_{5,1.O1}$: $N=4$ não pode ser satisfeita, portanto o **Cenário 1** é impossível - (pelo menos um dos **Cenários i** ($i>1$) deve ser possível).

- **Cenário 2:**

- $\theta_{2,1.O1} = \theta_{1,1.O1} + 2$ (resultado de $j_{1,1}$, $F_{2,1}$ e $e_{2,1}$); $N=1$ (resultado de $j_{2,1}$);
- $\theta_{3,1.O1/1,2.O1}^{(1)} = \theta_{2,1.O1}$ (resultado da Hipótese 1A);
- $\theta_{4,1.O1/4,2.O1}^{(1)} \geq \theta_{3,1.O1/1,2.O1}^{(1)}$;
- $\theta_{6,1.O1} = \theta_{4,1.O1/4,2.O1}^{(1)} + 2$ (resultado de $j_{4,1}$, $F_{5,1}$ e $e_{6,1}$); $N=2$ (resultado de $j_{6,1}$);
- $\theta_{3,1.O1/1,2.O1}^{(2)} = \theta_{6,1.O1} = \theta_{4,1.O1/4,2.O1}^{(1)} + 2$ (resultado da Hipótese 1A);
- $\theta_{4,1.O1/4,2.O1}^{(2)} \geq \theta_{3,1.O1/1,2.O1}^{(2)}$;
- $e_{5,1.O1}$: $N=4$ não pode ser satisfeita, portanto o **Cenário 2** é impossível - (pelo menos um dos **Cenários i** ($i>2$) deve ser possível)

- **Cenário 3:** da mesma forma que os **Cenários 1 e 2** esta análise também resulta na conclusão de que **Cenário 3 é impossível** - (pelo menos um dos **Cenários i** ($i > 3$) deve ser verdadeiro).
- **Cenário 4:**
 - $\theta_{2_1.O1} = \theta_{1_1.O1} + 2$; $N=1$;
 - $\theta_{3_1.O1/1_2.O1}^{(1)} = \theta_{2_1.O1}$;
 - $\theta_{4_1.O1/4_2.O1}^{(1)} \geq \theta_{3_1.O1/1_2.O1}^{(1)} = \theta_{1_1.O1} + 2$;
 - $\theta_{6_1.O1}^{(1)} = \theta_{4_1.O1/4_2.O1}^{(1)} + 1$; $N=2$;
 - $\theta_{3_1.O1/1_2.O1}^{(2)} = \theta_{6_1.O1}^{(1)} = \theta_{4_1.O1/4_2.O1}^{(1)} + 1$;
 - $\theta_{4_1.O1/4_2.O1}^{(2)} \geq \theta_{3_1.O1/1_2.O1}^{(2)} = \theta_{4_1.O1/4_2.O1}^{(1)} + 1$;
 - $\theta_{6_1.O1}^{(2)} = \theta_{4_1.O1/4_2.O1}^{(2)} + 2$; $N=3$;
 - $\theta_{3_1.O1/1_2.O1}^{(3)} = \theta_{6_1.O1}^{(2)} = \theta_{4_1.O1/4_2.O1}^{(2)} + 1$;
 - $\theta_{4_1.O1/4_2.O1}^{(3)} \geq \theta_{3_1.O1/1_2.O1}^{(3)} = \theta_{4_1.O1/4_2.O1}^{(2)} + 1$;
 - $\theta_{6_1.O1}^{(3)} = \theta_{4_1.O1/4_2.O1}^{(3)} + 2$; $N=4$;
 - $\theta_{3_1.O1/1_2.O1}^{(4)} = \theta_{6_1.O1}^{(3)} = \theta_{4_1.O1/4_2.O1}^{(3)} + 2$;
 - $\theta_{4_1.O1/4_2.O1}^{(4)} \geq \theta_{3_1.O1/1_2.O1}^{(4)} = \theta_{4_1.O1/4_2.O1}^{(3)} + 2$;
 - $\theta_{5_1.O1} = \theta_{4_1.O1/4_2.O1}^{(4)} + 2$; $N=1$.
 - Para que a propriedade seja verdadeira, tem-se:

$$- \theta_{5_1.O1} - \theta_{1_1.O1} = [2 + (\theta_{4_1.O1/4_2.O1}^{(1)} - \theta_{3_1.O1/1_2.O1}^{(1)}) + 1 + (\theta_{4_1.O1/4_2.O1}^{(2)} - \theta_{3_1.O1/1_2.O1}^{(2)}) + 1 + (\theta_{4_1.O1/4_2.O1}^{(3)} - \theta_{3_1.O1/1_2.O1}^{(3)}) + 1 + (\theta_{4_1.O1/4_2.O1}^{(4)} - \theta_{3_1.O1/1_2.O1}^{(4)}) + 2] < 20.$$
- **Cenário i** (onde $i > 4$): da mesma forma que os **Cenários 1 e 2** esta análise também resulta na conclusão de que **Cenário i é impossível**, pois a condição para o disparo de $t_{6_1.O1}^{(4)}$ (e_{6_1} : $N < 4$) nunca será satisfeita.

4.3.3.8. **Etapa 5 – Análise do Demais Objetos**

Uma vez determinado o conjunto de cenários que representam o comportamento do 1º objeto (**Etapa 4**), os próximos objetos a serem analisados são aqueles que cujas transições ou variáveis estão presentes nestes cenários.

Esta análise pode resultar em novas obrigações de análise, e assim sucessivamente, até que todos os objetos cujo comportamento é relevante para propriedade sejam analisados.

4.3.3.9. *Etapa 5.1 – Parte Discreta – Busca de cenários*

Para cada **Cenário i** resultante da análise do 1º objeto, é realizada uma análise no objeto em questão. Chamando genericamente o 1º objeto de $O_{w,y}$ e o objeto que está sendo analisado de $O_{v,u}$, esta análise é detalhada a seguir.

Cada análise é dividida em $n+1$ buscas, onde n é o número de disparo de transições da interface entre $O_{w,y}$ e $O_{v,u}$ que estão presentes no **Cenário i**. Estes disparos são chamados genericamente de $t_1, t_2, \dots, t_n$. Cada busca corresponde a determinar o comportamento de $O_{v,u}$ entre dois disparos: a *Busca 1* corresponde ao comportamento até o disparo de t_1 , a *Busca 2* entre t_1 e t_2 , e assim sucessivamente, até a *Busca n*, que corresponde ao comportamento de $O_{v,u}$ após o disparo de t_n . Este procedimento é ilustrado na Fig. 4.20.

Fig. 4.20. Busca de cenários nos demais objetos para propriedades de alcançabilidade.

O seqüente para cada busca é composto por: $\Gamma_0, M_0, !t_{1,y.Ow}, \dots, !t_{n,y.Ow} \vdash M_f \otimes \Gamma_f$. As marcações M_0, M_f e as transições do conjunto de disparos ' $!t_{1,y.Ow}, \dots, !t_{n,y.Ow}$ ' são definidas pelas seguintes regras:

- Regra 10 – Para $j = 1$ até n , no seqüente da *Busca j* tem-se M_f = pré-condição de t_j .
- Regra 11 – Para $j = 1$ até n , no seqüente da *Busca j+1* tem-se M_0 = pós-condição de t_j .
- Regra 12 – O conjunto de disparo ' $!t_{1,u.Ov}, \dots, !t_{n,u.Ov}$ ' contém todas as transições do objeto $O_{v,u}$ com exceção das transição da interface entre $O_{v,u}$ e $O_{w,y}$ e de eventuais restrições presentes na definição da propriedade a ser verificada.
- Regra 13 – Para a *Busca 1*, se nenhuma informação é fornecida sobre o estado do objeto do ponto de vista discreto no instante de ocorrência de e_0 , então a *Busca 1* é decomposta em ' m ' buscas, onde ' m ' é o número de marcações alcançáveis por

aquele objeto. Em cada busca, M_0 corresponde a uma marcação diferente e $\Gamma_0 = \emptyset$.

- Regra 14 – Para a *Busca* $n+1$, se nenhuma informação é fornecida sobre o estado do objeto do ponto de vista discreto no instante de ocorrência de e_f , então $M_f = \emptyset$.
- Regra 15 – Se $n=0$, M_0 e M_f são definidos de acordo com as Regra 13 e 14.

Eventualmente, se o comportamento de $O_{v,u}$ antes da 1ª interação com $O_{w,y}$ (disparo de t_1) e/ou após a última interação (disparo de t_n) for considerado irrelevante para a verificação da propriedade, as *Buscas* 1 e/ou $n+1$ podem ser omitidas.

A *Busca* $n+1$ é realizada até que os cenários gerados:

- d) resultem em marcações já anteriormente alcançadas;
- e) atinjam um estado onde nenhum disparo está habilitado;
- f) atinjam um número máximo de eventos arbitrariamente definido.

As *Buscas* 1 até n são realizadas até que os cenários gerados:

- d) resultem em marcações já anteriormente alcançadas;
- e) resultem em M_f ;
- g) atinjam um estado onde nenhum disparo está habilitado (neste caso, para que a propriedade seja verdadeira, deve-se então provar que este cenário é impossível).

Observa-se que, quando uma busca resulta em mais de um comportamento possível para o objeto analisado, são criados dois ou mais cenários a partir do cenário definido na análise do 1º objeto, estes cenários são chamados de **Cenário i-1**, **Cenário i-2**, etc.

➤ *Exemplo:* Para a **Propriedade 1** do sistema da Fig. 4.16, o segundo objeto analisado é $\underline{M}_2$ ($O_{1,2}$). O único cenário possível resultante da análise de $O_{1,1}$ é o **Cenário 4**, para o qual a análise de $O_{1,2}$ está dividida em 9 buscas:

- *Busca 1* – Esta busca é omitida porque a Hipótese 1A impõe que $t_{3_1.01/1_2.02}$ é imediatamente disparada.
- *Buscas 2, 4, 6 e 8* – O seqüente a ser buscado é $\Gamma_0, p_{2_2.01}, !t_{2_2.01} \vdash p_{3_2.01} \otimes \Gamma_f$ ($t_{3_2.01}$ é excluída por causa da Restrição 2A), a construção da árvore do seqüente resulta em $\Gamma_0 = \Gamma_f = \emptyset$ e em um único disparo de $t_{2_2.01}$:

$$\frac{p_{2_2.O1} \multimap p_{2_2.O1} \quad \Gamma_0, p_{3_2.O1}, !t_{2_2.O1} \multimap p_{3_2.O1} \otimes \Gamma_f}{\Gamma_0, p_{2_2.O1}, !t_{2_2.O1} \vdash p_{3_2.O1} \otimes \Gamma_f} \multimap O L (t_{2_2.O1})$$

- *Buscas 3, 5 e 7* – O seqüente a ser buscado é $\Gamma_0, p_{1_2.O1}, !t_{2_2.O1} \vdash p_{1_2.O1} \otimes \Gamma_f$, que resulta em $\Gamma_0 = \Gamma_f = \emptyset$ e em nenhum disparo.
- *Busca 9* – $\Gamma_0, p_{1_2.O1}, !t_{2_2.O1} \vdash \Gamma_f$, que resulta em $\Gamma_0 = \emptyset$, $\Gamma_f = p_{1_2.O1}$ e nenhum disparo.
- *Definição dos Cenários* – Como resultado das buscas acima é definido o seguinte cenário para os eventos neste objeto (Fig. 4.21):
 - **Cenário 4:** $t_{3_1.O1/1_2.O1}^{(1)}$; $t_{2_2.O1}^{(1)}$; $t_{4_1.O1/4_2.O1}^{(1)}$; $t_{3_1.O1/1_2.O1}^{(2)}$; $t_{2_2.O1}^{(2)}$; $t_{4_1.O1/4_2.O1}^{(2)}$; $t_{3_1.O1/1_2.O1}^{(3)}$; $t_{2_2.O1}^{(3)}$; $t_{4_1.O1/4_2.O1}^{(3)}$; $t_{3_1.O1/1_2.O1}^{(4)}$; $t_{2_2.O1}^{(4)}$; $t_{4_1.O1/4_2.O1}^{(4)}$.

Fig. 4.21. Ordem de disparos do **Cenário 4** para O_{1.2} - Propriedade 1.

4.3.3.10. Etapas 5.2 e 5.3 – Elaboração de Hipóteses e Parte Contínua – Evolução de variáveis contínuas e datas de disparos

São realizadas da mesma forma que para o 1º objeto analisado.

➤ *Exemplo:* Para a análise de O_{1.2} no caso da **Propriedade 1** do sistema da Fig. 4.16, nenhuma hipótese é elaborada. A análise da parte contínua resulta em:

- **Cenário 4:**
 - $\theta_{2_2.O1}^{(1)} = \theta_{3_1.O1/1_2.O1}^{(1)} + 2$ (resultado de j_{1_2} , F_{2_2} e e_{2_2});
 - $\theta_{4_1.O1/4_2.O1}^{(1)} = \theta_{2_2.O1}^{(1)} = \theta_{3_1.O1/1_2.O1}^{(1)} + 2$ (pois a única restrição em O_{1.1} é $\theta_{4_1.O1/4_2.O1}^{(1)} \geq \theta_{3_1.O1/1_2.O1}^{(1)}$);
 - $\theta_{4_1.O1/4_2.O1}^{(2)} = \theta_{2_2.O1}^{(2)} = \theta_{3_1.O1/1_2.O1}^{(2)} + 2$;
 - $\theta_{4_1.O1/4_2.O1}^{(3)} = \theta_{2_2.O1}^{(3)} = \theta_{3_1.O1/1_2.O1}^{(3)} + 2$;
 - $\theta_{4_1.O1/4_2.O1}^{(4)} = \theta_{2_2.O1}^{(4)} = \theta_{3_1.O1/1_2.O1}^{(4)} + 2$;

- Verifica-se então a condição imposta em $O_{1.1}$ para veracidade do cenário:
 - $\theta_{5_1.01} - \theta_{1_1.01} = [2 + 2 + 1 + 2 + 1 + 2 + 1 + 2 + 2] = 15 < 20$
- Como a análise do objeto $O_{1.2}$ não envolve a interação deste com outros objetos, além do já analisado $O_{1.1}$, a **Etapa 5** é interrompida. A única evolução possível para o sistema a partir do evento e_0 corresponde ao **Cenário 4**, que, de acordo com a análise realizada, *satisfaz a Propriedade 1* (se a Hipótese 1A for verdadeira).

4.3.3.11. **Etapa 6** – Construção dos Seqüentes Globais

A composição das análises realizadas para cada objeto pode ser verificada, do ponto de vista discreto, através da construção da árvore de prova de um seqüente global, contendo todos os eventos que ocorrem em todos os objetos analisados, de e_0 a e_f . Se as **etapas** anteriores foram realizadas corretamente, deve ser possível construir a árvore de prova do seqüente global correspondente a cada cenário.

Este seqüente global é composto por: $M_{0_T}, T \vdash M_{f_T}$, onde:

- M_{0_T} : bloco de fórmulas conectadas por ‘,’. Cada fórmula corresponde a marcação ‘ M_0, Γ_0 ’ definida para o seqüente da *Busca 1* de um objeto analisado (caso a *Busca 1* não tenha sido realizada, utiliza-se Γ_0 da *Busca 2* e M_0 =pré-condição de t_1).
- M_{f_T} : fórmula resultante da composição de um conjunto de fórmulas, usando o conector ‘ $\otimes$ ’. Cada fórmula deste conjunto corresponde a marcação ‘ $M_f \otimes \Gamma_f$ ’ definida para o seqüente da *Busca n+1* de um objeto analisado.
- T : bloco de fórmulas conectadas por ‘,’. Cada fórmula corresponde ao conjunto de transições disparados para todas as buscas de um objeto analisado.

➤ *Exemplo:* O seqüente global para o Cenário 4 da **Propriedade 1** do sistema da Fig. 4.16 é apresentada a seguir. A construção da árvore de prova é realizada através da aplicação da regra ‘ $\rightarrow$ ’, da forma como ilustrada anteriormente. A ordem parcial de disparos, obtida através da construção da árvore de prova, é apresentada na Fig. 4.22 e ilustra a relação de causalidade entre os eventos.

$$- M_{0_T} = \underbrace{p_{2_1.01}}_{de\ O_{1.1}}, \underbrace{p_{1_2.01}}_{de\ O_{1.2}}$$

4.3.4. Propriedades de Segurança

4.3.4.1. *Etapa 1 - Definição do enunciado da propriedade*

As propriedades de segurança consideradas neste trabalho são definidas através do seguinte enunciado:

PS1. Um determinado estado, definido através da especificação parcial ou completa da marcação $m_{w,y}$ de um objeto $O_{w,y}$, nunca é alcançado (exemplos: **Propriedade 1** do Estudo de Caso 2 (Capítulo 6) e **Propriedade 2** do Estudo de Caso 3 (Capítulo 7)).

➤ *Exemplo:* Para o sistema da Fig. 4.16, um exemplo de propriedade de segurança a ser verificada é:

- **Propriedade 2** (correspondente a PS1) – O estado ‘Reservatório vazio’ nunca é atingido: $m_{w,y} = m_{1,2} = \{p_{4_2,01}\}$.

4.3.4.2. *Etapa 2 - Definição do conjunto de restrições da propriedade*

A definição da propriedade também pode conter restrições, de forma semelhante ao apresentado para as propriedades de alcançabilidade.

➤ *Exemplo:* Para a **Propriedade 2** do exemplo da Fig. 4.16 considera-se a seguinte restrição:

- Restrição 2A (correspondente a R8) – O valor da vazão de entrada de produto em $\underline{M}_2$ se encontra sempre entre 10 e 15:
 - $q(\theta)$ (= variável de $X_{c,b}=X_{1,2}$) $\in [7, 15]$, para $0 (= \theta_g) \leq \theta \leq \infty (= \theta_h)$.
- Restrição 2B (correspondente a R8) – O valor inicial do volume de produto no reservatório de $\underline{M}_2$ se encontra entre 20 e 30 litros:
 - $V_R(\theta)$ (= variável de $X_{c,b}=X_{1,2}$) $\in [10, 20]$, para $\theta=0 (= \theta_g=\theta_h)$.

4.3.4.3. *Etapa 3 – Construção dos Diagramas de Colaboração Estáticos*

Esta **etapa** é realizada da mesma forma para o caso de propriedades de alcançabilidade e de segurança.

4.3.4.4. *Etapa 4 – Análise do 1º Objeto*

O primeiro objeto a ser analisado é aquele cuja marcação $m_{w,y}$ não pode ser alcançada.

No caso de propriedades de segurança utiliza-se o raciocínio para trás para determinar os possíveis cenários que resultam no estado proibido. Deve-se então provar que todos os cenários são impossíveis, ou seja, que para cada cenário existe uma transição (genericamente chamada de $t_{i,y,ow}$) que jamais estará habilitada.

4.3.4.5. *Etapa 4.1 – Parte Discreta – Busca de cenários*

Para determinar os cenários que resultam em $m_{w,y}$ o seguinte seqüente é analisado: *Busca 1* - $\Gamma_0, !t_{1,y,ow}, \dots, !t_{n,y,ow} \vdash M_f, \Gamma_f$, onde:

- Regra 16 - $M_f = m_{w,y}$
- Regra 17 - ' $!t_{1,y,ow}, \dots, !t_{n,y,ow}$ ' contém todas as transições do objeto $O_{w,y}$ com exceção de eventuais restrições presentes na definição da propriedade a ser verificada.

A busca de cenários deve ser realizada até que:

- a) resultem em marcações já anteriormente alcançadas;
- b) atinjam um estado onde nenhum disparo está habilitado;
- c) atinjam um número máximo de eventos arbitrariamente definido.

Para cada cenário encontrado, seleciona-se então um disparo de transição $t_{i,y,ow}$ que não deverá ocorrer para que a propriedade seja verdadeira. Como as hipóteses, esta escolha é realizada pela pessoa que está fazendo a análise tendo como base o seu conhecimento sobre o sistema. Caso a propriedade não seja provada considerando este disparo, um outro disparo do cenário é selecionado e repete-se o procedimento de análise.

Tendo como base os estudos de caso (Capítulos 5, 6 e 7), as seguintes situações foram identificadas para que o disparo $t_{i,y,ow}$ não ocorra (ilustradas através de exemplos na (Fig. 4.23):

- Caso 1 - $t_{i,y,ow}$ possui uma função de habilitação que nunca se torna verdadeira;
- Caso 2 - Existe uma transição $t_{j,y,ow}$ em conflito com $t_{i,y,ow}$, e a função de habilitação de $t_{j,y,ow}$ se torna verdadeira *antes* ($\Delta\theta > 0$) da função de habilitação de $t_{i,y,ow}$, portanto $t_{j,y,ow}$ *sempre* dispara no lugar de $t_{i,y,ow}$.

- Caso 3 - Existe uma transição $t_{i_y.Ow}$ em conflito com $t_{i_y.Ow}$, e as demais condições, do ponto de vista discreto, para o disparo de $t_{i_y.Ow}$ são satisfeitas *após* ($\Delta\theta > 0$) a satisfação de todas as condições para o disparo de $t_{i_y.Ow}$, portanto $t_{i_y.Ow}$ *sempre* dispara no lugar de $t_{i_y.Ow}$.
- Caso 4 - Existe uma transição $t_{i_y.Ow}$ em conflito com $t_{i_y.Ow}$, e uma das condições, do ponto de vista discreto, para o disparo de $t_{i_y.Ow}$ pode ser satisfeita apenas pelo disparo de $t_{i_y.Ow}$, o que significa que $t_{i_y.Ow}$ nunca terá todas as suas condições para disparo satisfeitas simultaneamente.

Fig. 4.23. Exemplos dos Casos 1 a 4, onde o disparo de $t_{i_y.Ow}$ é impossível.

Nos Casos 2, 3 e 4 os cenários contendo o disparo de $t_{i_y.Ow}$ são chamados de *cenários proibidos* (Cenário ip), enquanto os respectivos cenários contendo o disparo de $t_{i_y.Ow}$ são chamados de *cenários concorrentes* (Cenário ic).

➤ *Exemplo:* Para a **Propriedade 2** do sistema da Fig. 4.16, o primeiro objeto a ser analisado é $O_{1,2}$. A análise da parte discreta consiste na seguinte busca.

- *Busca 1* – $\Gamma_0, !t_{1_2.O1}, !t_{2_2.O1}, !t_{3_2.O1}, !t_{4_2.O1} \vdash p_{3_2.O1}, \Gamma_f$:

$$\begin{array}{c}
 \frac{p_{1_2.O1} \vdash p_{1_2.O1} \quad \Gamma_0, !t_{1_2.O1}, !t_{2_2.O1}, !t_{3_2.O1}, !t_{4_2.O1}, !t_{5_1.O1}, !t_{6_1.O1} \vdash p_{2_2.O1}, \Gamma_f}{p_{1_2.O1} \vdash p_{1_2.O1} \quad \Gamma_0, !t_{1_2.O1}, !t_{2_2.O1}, !t_{3_2.O1}, !t_{4_2.O1}, !t_{5_1.O1}, !t_{6_1.O1} \vdash p_{4_2.O1}, \Gamma_f} \text{---} \text{O L } (t_{2_2.O1}) \\
 \frac{p_{2_2.O1} \vdash p_{2_2.O1} \quad \Gamma_0, !t_{1_2.O1}, !t_{2_2.O1}, !t_{3_2.O1}, !t_{4_2.O1}, !t_{5_1.O1}, !t_{6_1.O1} \vdash p_{1_2.O1}, \Gamma_f}{p_{2_2.O1} \vdash p_{2_2.O1} \quad \Gamma_0, !t_{1_2.O1}, !t_{2_2.O1}, !t_{3_2.O1}, !t_{4_2.O1}, !t_{5_1.O1}, !t_{6_1.O1} \vdash p_{2_2.O1}, \Gamma_f} \text{---} \text{O L } (t_{4_2.O1}) \\
 \frac{p_{4_2.O1} \vdash p_{4_2.O1} \quad \Gamma_0, !t_{1_2.O1}, !t_{2_2.O1}, !t_{3_2.O1}, !t_{4_2.O1}, !t_{5_1.O1}, !t_{6_1.O1} \vdash p_{2_2.O1}, \Gamma_f}{\Gamma_0, !t_{1_2.O1}, !t_{2_2.O1}, !t_{3_2.O1}, !t_{4_2.O1}, !t_{5_1.O1}, !t_{6_1.O1} \vdash p_{4_2.O1}, \Gamma_f} \text{---} \text{O L } (t_{3_2.O1})
 \end{array}$$

- *Definição dos cenários proibidos* – Existem infinitos cenários que levam do estado inicial ao estado proibido. Cada ‘**Cenário i**’ ($1 \leq i \leq \infty$) corresponde ao caso onde são enchidos completamente ‘i - 1’ copos antes do reservatório de M_2 estar completamente vazio. Em todos os casos, tem-se que $\Gamma_0 = \Gamma_f = \emptyset$. A ordem de disparos em cada caso é apresentada a seguir, quando um cenário possui mais de um disparo, estes são identificados por um número entre parênteses:

- **Cenário 1p**: $t_{3_2.O1}; t_{1_2.O1/3_1.O1}$;
- **Cenário 2p**: $t_{3_2.O1}; t_{1_2.O1/3_1.O1}^{(2)}; t_{4_2.O1/4_1.O1}; t_{2_2.O1}^{(1)}; t_{1_2.O1/3_1.O1}^{(1)}$;
- ...
- **Cenário ip**: $t_{3_2.O1}; t_{1_2.O1/3_1.O1}^{(i)}; i^*(t_{4_2.O1/4_1.O1}^{(0)}; t_{2_2.O1}^{(0)}; t_{1_2.O1/3_1.O1}^{(0)})$;

- *Definição dos cenários concorrentes* – Para todos os cenários seleciona-se o disparo de $t_{3_2.O1}$ para verificar a propriedade. Do ponto de vista discreto esta transição está em conflito com $t_{2_2.O1}$, portanto são determinados os seguintes cenários concorrentes:

- **Cenário 1c**: $t_{2_2.O1}; t_{1_2.O1/3_1.O1}$;
- **Cenário 2c**: $t_{2_2.O1}^{(2)}; t_{1_2.O1/3_1.O1}^{(2)}; t_{4_2.O1/4_1.O1}; t_{2_2.O1}^{(1)}; t_{1_2.O1/3_1.O1}^{(1)}$;
- ...
- **Cenário ic**: $t_{2_2.O1}^{(i)}; t_{1_2.O1/3_1.O1}^{(i)}; i^*(t_{4_2.O1/4_1.O1}^{(0)}; t_{2_2.O1}^{(0)}; t_{1_2.O1/3_1.O1}^{(0)})$;

- *Condição p/ Propriedade 2* – Uma vez que não existem outras pre-condições para o disparo de $t_{2_2.O1}$ ou de $t_{3_2.O1}$, para verificarmos a **Propriedade 2** devemos provar que, após o disparo de $t_{1_2.O1/3_1.O1}$, e_{2_2} se torna verdadeira antes de $e_{3_2.O1}$ (Caso 2).

4.3.4.6. Etapas 4.2 e 4.3 – Elaboração de Hipóteses e Parte Contínua – Evolução de variáveis contínuas e datas de disparos

São realizadas da mesma forma que para o caso de propriedades de alcançabilidade. Após esta análise um conjunto de condições para a não ocorrência dos cenários proibidos ou para a ocorrência dos cenários concorrentes no lugar dos cenários proibidos é determinado.

➤ *Exemplo:* Apresenta-se a seguir a análise da parte contínua de $O_{1,2}$ no caso da Propriedade 2 do sistema da Fig. 4.16:

- **Cenário 1p e 1c:**

- Para **Cenário 1c**: $\theta_{2,2,01} = \theta_{1,2,01/3_1,01} + 2$ (resultado de $j_{1,2}$, $F_{2,2}$ e $e_{2,2}$);
- Portanto para **Cenário 1p**: $\theta_{1,2,01/3_1,01} \leq \theta_{3,2,01} \leq \theta_{1,2,01/3_1,01} + 2$;
- Mas de acordo com $e_{3,2}$, para **Cenário 1p**:

$$- V_R(\theta_{3,2,01}) = V_R(\theta_{1,2,01/3_1,01}) + \int_{\theta_{1,2,01/3_1,01}}^{\theta_{3,2,01}} (q - 10).d\theta < 0;$$

- Para **Cenário 1c e 1p**: $V_R(\theta_{1,2,01/3_1,01}) = V_R(0)$;
- Tem-se então que:
 - $V_R(\theta_{3,2,01}) \geq \min(V_R(0)) + (\min(q)-10) * \max(\theta_{3,2,01} - \theta_{1,2,01/3_1,01})$
 - $V_R(\theta_{3,2,01}) \geq 10 - 3*2 = 4 > 0 \Rightarrow$ Portanto o **Cenário 1** é impossível.

- **Cenário 2p e 2c:**

- Para **Cenário 2c**: $\theta_{2,2,01}^{(2)} = \theta_{1,2,01/3_1,01}^{(2)} + 2$;
- Portanto para **Cenário 2p**: $\theta_{1,2,01/3_1,01}^{(2)} \leq \theta_{3,2,01} \leq \theta_{1,2,01/3_1,01}^{(2)} + 2$;
- Mas de acordo com $e_{3,2}$, para **Cenário 2p**:

$$- V_R(\theta_{3,2,01}) = V_R(\theta_{1,2,01/3_1,01}^{(2)}) + \int_{\theta_{1,2,01/3_1,01}^{(2)}}^{\theta_{3,2,01}} (q - 10).d\theta < 0;$$

- Para **Cenário 2c e 2p**:
 - $\theta_{1,2,01/3_1,01}^{(2)} \geq \theta_{4,2,01/4_1,01}$;
 - $V_R(\theta_{1,2,01/3_1,01}^{(2)}) \geq V_R(\theta_{4,2,01/4_1,01}) + (\theta_{1,2,01/3_1,01}^{(2)} - \theta_{4,2,01/4_1,01}) * \min(q)$;
 - $\theta_{4,2,01/4_1,01}^{(2)} \geq \theta_{2,2,01}$;
 - $V_R(\theta_{4,2,01/4_1,01}) \geq V_R(\theta_{2,2,01}) + (\theta_{4,2,01/4_1,01} - \theta_{2,2,01}) * \min(q)$;

- $\theta_{2_2.O1} = \theta_{1_2.O1/3_1.O1}^{(1)} + 2$;
- $V_R(\theta_{2_2.O1}) = V_R(\theta_{1_2.O1/3_1.O1}^{(1)}) + 2 * [\min(q) - 10]$;
- $V_R(\theta_{1_2.O1/3_1.O1}^{(1)}) = V_R(0)$
- Tem-se então que:
 - $V_R(\theta_{3_2.O1}) \geq 10 + \min(q) * [(\theta_{4_2.O1/4_1.O1} - \theta_{2_2.O1}) + (\theta_{1_2.O1/3_1.O1}^{(2)} - \theta_{4_2.O1/4_1.O1})] + [\min(q)-10] * [\max(\theta_{3_2.O1} - \theta_{1_2.O1/3_1.O1}^{(2)}) + 2]$;
 - $V_R(\theta_{3_2.O1}) \geq 10 + 7 * [(\theta_{4_2.O1/4_1.O1} - \theta_{2_2.O1}^{(1)}) + (\theta_{1_2.O1/3_1.O1}^{(2)} - \theta_{4_2.O1/4_1.O1})] - 3 * 4$;
- Portanto para que o **Cenário 2p** seja possível é necessário que:
 - $10 + 7 * [(\theta_{4_2.O1/4_1.O1} - \theta_{2_2.O1}^{(1)}) + (\theta_{1_2.O1/3_1.O1}^{(2)} - \theta_{4_2.O1/4_1.O1})] < 12$;
- **Cenário ip ou ic**: seguindo um procedimento semelhante se obtém que a condição para que um **Cenário i** ($i > 2$) seja possível:
 - $10 + 7 * \sum_{j=1}^{i-1} [(\theta_{4_2.O1/4_1.O1}^{(j)} - \theta_{2_2.O1}^{(j)}) + (\theta_{1_2.O1/3_1.O1}^{(j+1)} - \theta_{4_2.O1/4_1.O1}^{(j)})] < 6 * i$

4.3.4.7. *Etapa 5 – Análise dos demais objetos*

Uma vez determinado o conjunto de cenários proibidos e concorrentes do 1º objeto, os próximos objetos a serem analisados são aqueles que cujas transições ou variáveis estão presentes na definição destes cenários. O procedimento é semelhante ao caso das propriedades de alcançabilidade, mas utiliza-se o ‘raciocínio para trás’ no lugar do ‘raciocínio para frente’.

Como no caso das propriedades de alcançabilidade, o processo continua até que todos os objetos cujo comportamento é relevante para propriedade tenham sido analisados.

4.3.4.8. *Etapa 5.1 – Parte Discreta – Busca de cenários*

Como no caso das propriedades de alcançabilidade, para cada **Cenário ip** e **ic** resultante da análise do 1º objeto ($O_{w,y}$), é realizada uma análise no objeto em questão. Chamando genericamente o objeto que está sendo analisado de $O_{v,u}$, para cada **Cenário ip** e **ic**, esta análise é dividida em $n+1$ buscas, onde n é o número de disparo de transições da interface entre $O_{w,y}$ e $O_{v,u}$ (chamados genericamente de $t_1, t_2, \dots, t_n$) que estão presentes neste cenário.

O seqüente para cada busca é composto por: $\Gamma_0 \not\vdash M_0, !t_{1,y.Ow}, \dots, !t_{n,y.Ow} \vdash M_f, \Gamma_f$. As marcações M_0 , M_f e as transições do conjunto de disparos ' $!t_{1,y.Ow}, \dots, !t_{n,y.Ow}$ ' são definidas pelas seguintes regras:

- Regra 18 – Para $j = 1$ até n , no seqüente da *Busca j* tem-se M_f = pré-condição de t_j .
- Regra 19 – Para $j = 1$ até n , no seqüente da *Busca j+1* tem-se M_0 = pós-condição de t_j .
- Regra 20 – O conjunto de disparo ' $!t_{1,u.Ov}, \dots, !t_{n,u.Ov}$ ' contém todas as transições do objeto $O_{v,u}$ com exceção das transições da interface entre $O_{v,u}$ e $O_{w,y}$ e de eventuais restrições presentes na definição da propriedade a ser verificada.
- Regra 21 – Para a *Busca n+1*, se nenhuma informação é fornecida sobre o estado do objeto do ponto de vista discreto no instante que o estado proibido é atingido, então a *Busca n+1* é decomposta em ' m ' buscas, onde m é o número de marcações alcançáveis por aquele objeto. Em cada busca, M_f corresponde a uma marcação diferente e $\Gamma_f = \emptyset$.
- Regra 22 – Para a *Busca 1*, $M_0 = \emptyset$.
- Regra 23 – Se $n=0$, M_0 e M_f são definidos de acordo com as Regra 21 e 22.

Eventualmente, se o comportamento de $O_{v,u}$ antes da 1ª interação com $O_{w,y}$ (disparo de t_1) e/ou após a última interação (disparo de t_n) for considerado irrelevante para a verificação da propriedade, as *Buscas 1* e/ou $n+1$ podem ser omitidas.

Observação: no caso específico dos **Cenários ic**, após cada disparo (no sentido inverso) deve-se verificar se, a partir do estado atingido alguma outra transição poderia ter sido disparada, isto é, se existe algum cenário possível além do **Cenário ic** e o correspondente ip (pois a verificação da propriedade deve garantir que o **Cenário 1c** sempre ocorrerá).

➤ *Exemplo:* Para a **Propriedade 2** do sistema da Fig. 4.16, o segundo objeto analisado é $\underline{M}_1$ ($O_{1,1}$). Para cada **Cenário ip** ou **ic** a análise da parte discreta é dividida em $(1+2*i)$ buscas:

- *Busca (1+2*i)* - A partir do disparo de $t_{1_2.O1/3_1.O1}^{(i)}$: Esta busca é omitida pois não é relevante p/ verificar a propriedade.
- Para $j=1$ até i , *Busca 2*j* - Do disparo de $t_{4_2.O1/4_1.O1}^{(i)}$ até a habilitação de $t_{1_2.O1/3_1.O1}^{(i)}$: $\Gamma_0 \not\models p_{5_1.O1}, !t_{1_1.O1}, !t_{2_1.O1}, !t_{5_1.O1}, !t_{6_1.O1} \vdash p_{3_1.O1}, \Gamma_f$ - a busca resulta em dois possíveis de cenários entre os dois eventos considerados, em ambos os casos, $\Gamma_0 = \Gamma_f = \emptyset$:

- Para $j=1$ até i , *Busca 2*j-1* - Do disparo de $t_{1_2.O1/3_1.O1}^{(i)}$ até a habilitação de $t_{4_2.O1/4_1.O1}^{(i)}$: $\Gamma_0 \not\models p_{4_1.O1}, !t_{1_1.O1}, !t_{2_1.O1}, !t_{5_1.O1}, !t_{6_1.O1} \vdash p_{4_1.O1}, \Gamma_f$ - a busca resulta em nenhum disparo e $\Gamma_0 = \Gamma_f = \emptyset$.
- *Busca 1* - Esta busca é omitida pois a data de disparo de $t_{1_2.O1/3_1.O1}^{(1)}$ não é relevante p/ verificar a propriedade.
- *Definição dos cenários* - como resultado das possíveis combinações das *Buscas 2j* (para $j=1$ até i), cada **Cenário ip** e **ic** resultante da análise de $O_{1,2}$ dá origem a 2^i cenários, chamados de **Cenários ip-1, ic-1, ip-2, ic-2, ..., ic-2ⁱ**. Por exemplo, no caso de $i=2$ os cenários resultantes são:
 - **Cenários 2p e 2c-1**: $t_{1_2.O1/3_1.O1}^{(2)}$; $t_{6_1.O1}$; $t_{4_2.O1/4_1.O1}$; $t_{1_2.O1/3_1.O1}^{(1)}$;
 - **Cenários 2p e 2c-2**: $t_{1_2.O1/3_1.O1}^{(2)}$; $t_{2_1.O1}$; $t_{1_1.O1}$; $t_{5_1.O1}$; $t_{4_2.O1/4_1.O1}$; $t_{1_2.O1/3_1.O1}^{(1)}$;

4.3.4.9. Etapas 5.2 e 5.3 – Elaboração de Hipóteses e Parte Contínua – Evolução de variáveis contínuas e datas de disparos

São realizadas da mesma forma que para o 1º objeto analisado.

Como no caso das propriedades de alcançabilidade, o processo continua até que todos os objetos cujo comportamento é relevante para propriedade sejam analisados.

➤ *Exemplo:* Resumidamente, no caso da **Propriedade 2** do sistema da Fig. 4.16 a análise da parte contínua de $O_{1,2}$ leva as seguintes conclusões, válida para todos os possíveis cenários:

- Para os casos onde antes do disparo de $t_{1_2.O1/3_1.O1}$ ocorre o disparo de $t_{6_1.O1}$, tem-se: $(\theta_{1_2.O1/3_1.O1}^{(j)} - \theta_{4_2.O1/4_1.O1}^{(j)}) = 1$
- Para os casos onde antes do disparo de $t_{1_2.O1/3_1.O1}$ ocorre o disparo de $t_{2_1.O1}$, tem-se: $(\theta_{1_2.O1/3_1.O1}^{(j)} - \theta_{4_2.O1/4_1.O1}^{(j)}) = 2$
- Em todos os casos tem-se: $(\theta_{4_2.O1/4_1.O1}^{(j)} - \theta_{2_2.O1}^{(j)}) = 0$;
- A condição para um cenário ser possível é então:
 - $10+7* \sum_{j=1}^{i-1} [(\theta_{4_2.O1/4_1.O1}^{(j)} - \theta_{2_2.O1}^{(j)}) + (\theta_{1_2.O1/3_1.O1}^{(j+1)} - \theta_{4_2.O1/4_1.O1}^{(j)})] < 6*i$
 - $10+7* \sum_{j=1}^{i-1} [...] \geq 10+7*\min(\sum_{j=1}^{i-1} [...]) = 10+7*i < 6*i \Rightarrow$ Condição impossível!
- Uma vez que todos os cenários levando ao estado proibido são impossíveis, a **Propriedade 2** também é verdadeira.

4.3.4.10. *Etapa 6 – Construção dos Seqüentes Globais*

Esta **etapa** não é realizada para as propriedades de segurança.

4.3.4.11. *Etapa 7 – Verificação das Hipóteses*

É realizada da mesma forma que para as propriedades de alcançabilidade.

4.4. Observações

Este capítulo tratou do problema de validação do Sistema Supervisório Híbrido. Esta validação é realizada através da verificação de propriedades no modelo em redes PTD-OO do Sistema Supervisório e seu Objeto de Controle.

Dois tipos de propriedades foram consideradas: *propriedades de alcançabilidade*, que visam provar que um determinado estado sempre é atingido em determinadas circunstâncias, e *propriedades de segurança*, que visam provar que um determinado estado nunca é atingido, independente do que ocorra no sistema.

Para fazer a verificação de propriedades, foi proposto um procedimento, que é dividido em 7 **etapas** principais:

- **Etapas 1 e 2:** consiste na definição das propriedades a serem verificadas para validação do Sistema Supervisório.
- **Etapas 3:** consiste na construção de um Diagrama de Colaboração Estático, que indica as possíveis seqüências de análise dos objetos.
- **Etapas 4:** se refere a análise do primeiro objeto.
- **Etapas 5:** se refere a análise dos demais objetos cujo comportamento eventualmente interfira na satisfação da propriedade a ser verificada.
- **Etapas 6:** consiste na construção de seqüentes globais para verificar a consistência das análises das **Etapas 4 e 5**.
- **Etapas 7:** consiste na verificação de hipóteses realizadas durante as **etapas** anteriores.

A principal característica deste procedimento, que o difere de outros presentes na literatura (discutidos na Seção 4.2), é a modularidade –analisa-se separadamente o comportamento de cada objeto (ou de poucos objetos).

Além de explorar a natural decomposição do modelo resultante dos conceitos de orientação a objetos, para auxiliar na decomposição do processo de análise o procedimento proposto introduz a participação do ser humano. Esta participação consiste na elaboração de hipóteses, que devem ser baseadas no conhecimento da pessoa sobre o sistema modelado. Cada hipótese é uma suposição *provável* de ser verdadeira, que simplifica a análise de um objeto, mas que não está explícita no modelo (está implícita, pois a verificação da hipótese é baseada no próprio modelo).

Uma vez que a elaboração de hipóteses depende da interpretação do modelo, o procedimento de análise não pode ser automatizado. Esta é claramente uma desvantagem do procedimento proposto em relação a utilização das ferramentas computacionais automáticas descritas na Seção 4.1. No entanto, observa-se que o objetivo deste procedimento não é ser mais rápido ou mais simples que a utilização de tais ferramentas, mas de ser uma alternativa no caso de problemas para os quais estas ferramentas não apresentam solução.

Apesar do processo de análise como um todo não ser passível de automação, algumas partes ainda o são, como a busca de cenários usando seqüentes da lógica linear. Uma futura evolução deste procedimento poderá então ser no sentido de aplicar o conceito de ‘automação balanceada’ (utilizado para Sistema de Controle (Camarinha-Matos; Rabelo; Osório, 1997)), isto é, de combinar de forma sinérgica a participação do computador (abordagem tecnocêntrica) e do homem (abordagem antropocêntrica).

Outra característica importante do procedimento proposto é a utilização da lógica linear, que enfoca a ordem parcial dos eventos na definição dos cenários, e assim, proporciona a redução do número de cenários a serem considerados. Além disso, que apesar de a abordagem apresentada consistir predominantemente em um procedimento do tipo *model checking*, técnicas de *theorem proving* também podem ser introduzidas na verificação de hipóteses, como por exemplo a utilização de invariantes de lugares, contribuindo para redução da complexidade do problema.

Salienta-se ainda que, uma vez que este é baseado nas redes PTD-OO, não são impostas restrições quanto a natureza do modelo, em particular em relação ao tipo de sistemas de equações diferenciais ou de funções de junção e habilitação dinâmica contínua. Como desvantagem, a análise da parte contínua não é estruturada.

Observa-se ainda que não existe garantia de solução. Além do problema da decidibilidade (apresentado na Seção 4.2), o sucesso do procedimento proposto depende da tomada de decisão do homem, se forem feitas más escolhas (ex.: hipóteses falsas ou que não simplificam o processo) o procedimento pode resultar em um número intratável de cenários, ou simplesmente não ser conclusivo (a propriedade não é verificada como verdadeira ou falsa).

Finalmente, quanto às propriedades a serem verificadas, foram introduzidos enunciados, referentes às propriedades de alcançabilidade e segurança. Observa-se que este conjunto de enunciados podem ser expandidos, assim como para o enunciado de restrições e hipóteses. Alguns exemplos são os eventos iniciais e/ou finais definidos tendo como base o estado de mais de um objeto, ou considerando seqüências de eventos, etc. Observa-se, no entanto, que nem todas as propriedades podem ser verificadas através da abordagem proposta. Um exemplo é a verificação

da vivacidade⁸ do modelo global, que, a não ser em casos muito particulares (discutidos em Sibertin-Blanc (1993)) implica na análise de todos os objetos simultaneamente.

⁸ Vivacidade: uma rede de Petri é ‘viva’ se todas as suas transições podem ser disparadas a partir de qualquer marcação que possa ser atingida a partir da marcação inicial (Cardoso; Valette, 1997).

5 ESTUDO DE CASO 1 – SISTEMA DE AR CONDICIONADO

O primeiro estudo de caso adotado refere-se ao sistema de ar condicionado de um conjunto de salas em um edifício. A escolha deste estudo de caso foi realizada em função da quantidade e qualidade de informações disponibilizadas pelo trabalho desenvolvido em (Villani, 2000), onde um Sistema Supervisório para sistema de ar condicionado do Edifício dos Ambulatórios do Hospital das Clínicas da Faculdade de Medicina da Universidade de São Paulo foi definido e modelado usando uma abordagem *orientada a processos* e as redes PTD.

Diferentemente do trabalho apresentado em Villani (2000) o estudo de caso aqui descrito se refere unicamente ao sistema de condicionamento de uma zona, isto é, uma sala (ou um conjunto de salas) cujo controle é realizado através das medições de um único sensor de temperatura. Os sistemas de produção de água gelada e de água quente não são considerados. O foco aqui são duas possíveis configurações para o sistema, chamadas de *Sistema de Ar Condicionado A* e *Sistema de Ar Condicionado B*, que permitem melhor ilustrar as vantagens e os limites da abordagem proposta para modelagem e análise de Sistemas Supervisórios Híbridos.

Em particular, o objetivo deste capítulo é ilustrar a aplicação dos procedimentos propostos no Capítulos 3 e 4 para modelagem e análise, usando como exemplo o Sistema de Ar Condicionado A. Além disso, este estudo de caso permite destacar os seguintes pontos:

- A utilização dos modelos em PFS da **Atividade 1** da modelagem para identificar possíveis ciclos fechados de compartilhamento de variáveis entre objetos, tendo como exemplo o Sistema de Ar Condicionado B.
- A utilização da relação de *decomposição/composição* (apresentada no Capítulo 3, Seção 3.2.1) para a obtenção de modelos em redes PTD-OO de classes no caso

de compartilhamento de variáveis em ciclo fechado. O Sistema de Ar Condicionado B é usado como exemplo.

- A utilização da relação de *generalização/especialização* (apresentada no Capítulo 3, Seção 3.2.2) para a reutilização de modelos em redes PTD-OO de classes entre sistemas diferentes mas com características ou componentes semelhantes (neste caso os Sistemas de Ar Condicionado A e B).

A seguir, a Seção 5.1. apresenta uma descrição de ambos os sistemas de ar condicionado e dos requisitos dos Sistemas Supervisórios. Em seguida, tendo como base os objetivos deste capítulo, a Seção 5.2. ilustra as **Atividades 1 a 7** para o Sistema de Ar Condicionado A e as **Atividades 1, 4 e 6** para o Sistema de Ar Condicionado B (as **Atividades 2, 3, 5 e 7** são semelhantes para ambos os sistemas e portanto não são apresentadas para o Sistema de Ar Condicionado B). A aplicação do procedimento de análise é ilustrada na Seção 5.3. através da verificação de algumas propriedades do Sistema de Ar Condicionado A.

5.1. Descrição do Sistema

5.1.1. Objeto de Controle

Neste estudo de caso considera-se duas diferentes configurações para o sistema de ar condicionado a ser supervisionado, chamadas de Sistema de Ar Condicionado A (Fig. 5.1) e Sistema de Ar Condicionado B (Fig. 5.2). Em ambos os casos, um ventilador (Ventilador A ou Ventilador B) impõe um fluxo de ar contínuo entre sistema de ar condicionado e o ambiente condicionado.

No Sistema de Ar Condicionado A, todo o ar que atravessa o sistema de ar condicionado é proveniente do exterior. Este ar é enviado a serpentina de resfriamento (Serpentina A), onde troca calor com o fluxo de água gelada, sendo então insuflado no ambiente.

No caso do Sistema de Ar Condicionado B, o ar que atravessa a serpentina de resfriamento (Serpentina B) é resultado da mistura de ar retirado do ambiente com ar proveniente do exterior. Esta mistura é realizada na Caixa de Mistura B. Após o condicionamento, a mistura de ar é insuflada no ambiente.

Ambos os sistemas de ar condicionado são do tipo VAC (Volume de Ar Constante), pois o ajuste da temperatura no ambiente é realizado através da variação do fluxo de água que atravessa a serpentina, variando assim a temperatura do ar insuflado, e não seu fluxo.

Uma segunda diferença entre os sistemas é o controlador da posição da válvula da serpentina. No caso do Sistema de Ar Condicionado A o controlador é do tipo On/Off, no caso do Sistema de Ar Condicionado B é do tipo PID (Proporcional Integral Derivativo). Em ambos os sistemas, a variação da temperatura no ambiente depende não somente da temperatura e volume do ar insuflado, mas também da carga térmica introduzida por pessoas e equipamentos.

Fig. 5.1. Sistema de Ar Condicionado A.

Fig. 5.2. Sistema de Ar Condicionado B.

5.1.2. Requisitos do Sistema Supervisório

Considera-se que o Sistema Supervisório deve ter as seguintes características:

- Atuar sobre os equipamentos de acordo o modo de operação selecionado pelo usuário. Os modos de operação disponíveis são desligado, ventilação, resfriamento.
- Permitir ao operador do ar condicionado selecionar a temperatura desejada no ambiente.
- Supervisionar o funcionamento da serpentina, identificando eventuais vazamentos e notificando o operador do ar condicionado.
- Em caso de incêndio (informado pelo sistema de gerenciamento do edifício) modificar a velocidade do ventilador e, no caso do sistema A, posicionar a caixa de mistura para 100% de renovação.

5.2. Modelagem do Sistema Supervisório e seu Objeto de Controle

5.2.1. Atividade 1 – Modelagem do Fluxo de Materiais

A Fig. 5.3 e a Fig. 5.4 apresentam os modelos em PFS desenvolvidos a partir do fluxo de materiais através do sistema. Em ambas as figuras, o fluxo de ar é representado por setas em preto e o fluxo de água por setas em cinza.

Fig. 5.3. PFS para o Sistema de Ar Condicionado A.

Fig. 5.4. PFS para o Sistema de Ar Condicionado B.

Uma importante diferença entre os casos A e B é que no Sistema de Ar Condicionado B as etapas de processamento do ar estão em ciclo fechado. Este ciclo sugere o compartilhamento de variáveis entre os objetos relacionados aos

equipamentos envolvidos no processamento. No Sistema de Ar Condicionado A não existe ciclo.

5.2.2. *Atividade 2 – Definição dos Casos de Uso*

Prosseguindo com o procedimento apresentado no Capítulo 3, a Fig. 5.5 apresenta o Diagrama de Casos de Uso desenvolvido para o Sistema de Ar Condicionado A.

Fig. 5.5. Diagrama de Casos de Uso para o Sistema de Ar Condicionado A.

5.2.3. *Atividade 3 – Construção dos Diagramas de Atividades*

Esta **atividade** consiste no detalhamento cada Caso de Uso em um Diagrama de *Atividades*.

Observa-se no entanto que o detalhamento é feito de forma semelhante para todos os Casos de Uso e que a apresentação exhaustiva de todos os Diagramas de *Atividades* sobrecarregaria este texto sem acrescentar novas contribuições ou ilustrar aspectos diferentes do procedimento de modelagem.

Assim, apresenta-se, como exemplo, apenas o Diagrama de *Atividades* relativo ao Caso de Uso ‘Iniciar procedimento alarme’ para o Sistema de Ar Condicionado A (Fig. 5.6).

Fig. 5.6. Diagrama de *Atividades* do Caso de Uso 'Iniciar procedimento alarme' - Sistema de Ar Condicionado A.

5.2.4. *Atividade 4 – Definição das Classes e Objetos*

A definição dos objetos é realizada usando as Regras de Decomposição apresentadas no Capítulo 3, Seção 3.1.4.

No caso do Sistema de Ar Condicionado A, para o Objeto de Controle, se considerarmos como candidatos a objetos os equipamentos do Sistema, todos eles compartilharam variáveis contínuas, uma vez que, segundo o PFS da Fig. 5.3 (**Atividade 1**), todos interagem com o fluxo de ar contínuo, cujas propriedades devem ser modeladas. Assim, qualquer decomposição só é possível através da aplicação da 3ª Regra de Decomposição (p. 58), que resulta nos seguintes candidatos a objetos: Ventilador A, Serpentina A, o Controlador On/Off A e o Ambiente A. Para o Sistema Supervisório, aplicando-se a 1ª. Regra de Decomposição (p. 57) tem-se como candidatos: Interface Usuário A, Interface Gerenciamento do Edifício A e Interface Ventilador A. A aplicação da 2ª Regra de Decomposição (p. 57) não resulta em nenhuma decomposição adicional. A aplicação da 3ª Regra resulta nos objetos Regulagem T_{sp} A e Interface Controlador A, o primeiro deles compartilha a temperatura desejada no ambiente (T_{sp}), e o segundo monitora continuamente a temperatura na saída da serpentina para detectar eventuais falhas.

No caso do Sistema de Ar Condicionado B, qualquer decomposição também só é possível através da aplicação da 3ª Regra de Decomposição. Neste caso, no

entanto, de acordo com o PFS da Fig. 5.4 (**Atividade 1**), o fluxo contínuo de ar percorre um ciclo, o que sugere o compartilhamento de variáveis em ciclo fechado entre os objetos correspondentes aos equipamentos que interagem com o fluxo de ar. De fato, a temperatura do ar nos diversos pontos do sistema, é definida pelo balanceamento de diversas interações: a temperatura no ambiente condicionado depende, entre outras coisas, da temperatura do ar na saída da serpentina, que por sua vez, varia de acordo com o ar fornecido pela caixa de mistura, cuja temperatura depende da temperatura no ambiente. Um segundo caso de compartilhamento de variáveis, é composto pela dependência entre a temperatura no ambiente, a temperatura na saída da serpentina e a posição da válvula definida pelo controlador PID em função da temperatura no ambiente. Estes compartilhamentos de variáveis impõem a definição de um único objeto, chamado de Ciclo de Ar B, do qual faz parte a serpentina, a caixa de mistura, o ambiente e o controlador PID. Apesar do ventilador também interagir com o fluxo de ar em ciclo fechado, a definição de um objeto Ventilador B está de acordo com a 3ª Regra de Decomposição porque este é o único equipamento que interfere na variável ‘vazão’ do fluxo de ar, vazão esta que não depende das demais propriedades do fluxo. Para o Sistema Supervisório, os objetos são definidos da mesma forma que para o Sistema de Ar Condicionado B: Regulagem T_{sp} B, Interface Usuário B, Interface Gerenciamento do Edifício B, Interface Caixa de Mistura B, Interface Ventilador B e Interface Caixa de Mistura B.

Estes objetos são organizados nas seguintes classes:

- C_1 – Ventilador: $O_{1,1} = \text{Ventilador A}$, $O_{2,1} = \text{Ventilador B}$;
- C_5 – Serpentina A: $O_{1,5} = \text{Serpentina A}$;
- C_7 – Controle On/Off: $O_{1,7} = \text{Controle On/Off A}$;
- C_9 – Ambiente: $O_{1,9} = \text{Ambiente A}$;
- C_{10} – Ciclo de Ar: $O_{1,10} = \text{Ciclo de Ar B}$;
- C_{11} – Regulagem T_{sp} : $O_{1,11} = \text{Regulagem } T_{sp} \text{ A}$, $O_{2,11} = \text{Regulagem } T_{sp} \text{ B}$;
- C_{12} – Interface Controlador: $O_{1,12} = \text{Interface Controlador A}$, $O_{2,12} = \text{Interface Controlador B}$;
- C_{14} – Interface Ventilador: $O_{1,14} = \text{Interface Ventilador A}$, $O_{2,14} = \text{Interface Ventilador B}$;
- C_{15} – Interface Caixa de Mistura: $O_{1,15} = \text{Interface Caixa de Mistura B}$;

- C_{16} – Interface Gerenciamento do Edifício A: $O_{1.16}$ = Interface Gerenciamento do Edifício A;
- C_{17} – Interface Gerenciamento do Edifício B: $O_{1.17}$ = Interface Gerenciamento do Edifício B;
- C_{19} – Interface Usuário A: $O_{1.19}$ = Interface Usuário A;
- C_{20} – Interface Usuário B: $O_{1.20}$ = Interface Usuário B;

As demais classes (C_2 , C_3 , C_4 , C_6 , C_8 , C_{13} e C_{18}) são resultados da aplicação das relações de decomposição/composição e generalização/especialização, e são apresentadas na Seção 5.2.6.

5.2.5. *Atividade 5 – Construção dos Diagramas de Seqüência ou Colaboração*

Semelhantemente a **Atividade 3**, para a **Atividade 5** apresenta-se apenas um exemplo de Diagrama de Seqüência (Fig. 5.7), correspondente ao mesmo Caso de Uso selecionado para ilustrar a **Atividade 3**: o Caso de Uso ‘Iniciar procedimento de alarme’. Este diagrama considera que o Sistema de Ar Condicionado A está desligado quando o procedimento é solicitado.

Fig. 5.7. Diagrama de Seqüência do Caso de Uso ‘Iniciar procedimento alarme’ - Sistema de Ar Condicionado A.

A construção dos Diagramas de *Atividades* e de Seqüência leva a identificação dos métodos e atributos necessários a cada classe (Fig. 5.8). Nesta figura, os métodos e as variáveis identificadas com base nos Diagramas de *Atividades* da Fig. 5.6 e de Seqüência da Fig. 5.7 são apresentados em negrito.

C_1 - Ventilador $K_{q_ar_1}, K_{q_ar_2}$ q_{ar} Ligar Desligar Colocar em velocidade alta Retornar p/ velocidade normal	C_5 - Serpentina B $q_w, T_w, \epsilon, K_1, K_2, K_3, K_4, K_5,$ K_w, K_t, I_1, I_2 $T_{ar_in}, P_v, T_{ar_out}$ $q_{ar.I1.C1}, T_{ext}$ Início do fluxo de água Fim do fluxo de água	C_{11} - Regulagem T_{sp} K T_{sp} Fim diminuir Início diminuir Início aumentar Fim aumentar
C_{14} - Interface Ventilador I_1 Ligar ventilação Desligar ventilação Iniciar ventilação alta Finalizar ventilação alta	C_9 - Ambiente $Q_{ac}, K_{ac}, N_p, K_p, K_{p_max}, N_{eq},$ $K_{eq}, K_{eq_max}, Vol_{amb}, K_{amb}, I_1, I_2$ T_{amb} $q_{ar.I1.C1}, T_{ar_out.I2.C3}$	C_{20} - Interface Usuário A I_1 Iniciar ventilação Finalizar ventilação Iniciar resfriamento Finalizar resfriamento
C_{12} - Interface Controlador $T_{ar_out_teor}, E, K_E, K_w, q_w, \Delta, \epsilon, K_1,$ $K_2, K_3, K_4, K_5, K_t, I_1, I_2, I_3$ $q_{ar.I1.C1}, P_{V.I2.C3}, T_{ar_in.I2.C3}, T_{ar_out.I2.C3}$ Ligar resfriamento Desligar resfriamento	C_7 - Controle On/Off K_A, I_1, I_2, I_3 $T_{amb.I1.C9}, T_{sp.I2.C11}$ Ligar controlador Desligar controlador	C_{17} - Interface Ger. Edifício A I_1 Iniciar procedimento alarme Finalizar procedimento alarme

Fig. 5.8.Métodos e atributos das classes do Sistema de Ar Condicionado A.

O Diagrama de *Atividades* da Fig. 5.6, é então detalhado (Fig. 5.9), considerando também as atividades referentes às comunicações entre os objetos.

Fig. 5.9. Detalhamento do Diagrama de *Atividades* da Fig. 5.6 - Sistema de Ar Condicionado A.

5.2.6. Atividade 6 – Modelagem das Classes em redes PTD-OO

Uma vez identificados os métodos e atributos dos objetos, o passo seguinte é a modelagem em redes PTD-OO. A fim de ilustrar a reutilização de modelos entre os Sistemas de Ar Condicionado A e B apresentam-se as classes de ambos os sistemas.

Assim, utiliza-se a relação de decomposição/composição para definir a classe C_{10} - *Ciclo de Ar B* como composição das classes C_2 - *Caixa de Mistura*, C_4 - *Serpentina B*, C_8 - *Controle PID* e C_9 - *Ambiente*, que ilustram separadamente o comportamento dos respectivos equipamentos no Sistema de Ar Condicionado B. Utiliza-se também a relação de generalização/especialização para definição de uma classe C_3 - *Serpentina Genérica*, que evidencia o comportamento em comum entre as classes C_4 - *Serpentina A* e C_5 - *Serpentina B*. Semelhantemente, C_{15} e C_{14} são definidas como especialização de C_{13} , C_8 e C_7 como especialização de C_6 , e C_{19} e C_{20} como especialização de C_{18} . A Fig. 5.10 apresenta o Diagrama de Classes para os Sistemas de Ar Condicionado A e B, ilustrando estas relações e as classes compartilhadas entre os dois sistemas.

Fig. 5.10. Diagrama de Classes dos Sistemas de Ar Condicionado A e B.

A seguir são apresentadas as redes de cada uma das classes da Fig. 5.10.

C_1 – Ventilador (Fig. 5.11)

Um objeto da classe C_1 - Ventilador pode estar desligado (p_{1_1}) ou operar em duas velocidades diferentes (p_{2_1} e p_{3_1}). A vazão de ar (q_{ar}) em cada uma destas velocidades é dada pelas constantes $K_{q_ar_1}$ e $K_{q_ar_2}$.

Fig. 5.11. Modelo em redes PTD-OO da classe C_1 – Ventilador.

C_2 – Caixa de Mistura (Fig. 5.12)

A caixa de mistura pode impor 0% de renovação do ar (p_{1_2}), renovação parcial (p_{2_2} - cuja porcentagem é dada por K_{mbox}) ou 100% (p_{3_2}). Em função do seu estado, a temperatura do ar enviado a serpentina (T_{mbox}) é determinada de acordo com a temperatura do ar exterior (T_{ext}) e com a temperatura do ar no ambiente (T_{amb}).

Fig. 5.12. Modelo em redes PTD-OO da classe C_2 – Caixa de Mistura.

C_3 – Serpentina Genérica (Fig. 5.13)

O modelo da troca de calor na serpentina é definido de acordo com Incropera; De Witt (1990) e com Salsbury (1996). A temperatura do ar na saída da serpentina (T_{ar_out}) é função da posição da válvula de água fria (P_v), de um conjunto de constantes ($K_1, \dots, K_5, K_w$), do atraso de tempo (K_t), da temperatura do ar na entrada da serpentina (T_{ar_in}), da temperatura da água (T_w) e do fluxo de água (q_w). O disparo de t_{3_3} simula a ocorrência de vazamento na serpentina, impondo uma redução de 20% no fluxo de água.

Fig. 5.13. Modelo em redes PTD-OO da classe C₃ – Serpentina Genérica.**C₄ – Serpentina B (Fig. 5.14)**

No Sistema de Ar Condicionado B, a temperatura na entrada da serpentina é a temperatura na saída da caixa de mistura ($T_{mbox.I4.C2}$), e a posição da válvula é continuamente determinada pelo controlador PID ($P_{I3.C8}$). Os elementos adicionais desta classe em relação a classe C₃ estão representados em **negrito**.

Fig. 5.14. Modelo em redes PTD-OO da classe C₄ – Serpentina B.**C₅ – Serpentina A (Fig. 5.15)**

No Sistema de Ar Condicionado A, a temperatura na entrada da serpentina é a temperatura externa (T_{ext}), e a posição da válvula varia entre 0 e 1, de acordo com o disparo de t_{1_5} e t_{2_5} , que são habilitadas pelo controlador On/Off.

Fig. 5.15. Modelo em redes PTD-OO da classe C₅ – Serpentina A.**C₆ – Controle Genérico (Fig. 5.16)**

Basicamente esta classe permite que o resfriamento seja ligado ou desligado (t_{1_6} e t_{4_6}).

Fig. 5.16. Modelo em redes PTD-OO da classe C₆ – Controle Genérico.**C₇ – Controle On/Off (Fig. 5.17)**

Nesta classe, a válvula da serpentina é aberta ou fechada (disparo de t_{5_7} e t_{6_7}) de acordo com o valor da temperatura no ambiente ($T_{amb.I1.C9}$) e da temperatura desejada ($T_{sp.I2.C11}$).

Fig. 5.17. Modelo em redes PTD-OO da classe C₇ – Controle On/Off.**C₈ – Controle PID (Fig. 5.18)**

Nesta classe, a posição da válvula da serpentina é determinada de acordo com a equação de um PID (F_{5_8}), se o valor determinado está além dos limites da válvula (P negativo ou maior que 1), tem-se os estados p_{4_8} e p_{7_8} .

Fig. 5.18. Modelo em redes PTD-OO da classe C₈ – Controle PID.

C_9 – Ambiente (Fig. 5.19)

A temperatura no ambiente (T_{amb}) é determinada em função do número de pessoas no ambiente (N_p), de equipamentos ligados (N_{eq}) e da carga térmica retirada pelo ar condicionado (Q_{ac}), que é função da vazão de ar ($q_{ar.I1.C1}$) e da temperatura do ar na saída da serpentina ($T_{ar.out.I2.C3}$).

Fig. 5.19. Modelo em redes PTD-OO da classe C_9 – Ambiente.

C_{10} – Ciclo de Ar (Fig. 5.20)

Esta classe é a simples união das classes C_2 , C_4 , C_8 e C_9 . Não existe fusão de transições, uma vez que não existe chamada de métodos entre as classes, apenas compartilhamento de variáveis contínuas. Este compartilhamento é ilustrado na Fig. 5.20, onde evidencia-se os ciclos fechados.

Fig. 5.20. Ciclo fechado de compartilhamento de variáveis entre as classes C_2 , C_4 , C_8 e C_9 .

As classes até aqui apresentadas modelam o Objeto de Controle para ambos os Sistemas de Ar Condicionado A e B. As próximas classes se referem aos Sistemas Supervisórios.

C_{11} – Regulagem T_{sp} (Fig. 5.21)

Esta classe permite ao operador do sistema de ar condicionado alterar a temperatura de set-point do controlado (T_{sp}), que corresponde à temperatura desejada no ambiente.

Fig. 5.21. Modelo em redes PTD-OO da classe C_{11} – Regulagem T_{sp} .

C_{12} – Interface Controlador (Fig. 5.22)

Esta classe faz a interface com o controlador da serpentina (classe C_6) e monitora seu funcionamento, estimando a temperatura de saída do ar ($T_{ar_out_teor}$) e comparando com a temperatura real ($T_{ar_out.I2.C3}$). No caso de discrepância entre os dois valores, o controlador é desligado, permanecendo bloqueado. O operador do sistema é avisado através do disparo de t_{6_12} .

Fig. 5.22. Modelo em redes PTD-OO da classe C_{12} – Interface Controlador.

C₁₃ – Interface Genérica – Equipamento (Fig. 5.23)

Esta classe representa o comportamento em comum entre as classes *C₁₄* e *C₁₅*, que diferem entre si apenas na definição de sua interface discreta.

Fig. 5.23. Modelo em redes PTD-OO da classe *C₁₃ – Interface Genérica Equipamento*.

C₁₄ – Interface Ventilador (Fig. 5.24)

Esta classe interage com a classe *C₁ – Ventilador*.

Fig. 5.24. Modelo em redes PTD-OO da classe *C₁₄ – Interface Ventilador*.

C₁₅ – Interface Caixa de Mistura (Fig. 5.25)

Esta classe interage com a classe *C₂ – Caixa de Mistura*.

Fig. 5.25. Modelo em redes PTD-OO da classe C_{15} – Interface Caixa de Mistura.

C_{16} – Interface Gerenciamento Edifício B (Fig. 5.26)

Esta classe permite ao sistema de gerenciamento do edifício interferir no funcionamento do Sistema de Ar Condicionado B, iniciando (t_{1_16}) e suspendendo (t_{8_16}) o procedimento de alarme em caso de incêndio. Este procedimento consiste em alterar o estado do ventilador e da caixa de mistura.

Fig. 5.26. Modelo em redes PTD-OO da classe C_{16} – Interface Gerenciamento do Edifício B.

C₁₇ – Interface Gerenciamento Edifício A

Esta classe tem a mesma função que a classe C₁₆ no Sistema de Ar Condicionado B, mas neste caso apenas o ventilador tem seu estado alterado, uma vez que o Sistema de Ar Condicionado A não possui caixa de mistura.

Fig. 5.27. Modelo em redes PTD-OO da classe C₁₇ – Interface Gerenciamento Edifício A.

C₁₈ – Interface Usuário Genérica (Fig. 5.28)

Esta classe permite aos usuários do sistema de ar condicionado selecionar entre os modos ‘Desligado’ ($p_{1,18}$), ‘Ventilação’ ($p_{2,18}$) e ‘Resfriando’ ($p_{3,18}$), atuando sobre o ventilador e o controlador da serpentina através de suas interfaces (classes C₁₄ e C₁₂).

Fig. 5.28. Modelo em redes PTD-OO da classe C₁₈ – Interface Usuário Genérica.

C₁₉ – Interface Usuário B (Fig. 5.29)

Esta classe corresponde a classe C₁₈ para o caso do Sistema de Ar Condicionado B, atuando também sobre a caixa de mistura, cuja interface é modelada pela classe C₁₅.

Fig. 5.29. Modelo em redes PTD-OO da classe *C₁₉ – Interface Usuário B*.*C₂₀ – Interface Usuário B (Fig. 5.30)*

Esta classe complementa a classe *C₁₈* para o caso do Sistema B.

Fig. 5.30. Modelo em redes PTD-OO da classe *C₂₀ – Interface Usuário B*.

Como exemplo de possível estado inicial para este estudo de caso, apresenta-se o seguinte estado para o Sistema de Ar Condicionado B:

- $O_{2.1} = \text{Ventilador B}; X_{2.1} = \{K_{q_ar_1} = 0,7 \text{ m}^3/\text{s}, K_{q_ar_2} = 1,4 \text{ m}^3/\text{s}; q_{ar} = 0\}; m_{2.1} = \{p_{1_1}\};$
- $O_{1.5} = \text{Serpentina B}; X_{1.5} = \{q_w = 0, T_{ar_in} = ind, P_V = 0, T_{ar_out} = ind, T_w = 7^\circ\text{C}, \varepsilon = 0, K_1 = 6464, K_2 = 0,8, K_3 = 10^7, K_4 = 0,8, K_5 = 4,15 \cdot 10^6, K_w = 6,8 \cdot 10^{-4} \text{ m}^3/\text{s}, K_t = 300 \text{ s}, l_1 = \text{Ventilador B}\}; m_{1.5} = \{p_{1_5}\};$

- $O_{1.7} = \text{Controle On/Off B}$; $X_{1.7} = \{K_{\Delta} = 2, I_1 = \text{Ambiente B}, I_2 = \text{Regulagem } T_{sp} \text{ B}, I_3 = \text{Serpentina B}\}$; $m_{1.7} = \{p_{1.7}\}$;
- $O_{1.9} = \text{Ambiente B}$; $X_{1.9} = \{Q_{ac} = ind, K_{ac} = 1,2987 \cdot 10^3, N_p = 0, K_p = 100 \text{ W}, K_{p_max} = 5, N_{eq} = 0, K_{eq} = 200 \text{ W}, K_{eq_max} = 5, Vol_{amb} = 500 \text{ m}^3, K_{amb} = 1,2987 \cdot 10^3, I_1 = \text{Ventilador B}, I_2 = \text{Serpentina B}, T_{amb} = ind\}$; $m_{1.7} = \{p_{1.9}\}$;
- $O_{2.11} = \text{Regulagem } T_{sp} \text{ B}$; $X_{2.11} = \{K = 1, T_{sp} = 23\}$; $m_{1.7} = \{p_{2.11}\}$;
- $O_{2.12} = \text{Interface Controlador B}$; $X_{2.12} = \{T_{ar_out_teor} = ind, E = ind, K_E = 3^{\circ}\text{C}, q_w = ind, \varepsilon = ind, K_1 = 6464, K_2 = 0,8, K_3 = 10^7, K_4 = 0,8, K_5 = 4,15 \cdot 10^6, K_w = ind, K_{\tau} = 300 \text{ s}, I_1 = \text{Ventilador B}, I_2 = \text{Serpentina B}, I_3 = \text{Controlador On/Off B}\}$; $m_{2.12} = \{p_{1.12}\}$;
- $O_{2.14} = \text{Interface Ventilador B}$; $X_{2.14} = \{I_1 = \text{Ventilador B}\}$; $m_{2.14} = \{p_{1.14}, p_{11.14}\}$;
- $O_{1.17} = \text{Interface Gerenciamento do Edifício B}$; $X_{1.17} = \{I_1 = \text{Interface Ventilador B}\}$; $m_{1.17} = \{p_{1.17}\}$;
- $O_{1.20} = \text{Interface Usuário B}$; $X_{1.20} = \{\theta_{aux} = 0, \varepsilon = 1, I_1 = \text{Interface Ventilador B}, I_2 = \text{Interface Controlador B}\}$; $m_{1.20} = \{p_{1.20}\}$;

5.2.7. Atividade 7 – Verificação dos Modelos

Modelo em redes PTD-OO e Diagramas de Sequência e/ou Colaboração

Continuando a aplicação do procedimento de modelagem para o Sistema de Ar Condicionado A, a Fig. 5.31 apresenta a relação entre as interação do Diagrama de Sequência do Caso de Uso ‘Iniciar procedimento de alarme’ (Fig. 5.7) e as transições dos modelos em redes PTD das classes.

Fig. 5.31. Relação entre o Diagrama de Sequência da Fig. 5.7 e as transições das classes - Sistema de Ar Condicionado A.

Modelo em redes PTD-OO e Diagramas de Atividades

O Diagrama de Atividade apresentado na Fig. 5.9 é então convertido para um modelo em redes de Petri (Fig. 5.32), cujos elementos estão relacionados com os elementos do modelo em redes PTD-OO das classes que compõem o Sistema de Ar Condicionado A.

Fig. 5.32. Conversão para redes de Petri do Diagrama de Atividades da Fig. 5.9.

5.3. Análise dos Modelos em redes PTD-OO

De acordo com o apresentado anteriormente, no caso do Sistema de Ar Condicionado B, a relação de composição foi utilizada para gerar o objeto Ciclo de Ar, pois existe compartilhamento contínuo de variáveis entre os diversos componentes do sistema, inviabilizando uma posterior decomposição. Sendo assim, neste item considerou-se apenas o Sistema de Ar Condicionado A. O modelo deste sistema apresenta um maior grau de decomposição, o que viabiliza a verificação por partes de propriedades e, portanto, ilustra de forma mais representativa o procedimento de análise proposto no Capítulo 4.

São apresentadas as verificações de duas propriedades relacionadas ao Caso de Uso ‘Selecionar resfriamento’:

- **Propriedade 1** - Ilustra a verificação de uma propriedade de alcançabilidade que depende quase que exclusivamente da dinâmica discreta do sistema. Neste caso a parte contínua se restringe ao cálculo de intervalos de tempos para determinação e das datas de disparo das transições.
- **Propriedade 2** - Apresenta um exemplo de propriedade de alcançabilidade onde a dinâmica contínua do Sistema de Ar Condicionado A tem papel relevante. Além disso, este exemplo ilustra a reutilização no procedimento de análise através do aproveitamento de resultados da verificação da **Propriedade 1**.

5.3.1. Propriedade 1

5.3.1.1. Etapa 1 - Definição do enunciado da propriedade

O enunciado da **Propriedade 1** é definido de acordo com o tipo de enunciado PA2 (apresentado no Capítulo 4, Seção 4.3.3.1):

- **Propriedade 1** - Quando o usuário seleciona o modo ‘resfriamento’ (evento e_0), o controlador da serpentina deve ser imediatamente ligado (evento e_i) e assim permanecer até que outro modo de operação seja selecionado (evento e_f): e_0 = disparo de $t_{5_20.O1}$; e_i = alcance de $m_{1.7} = \{p_{2_7.O1}\}$; e_f = disparo de $t_{8_20.O1}$; $\Delta\theta = 0$.

5.3.1.2. Etapa 2 - Definição do conjunto de restrições da propriedade

A única restrição considerada para a **Propriedade 1** utiliza o tipo de restrição R2 (apresentado no Capítulo 4, Seção 4.3.3.2):

- Restrição 1A - Não ocorre e não ocorreu anteriormente falha na serpentina:
 $t_{5_12.O2/4_7.O1}$ e $t_{3_5.O1}$ não disparam em $0 \leq \theta \leq \theta_{8_20.O1}$.

5.3.1.3. Etapa 3 – Construção dos Diagramas de Colaboração Estáticos

O Diagrama de Colaboração Estático do Sistema de Ar Condicionado A é apresentado na Fig. 5.33, onde evidenciam-se as interações entre objetos que interferem na verificação da **Propriedade 1**.

Fig. 5.33. Interações relevantes para **Propriedade 1**.

De acordo com a Fig. 5.33, a relação entre os objetos Interface Usuário A (onde ocorre e_0 e e_f) e Controlador On/Off A (onde ocorre e_i) é estabelecida através do objeto Interface Controlador On/Off A. Sendo assim, a verificação desta propriedade deve, no mínimo, envolver estes 3 objetos. Inicia-se assim a análise pelo objeto Interface Usuário A.

5.3.1.4. **Etapa 4.1** – Parte Discreta – Busca de Cenários ($O_{1.20}$ - Interface Usuário A)

O evento inicial que caracteriza o início dos cenários é o disparo de $t_{5_20.O1}$. O final dos cenários é determinado pelo disparo de $t_{8_20.O1}$. A análise da parte discreta constitui portanto, na busca de um único seqüente, onde $p_{5_20.O1}$ = pós-condição de $t_{5_20.O1}$ e $p_{6_20.O1}$ = pós-condição de $t_{8_20.O1}$:

- **Busca 1** (do disparo de $t_{5_20.O1}$ ao disparo de $t_{8_20.O1}$): $\Gamma_0, p_{5_20.O1}, !t_{1_20.O1}, !t_{2_20.O1}, !t_{3_20.O1}, !t_{4_20.O1}, !t_{5_20.O1}, !t_{6_20.O1}, !t_{7_20.O1}, t_{8_20.O1} \vdash p_{6_20.O1} \otimes \Gamma_f$:

$$\frac{\frac{p_{7_20.O1} \vdash p_{7_20.O1} \quad \Gamma_0, p_{6_20.O1}, !t_{1_20.O1}, \dots, !t_{7_20.O1} \vdash p_{6_20.O1} \otimes \Gamma_f}{p_{5_20.O1} \vdash p_{5_20.O1} \quad \Gamma_0, p_{7_20.O1}, !t_{1_20.O1}, \dots, !t_{7_20.O1}, t_{8_20.O1} \vdash p_{6_20.O1} \otimes \Gamma_f} \text{---o L } (t_{8_20.O1})}{\Gamma_0, p_{5_20.O1}, !t_{1_20.O1}, !t_{2_20.O1}, !t_{3_20.O1}, !t_{4_20.O1}, !t_{5_20.O1}, !t_{6_20.O1}, !t_{7_20.O1}, t_{8_20.O1} \vdash p_{6_20.O1} \otimes \Gamma_f} \text{---o L } (t_{7_20.O1})$$
- **Definição dos Cenários** – A construção da árvore resulta em uma única seqüência de disparos possível, onde $\Gamma_0 = \Gamma_f = \emptyset$:
 - **Cenário 1**: $t_{7_20.O1/1_12.O1}; t_{8_20.O1}$.

5.3.1.5. **Etapa 4.2** – Elaboração de Hipóteses ($O_{1.20}$ - Interface Usuário A)

É feita a seguinte hipótese, que corresponde ao tipo de hipótese H1 (apresentado no Capítulo 4, Seção 4.3.3.6):

- **Hipótese 1A** – As chamadas de métodos solicitadas pelo objeto são imediatamente executados: $t_{7_20.O1/1_12.O2}$ dispara em $\Delta\theta = 0$ após sua habilitação em $O_{1.20}$.

5.3.1.6. **Etapa 4.3** – Parte Contínua – Evolução de variáveis contínuas e datas de disparos ($O_{1.20}$ - Interface Usuário A)

Para o **Cenário 1** tem-se que:

- $\theta_{7_20.O1/1_12.O2} = \theta_{5_20.O1}$ (de acordo com a Hipótese 1A).

- $\theta_{8_20} \geq \theta_{5_20.O1} + \varepsilon$ (de acordo com j_{7_20} , F_{7_20} e e_{8_20}).

5.3.1.7. ***Etap**a 5.1 – Parte Discreta – Busca de Cenários ($O_{2.12}$ - Interface Controlador A)*

Existe apenas um disparo de transição da interface entre $O_{2.12}$ e $O_{1.20}$, portanto, a análise deste objeto consiste em duas buscas, onde não foram incluídas as transições $t_{5_12.O2}$ (Restrição 1A), $t_{7_20.O1/1_12.O2}$ e $t_{6_20.O1/4_12.O2}$ (interface entre $O_{1.20}$ e $O_{2.12}$) e onde $p_{2_12.O2}$ = pós-condição de $t_{7_20.O1/1_12.O2}$:

- *Busca 1* (até o disparo de $t_{7_20.O1/1_12.O2}$): Uma vez que a data de disparo de $t_{7_20.O1/1_12.O2}$ é imposta pela Hipótese 1A, esta busca é omitida.
- *Busca 2* (do disparo de $t_{7_20.O1/1_12.O2}$): $\Gamma_0, p_{2_12.O2}, !t_{2_12.O2}, !t_{3_12.O2}, !t_{6_12.O2} \vdash \Gamma_f$:

$$\frac{p_{2_12.O2} \vdash p_{2_12.O2} \quad p_{4_12.O2}, !t_{2_12.O2}, !t_{3_12.O2}, !t_{6_12.O2} \vdash \Gamma_f}{\Gamma_0, p_{2_12.O2}, !t_{2_12.O2}, !t_{3_12.O2}, !t_{6_12.O2} \vdash \Gamma_f} \rightarrow O L (t_{3_12.O2})$$

- *Definição de Cenários* – A construção da árvore resulta em um único disparo possível, $t_{3_12.O2/1_7.O1}$. Uma vez que este evento não é pre-condição para o evento e_f , dois cenários devem ser considerados, incluindo ou não a ocorrência deste disparo. No primeiro caso, $\Gamma_0 = \emptyset$ e $\Gamma_f = p_{2_12.O2}$, e no segundo caso $\Gamma_0 = \emptyset$ e $\Gamma_f = p_{4_12.O2}$:

- **Cenário 1 - 1:** $t_{7_20.O1/1_12.O1}; t_{3_12.O2/1_7.O1}$.
- **Cenário 1 - 2:** $t_{7_20.O1/1_12.O1}$.

5.3.1.8. ***Etap**a 5.2 – Elaboração de Hipóteses ($O_{2.12}$ - Interface Controlador A)*

É feita a seguinte hipótese, também correspondente ao tipo de hipótese H1:

- Hipótese 1B – As chamadas de métodos solicitadas pelo objeto são imediatamente executados: $t_{3_12.O2/1_7.O1}$ dispara em $\Delta\theta = 0$ após sua habilitação em $O_{2.12}$.

5.3.1.9. ***Etap**a 5.3 – Parte Contínua – Evolução de variáveis contínuas e datas de disparos ($O_{2.12}$ - Interface Controlador A)*

De acordo com a Hipótese 1B, o **Cenário 1-2** é impossível. Para o **Cenário 1-1** tem-se que:

- $\theta_{3_12.O2/1_7.O1} = \theta_{7_20.O1/1_12.O2} = \theta_{5_20.O1}$.

5.3.1.10. *Etapa 5.1 – Parte Discreta – Busca de Cenários ($O_{1,7}$ - Controle On/Off A)*

Semelhantemente à análise de $O_{1,12}$, esta análise é dividida em duas partes:

- *Busca 1* (até o disparo de $t_{3_12.02/1_7.01}$): Uma vez que a data de disparo de $t_{3_12.02/1_7.01}$ é imposta pela Hipótese 1B, esta busca também é omitida.
- *Busca 2* (do disparo de $t_{3_12.02/1_7.01}$): $\Gamma_0, p_{2_7.01} \otimes p_{4_7.01}, !t_{2_7.01}, !t_{3_7.01}, !t_{5_7.01}, !t_{6_7.01} \vdash \Gamma_f$:

$$\begin{array}{c}
 \frac{p_{5_7.01} \vdash p_{5_7.01} \quad p_{2_7.01}, p_{4_7.01}, !t_{2_7.01}, !t_{3_7.01}, !t_{5_7.01}, !t_{6_7.01} \vdash \Gamma_f}{p_{4_7.01} \vdash p_{4_7.01} \quad \Gamma_0, p_{2_7.01}, p_{5_7.01}, !t_{2_7.01}, !t_{3_7.01}, !t_{5_7.01}, !t_{6_7.01} \vdash \Gamma_f} \text{---} \text{O L } (t_{6_7.01}) \\
 \frac{\Gamma_0, p_{2_7.01}, p_{4_7.01}, !t_{2_7.01}, !t_{3_7.01}, !t_{5_7.01}, !t_{6_7.01} \vdash \Gamma_f}{\Gamma_0, p_{2_7.01} \otimes p_{4_7.01}, !t_{2_7.01}, !t_{3_7.01}, !t_{5_7.01}, !t_{6_7.01} \vdash \Gamma_f} \text{---} \text{O L } (t_{5_7.01}) \\
 \frac{\Gamma_0, p_{2_7.01}, p_{4_7.01}, !t_{2_7.01}, !t_{3_7.01}, !t_{5_7.01}, !t_{6_7.01} \vdash \Gamma_f}{\Gamma_0, p_{2_7.01} \otimes p_{4_7.01}, !t_{2_7.01}, !t_{3_7.01}, !t_{5_7.01}, !t_{6_7.01} \vdash \Gamma_f} \otimes L
 \end{array}$$

- *Definição dos cenários* – A construção da árvore resulta em infinitos cenários, que variam entre si pelo número de disparos de $t_{5_7.01/1_5.01}$ e $t_{6_7.01/2_5.01}$. Caso a última transição a ser disparada seja $t_{3_12.02/1_7.01}$ ou $t_{6_7.01/2_5.01}$, $\Gamma_f = p_{2_7.01} \otimes p_{4_7.01}$; caso seja $t_{5_7.01/1_5.01}$, $\Gamma_f = p_{2_7.01} \otimes p_{5_7.01}$: . São definidos então os seguintes cenários, onde $1 \leq j \leq \infty$:
 - **Cenário 1-1-1:** $t_{3_12.02/1_7.01}$.
 - **Cenário 1-1-2:** $t_{3_12.02/1_7.01}; t_{5_7.01/1_5.01}$.
 - **Cenário 1-1-3:** $t_{3_12.02/1_7.01}; t_{5_7.01/1_5.01}; t_{6_7.01/2_5.01}$.
 - ...
 - **Cenário 1-1-2*j:** $t_{3_12.02/1_7.01}; (j-1) \cdot (t_{5_7.01/1_5.01}; t_{6_7.01/2_5.01}); t_{5_7.01/1_5.01}$.
 - **Cenário 1-1-(2*j+1):** $t_{3_12.02/1_7.01}; j \cdot (t_{5_7.01/1_5.01}; t_{6_7.01/2_5.01});$.

5.3.1.11. *Etapa 5.2 – Elaboração de Hipóteses ($O_{1,7}$ - Controle On/Off A)*

Nenhuma hipótese é feita sobre o estado ou os eventos no objeto Serpentina B.

5.3.1.12. *Etapa 5.3 – Parte Contínua – Evolução de variáveis contínuas e datas de disparos ($O_{1,7}$ - Controle On/Off A)*

Para todos os cenários possíveis, independente da evolução das variáveis contínuas, e da data de disparo das transições, a condição $p_{2_7.01}=1$ é em mantida de $\theta_{3_12.02/1_7.01} \equiv \theta_{5_20.01}$ até $\theta_{8_20.01}$, portanto:

$\Rightarrow$ A **Propriedade 1** é verdadeira se as Hipóteses 1A e 1B são verdadeiras.

5.3.1.13. *Etapa 6 – Construção dos Seqüentes Globais*

Os seqüentes que definem as possíveis evoluções do sistema a partir do disparo de $t_{5_20.01}$ são os seguintes:

- **Cenário 1-1-1:** $p_{4_20.01}, p_{1_12.01}, p_{1_7.01}, t_{5_20.01}, t_{7_20.01/1_12.02}, t_{8_20.01}, t_{3_12.01/1_7.01} \vdash p_{6_20.01} \otimes p_{4_12.01} \otimes p_{2_7.01} \otimes p_{4_7.01}$.
- **Cenário 1-1-2:** $p_{4_20.01}, p_{1_12.01}, p_{1_7.01}, p_{1_5.01}, t_{5_20.01}, t_{7_20.01/1_12.02}, t_{8_20.01}, t_{3_12.01/1_7.01}, t_{5_7.01/1_5.01} \vdash p_{6_20.01} \otimes p_{4_12.01} \otimes p_{2_7.01} \otimes p_{5_7.01} \otimes p_{2_5.01}$.
- **Cenário 1-1-3:** $p_{4_20.01}, p_{1_12.01}, p_{1_7.01}, p_{1_5.01}, t_{5_20.01}, t_{7_20.01/1_12.02}, t_{8_20.01}, t_{3_12.01/1_7.01}, t_{5_7.01/1_5.01}, t_{6_7.01/2_5.01} \vdash p_{6_20.01} \otimes p_{4_12.01} \otimes p_{2_7.01} \otimes p_{4_7.01} \otimes p_{1_5.01}$.

Os seqüentes para os demais cenários são semelhantes, apenas alterando o número de disparo de $t_{5_7.01/1_5.01}$ e $t_{6_7.01/2_5.01}$. Observa-se que, no caso de disparos de $t_{5_7.01/1_5.01}$ e $t_{6_7.01/2_5.01}$ fazerem parte do cenário, é necessário adicionar a marcação inicial e final do objeto Serpentina A.

Como exemplo, a Fig. 5.34 ilustra a ordem parcial de disparos das transições, obtida através da construção da árvore de prova do seqüente, considerando o caso do **Cenário 1-1-3**.

Fig. 5.34. Ordem parcial de disparos – **Propriedade 1**.

Para finalizar a verificação da **Propriedade 1** é necessário provar a veracidade das Hipóteses 1A e 1B.

5.3.1.14. *Etapa 7 – Verificação das Hipóteses*

A verificação da Hipótese 1A pode ser realizada através da composição dos objetos $O_{1.20}$ e $O_{2.12}$ em um único objeto. Considerando a marcação inicial deste objeto e a Restrição 1A, a Hipótese 1A pode ser comprovada através de invariantes de lugares ou da construção da árvore de alcançabilidade do objeto. Semelhantemente, a Hipótese 1B pode ser realizada através da composição dos objetos $O_{2.12}$ e $O_{1.7}$ em um único objeto.

A verificação da Hipótese 1A é feita de forma semelhante a verificação da Hipótese 1B, através da fusão dos objetos $O_{1.20}$ e $O_{2.12}$.

5.3.2. Propriedade 2

5.3.2.1. *Etapas 1 e 2 - Definição do enunciado da propriedade e Definição do conjunto de restrições da propriedade*

Esta propriedade é definida pelos seguintes enunciado e restrições:

- **Propriedade 2** (correspondente a PA1) - Quando o usuário seleciona o modo ‘resfriamento’ (evento e_0), a temperatura na sala deve atingir a temperatura de set-point (evento e_f) em um intervalo de tempo máximo de K_θ : $e_0 =$ disparo de $t_{5_20.O1}$; $e_f =$ alcance de $T_{amb}=T_{sp}$; $\Delta\theta \leq 30$ min.
 - Restrição 2A (correspondente a R2) - Não ocorre e não ocorreu anteriormente falha na serpentina: $t_{5_12.O2/4_7.O1}$ e $t_{3_5.O1}$ não disparam em $0 \leq \theta \leq (\theta_{5_20.O1} + 30$ min).
 - Restrição 2B (correspondente a R2) - O usuário não modifica o modo de operação do sistema de ar condicionado neste intervalo: $t_{1_20.O1}$, $t_{4_20.O1}$ e $t_{8_20.O1}$ não disparam em $\theta_{5_20.O1} \leq \theta \leq (\theta_{5_20.O1} + 30$ min).
 - Restrição 2C (correspondente a R9) - O usuário não modifica a temperatura de set-point neste intervalo: $\dot{T}_{sp} = 0$ em $\theta_{5_20.O1} \leq \theta \leq (\theta_{5_20.O1} + 30$ min).
 - Restrição 2D (correspondente a R8) – Quando o modo resfriamento é selecionado, a temperatura de set-point está entre 18 e 25°C: $T_{sp}(\theta) \in [18, 25]$, em $\theta = \theta_{5_20.O1}$.
 - Restrição 2E (correspondente a R8) – Quando o modo resfriamento é selecionado, a temperatura ambiente está entre 26 e 35°C: $T_{amb}(\theta) \in [26, 35]$, em $\theta = \theta_{5_20.O1}$.
 - Restrição 2F (correspondente a R9) - A temperatura externa é considerada constante neste intervalo: $\dot{T}_{amb} = 0$ em $\theta_{5_20.O1} \leq \theta \leq (\theta_{5_20.O1} + 30$ min).
 - Restrição 2G (correspondente a R8) – A temperatura externa está entre 26 e 35°C neste intervalo: $T_{ext}(\theta) \in [26, 35]$, em $\theta_{5_20.O1} \leq \theta \leq (\theta_{5_20.O1} + 30$ min).

5.3.2.2. *Etapa 3 – Construção dos Diagramas de Colaboração Estáticos*

O Diagrama de Colaboração Estático do Sistema de Ar Condicionado A é apresentado na Fig. 5.35, onde evidenciam-se as interações entre objetos que interferem na verificação da **Propriedade 2**.

Fig. 5.35. Interações relevantes para Propriedade 1.

De acordo com a Fig. 5.35, o estado do objeto Ambiente A (onde ocorre e_f) está relacionado ao estado do objeto Interface Usuário A (onde ocorre e_0) através dos objetos Interface Ventilador A, Interface Controlador On/Off A, Ventilador A, Controlador On/Off A e Serpentina A. Estes são portanto os prováveis objetos a serem considerados nesta análise.

5.3.2.3. *Etapa 4.1 – Parte Discreta – Busca de Cenários ($O_{1.20}$ - Interface Usuário A)*

O evento e_0 que caracteriza o início dos cenários relacionados a esta propriedade é o disparo de $t_{5_20.O1}$:

- *Busca 1* (do disparo de $t_{5_20.O1}$): $\Gamma_0, p_{5_20.O1}, !t_{2_20.O1}, !t_{3_20.O1}, !t_{5_20.O1}, !t_{6_20.O1}, !t_{7_20.O1} \vdash \Gamma_f$ – Os disparos de $t_{1_20.O1}, t_{4_20.O1}$ e $t_{8_20.O1}$ não são consideradas devido à Restrição 2B:

$$\frac{p_{5_20.O1} \vdash p_{5_20.O1} \quad \Gamma_0, p_{7_20.O1}, !t_{2_20.O1}, !t_{3_20.O1}, !t_{6_20.O1}, !t_{7_20.O1} \vdash \Gamma_f}{\Gamma_0, p_{5_20.O1}, !t_{2_20.O1}, !t_{3_20.O1}, !t_{6_20.O1}, !t_{7_20.O1} \vdash \Gamma_f} \text{—O L } (t_{7_20.O1})$$

- *Definição de Cenários* – Dois cenários são possíveis: incluindo ou não o disparo de $t_{7_20.01/1_12.02}$. No primeiro caso $\Gamma_0 = \emptyset$ e $\Gamma_f = p_{7_20.01}$, e no segundo caso $\Gamma_0 = \emptyset$ e $\Gamma_f = p_{5_20.01}$:
 - **Cenário 1:** $t_{7_20.01/1_12.02}$.
 - **Cenário 2:** não ocorre nenhum disparo.

5.3.2.4. ***Etapla 4.2** – Elaboração de Hipóteses ($O_{1.20}$ - Interface Usuário A)*

A Hipótese 2A considerada é semelhante a Hipótese 1A da Propriedade 1 (Seção 5.3.1.5).

5.3.2.5. ***Etapla 4.3** – Parte Contínua – Evolução de variáveis contínuas e datas de disparos ($O_{1.20}$ - Interface Usuário A)*

De acordo com a Hipótese 2A, o **Cenário 2** é impossível. Para o **Cenário 1** tem-se que:

- $\theta_{3_12.02/1_7.01} = \theta_{7_20.01/1_12.02}$ (de acordo com a Hipótese 2A).

5.3.2.6. ***Etapla 5** – Análise do objeto $O_{2.12}$ - Interface Controlador A*

A análise deste objeto para **Propriedade 2** é semelhante à realizada para **Propriedade 1**.

5.3.2.7. ***Etapla 5.1** – Parte Discreta – Busca de Cenários ($O_{1.7}$ - Controle On/Off A)*

A análise da parte discreta é deste objeto é semelhantemente à realizada para a **Propriedade 1**.

5.3.2.8. ***Etapla 5.2** – Elaboração de Hipóteses ($O_{1.7}$ - Controle On/Off A)*

É feita a seguinte hipótese:

- Hipótese 2C (correspondente a H1) – As chamadas de métodos solicitadas pelo objeto são imediatamente executados: $t_{5_7.01/1_5.01}$ e $t_{6_7.01/2_5.01}$ disparam em $\Delta\theta = 0$ após sua habilitação em $O_{1.7}$.

5.3.2.9. **Etapa 5.3 – Parte Contínua – Evolução de variáveis contínuas e datas de disparos** ($O_{1.7}$ - Controle On/Off A)

A parte contínua do modelo desta classe se restringe a duas funções de habilitação – $e_{5.7}$: $T_{amb.I1.C9} < (T_{sp.I2.C11} - K_A)$; $e_{6.7}$: $T_{amb.I1.C9} > (T_{sp.I2.C11} + K_A)$. Tem-se então que:

- **Cenário 1-1-1** ($t_{3_12.02/1_7.01}$): De acordo com as Restrições 2D e 2F, $e_{5.7}(\theta_{5_20.01})$ e $e_{5.7}(\theta_{3_12.02/1_7.01})$ são verdadeiras, e, de acordo com a Hipótese 2C, $t_{5_7.01/1_5.01}$ dispara. O **Cenário 1-1-1** é portanto impossível - (pelo menos um dos Cenários 1-1-i ($i>1$) deve ser verdadeiro).
- **Cenário 1-1-2** ($t_{3_12.02/1_7.01}$; $t_{5_7.01/1_5.01}$):
 - $\theta_{5_7.01/1_5.01} = \theta_{3_12.02/1_7.01}$;
- **Cenários 1-1-i** ($i>2$): a condição que determina o fim dos cenários referentes à esta propriedade é $T_{amb} = T_{sp}$, o que significa que $e_{6.7}$ é falsa no intervalo de tempo considerado. Portanto os **Cenários 1-1-i** são impossíveis.

5.3.2.10. **Etapa 5.1 – Parte Discreta – Busca de Cenários** ($O_{1.5}$ - Serpentina A)

É realizada a seguinte busca:

- **Busca 1** (do disparo de $t_{5_7.01/1_5.01}$): $\Gamma_0, p_{2_5.01} \vdash \Gamma_f$ - nenhuma transição pode ser disparada.
- **Definição de Cenários** – para o único cenário possível $\Gamma_0 = \emptyset$ e $\Gamma_f = p_{2_5.01}$:
 - **Cenário 1-1-2**: $t_{5_7.01/1_5.01}$.

5.3.2.11. **Etapa 5.2 – Elaboração de Hipóteses** ($O_{1.5}$ - Serpentina A)

Do ponto de vista contínuo, a evolução das variáveis contínuas de $O_{1.7}$ depende da variável externa q_{ar} de $O_{2.1}$ – Ventilador B. É feita então uma hipótese sobre q_{ar} :

- Hipótese 2D (correspondente a H7): $q_{ar} \in [0,5; 1,5]$ para $\theta_{5_20.01} \leq \theta \leq \theta(T_{amb}=T_{sp})$.

5.3.2.12. **Etapa 5.3 – Parte Contínua – Evolução de variáveis contínuas e datas de disparos** ($O_{1.5}$ - Serpentina A)

Para o Cenário 1-1-2 tem-se que:

- $P_V = 1$ (resultado de por $j_{1.5}$).
- $T_{air_in} = T_{ext} \in [26, 35]$ (imposto pela Restrição 2F).

- $q_w, T_w, K_1, K_2, K_3, K_4, K_5, K_w, K_\tau$ são constantes.
- Considerando a Hipótese 2D, o sistema de equações é resolvido algebricamente, resultando em:
 - $\varepsilon(\theta) \in [0,6893; 0,9119]$ p/ $\theta_{5_20.01} \leq \theta \leq \theta(T_{amb}=T_{sp})$.
 - T_{ar_out} pode variar dentro da faixa de valores apresentada pela Fig. 5.36.

Fig. 5.36. Faixa de variação de T_{ar_out} .

5.3.2.13. *Etapa 5.1 – Parte Discreta – Busca de Cenários ($O_{1.10}$ – Ambiente A)*

Nenhuma informação é fornecida sobre a marcação da rede de Petri de $O_{2.9}$ no intervalo da prova. No entanto, a única marcação possível para este objeto é $p_{1_9.01}=1$. Partindo da marcação inicial, as possíveis evoluções para o sistema são:

- *Busca 1* – Evolução a partir de $\theta_{5_20.01}$: $p_{1_9.01}, !t_{1_9.01}, !t_{1_9.01}, !t_{3_9.01}, !t_{4_9.01} \vdash \Gamma_f$.

- *Definição de cenários* - todas as transições podem ser disparadas retornando a marcação inicial. Existem portanto infinitos cenários combinando de 0 a ∞ disparos destas transições. Alguns exemplos são apresentados a seguir ($\Gamma_f = p_{1_9.01}$):

- **Cenário 1-1-2-1:** nenhum disparo.
- **Cenário 1-1-2-2:** $t_{3_9.01}$.
- **Cenário 1-1-2-3:** $t_{1_9.01}$; $t_{2_9.01}$.

5.3.2.14. *Etapa 5.2 – Elaboração de Hipóteses ($O_{1.10}$ – Ambiente A)*

Nenhuma hipótese é elaborada.

5.3.2.15. *Etapa 5.3 – Parte Contínua – Evolução de variáveis contínuas e datas de disparos ($O_{1.10}$ – Ambiente A)*

De acordo com e_{1_9} , e_{2_9} , e_{3_9} , e_{4_9} , j_{1_9} , j_{2_9} , j_{3_9} e j_{4_9} , tem-se $N_{eq} \in [0, 20]$ e $N_p \in [0, 20]$. As variáveis Q_{ac} , K_{ac} , N_p , K_p , K_{p_max} , N_{eq} , K_{eq} , K_{eq_max} , Vol_{amb} , K_{amb} são constantes e definidas na Seção 0. Como resultado, resolvendo o sistema de equações F_{1_9} obtém-se a faixa de variação para T_{amb} apresentada na Fig. 5.37. Observa-se que em qualquer caso T_{amb} atinge T_{sp} em $\theta \leq 1800$.

Fig. 5.37. Faixa de variação de T_{amb} .

$\Rightarrow$ A **Propriedade 2** é verdadeira se as Hipóteses 2A, 2B, 2C e 2D são verdadeiras.

5.3.2.16. *Etapa 6 – Construção dos Seqüentes Globais*

Os seqüentes globais para os infinitos cenários variam entre si apenas pelo número de disparo das transições $t_{1_9.01}$, $t_{2_9.01}$, $t_{3_9.01}$ e $t_{4_9.01}$. Alguns exemplos são:

- **Cenário 1-1-2-1:** $p_{4_20.01}, p_{1_12.01}, p_{1_7.01}, p_{1_5.01}, p_{1_9.01}, t_{5_20.01}, t_{7_20.01/1_12.02}, t_{3_12.01/1_7.01}, t_{5_7.01/1_5.01} \vdash p_{6_20.01} \otimes p_{4_12.01} \otimes p_{2_7.01} \otimes p_{5_7.01} \otimes p_{2_5.01} \otimes p_{1_9.01}$.
- **Cenário 1-1-2-2:** $p_{4_20.01}, p_{1_12.01}, p_{1_7.01}, p_{1_5.01}, p_{1_9.01}, t_{5_20.01}, t_{7_20.01/1_12.02}, t_{3_12.01/1_7.01}, t_{5_7.01/1_5.01}, t_{3_9.01} \vdash p_{6_20.01} \otimes p_{4_12.01} \otimes p_{2_7.01} \otimes p_{5_7.01} \otimes p_{2_5.01} \otimes p_{1_9.01}$.

A ordem parcial de disparos das transições para o caso do Cenário 1-1-2-2 é apresentada na Fig. 5.38. Observa-se que, do ponto de vista discreto, o disparo de $t_{3_9.01}$ (entrada de uma pessoa no ambiente condicionado) não está relacionado com os demais disparos do cenário.

Fig. 5.38. Ordem parcial de disparos – Propriedade 2, Cenário 1.

5.3.2.17. *Etapa 7 – Verificação das Hipóteses*

A verificação Hipóteses 2A e 2B é semelhante a verificação das Hipóteses 1A e 1B para Propriedade 1. A Hipótese 2C pode ser verificada através da composição dos objetos $O_{1.7}$ e $O_{1.5}$. A verificação da Hipótese 2D é feita através da composição dos objetos $O_{2.1}$, $O_{2.14}$ e $O_{1.20}$.

5.4. Observações

O Estudo de Caso 1 apresenta dois exemplos onde o processamento de material (no caso, o ar) é contínuo, ilustrando as vantagens e as restrições das abordagens propostas nos Capítulos 3 e 4.

A modelagem e análise do Sistema de Ar Condicionado A, onde não existe ciclo fechado de processamento de material, ilustra as vantagens dos procedimentos propostos nos Capítulos 3 e 4. Na análise de cada objeto, apenas os aspectos relevantes para a verificação da propriedade são considerados. Um exemplo é o caso das Propriedade 1, onde a entrada e saída de pessoas do ambiente, ou a modificação

da temperatura de set-point não interfere no estado do ventilador ou do controlador on/off.

Por outro lado, para o Sistema de Ar Condicionado B, foi verificado que a presença de ciclo fechado no processamento de material impede a decomposição plena do sistema, pois implica no compartilhamento de variáveis em ciclo fechado entre os modelos referentes aos equipamentos envolvidos. Para a modelagem esta limitação na decomposição não é particularmente problemática, uma vez que o modelo em redes PTD-OO do objeto responsável pelo processamento do material (neste caso o objeto Ciclo de Ar B) pode ser definido através da relação de composição/decomposição, onde suas partes são modeladas independentemente. A análise do sistema no entanto fica prejudicada pois não é possível separar a resolução do sistema de equações de uma das partes do objeto Ciclo de Ar B da resolução dos sistemas das demais partes. Isto é, o comportamento do Ciclo de Ar B não pode ser deduzido a partir da análise, de forma isolada, do comportamento de suas partes.

Em ambos os casos, o modelo desenvolvido pode ser utilizado para verificar a influência de eventos discretos no Sistema de Controle Local do ar condicionado. Através da simulação ou da verificação de propriedades do modelo é possível analisar o quanto variações discretas de carga térmica no ambiente perturbam o controle da temperatura no ambiente. O Sistema de Controle Local e o Sistema Supervisório podem então ser redefinidos de forma a minimizar o efeito de tais perturbações.

6 ESTUDO DE CASO 2 – SISTEMA DE ATERRISSAGEM

O segundo estudo de caso considerado neste trabalho é o Sistema de Aterrissagem do avião militar Rafale, fabricado pela empresa Dassault Aviation.

A adoção deste estudo de caso foi incentivada por Boniol; Carennac (2002), onde a verificação de propriedades para este sistema é descrita como um problema aberto, para os quais os métodos tradicionais de análise não apresentaram resultados satisfatórios.

O Sistema de Aterrissagem do avião Rafale vem sendo adotado como um estudo de caso pelo grupo de pesquisa francês StrQdS (Système Temp-réel Qualité de Service⁹) do GdR-CNRS ARP (Architecture, Réseaux et systèmes, Parallélisme¹⁰), que tem como objetivo analisar, testar e comparar técnicas, ferramentas e abordagens para verificação de propriedades comportamentais em sistemas. Alguns resultados obtidos por estes pesquisadores são discutidos na Seção 6.4.

Assim, este estudo de caso visa avaliar a aplicação do procedimento de análise (proposto no Capítulo 4) para sistemas que apresentam elevada complexidade do ponto de vista discreto. Esta avaliação é importante pois a decomposição do sistema em objetos é realizada tendo como base as comunicações contínuas entre os possíveis candidatos (de acordo com o conjunto de Regras de Decomposição proposto no Capítulo 3, Seção 3.1.4).

Em particular, este capítulo ilustra a aplicação do procedimento de análise para verificação de propriedades de segurança. A seguir a Seção 6.1. apresenta uma

⁹ <http://www.laas.fr/strqds/>

¹⁰ <http://www.arp.cnrs.fr/>

descrição do Sistema de Aterrissagem e dos requisitos de seu Sistema Supervisório. A Seção 6.2. apresenta os modelos em redes PTD-OO de algumas classes do sistema que são usadas na análise (as demais classes são apresentadas no Anexo A). Em seguida a Seção 6.3. apresenta como exemplo a verificação de uma propriedade de segurança.

6.1. Descrição do Sistema

6.1.1. Objeto de Controle

A descrição aqui apresentada é baseada nos documentos Dassault (1995) e Dassault (1996), fornecidos pela Dassault Aviation.

O Sistema de Aterrissagem do avião Rafale é formado por 3 conjuntos cada um dos quais compostos um por uma *porta* e um *trem de pouso*. Um esquema simplificado é apresentado na Fig. 6.1.

Fig. 6.1. Conjunto de porta e trem de pouso.

Para aterrisar, a seguinte seqüência deve ser realizada (Fig. 6.2): abrir as portas, estender trens de pouso, fechar portas. Após a decolagem, a seqüência a ser realizada é: abrir as portas, retrain os trens de pouso, fechar as portas.

Fig. 6.2. Seqüência de aterrisagem.

O piloto controla o Sistema de Aterrissagem através de uma alavanca de duas posições (*up* e *down*) que executam as seqüências de aterrisagem (*down*) e

decolagem (*up*). Através de lâmpadas e painéis sinalizadores, o sistema disponibiliza ao piloto uma série de informações sobre o seu estado, incluindo a ocorrência de falhas.

Um esquema ilustrando os demais componentes do sistema é apresentado na Fig. 6.3.

Fig. 6.3. Componentes do Sistema de Aterrissagem.

A movimentação das portas e dos trens de pouso é realizada por pistões hidráulicos. A pressão no diversos circuitos hidráulicos é determinada por um

conjunto de eletro-válvulas. Uma série de sensores discretos do tipo *on/off* informam ao programa de controle os estados de alguns componentes do sistema. Entre os componentes de atuação existe também um relé analógico que isola o computador das eletro-válvulas. Este relé é fechado quando a alavanca do piloto é movimentada e aberto após um determinado tempo da ocorrência da última movimentação da alavanca.

6.1.2. Requisitos do Sistema Supervisório

Entre as funções do Sistema Supervisório está monitorar o Sistema de Aterrissagem através da verificação do estado dos sensores a cada intervalo de K_0 ($K_0 = 40$ ms) e detectar inconsistências. Três níveis de inconsistência são considerados: entre os sensores de uma porta ou de um trem, entre os estados de uma porta e do respectivo trem, entre os estados dos 3 conjuntos de porta e trem. Estes níveis são detalhados a seguir.

Nível 1: Consistência entre os sensores de uma porta ou de um trem.

O estado de cada porta é definido de acordo com os sinais dos sensores, tendo como base a Tabela 6.1.

Tabela 6.1. Estados das portas.

<i>Estado da porta</i>	<i>Sensor porta fechada</i>	<i>Sensor porta aberta</i>
Porta fechada	ON	OFF
Porta em movimento	OFF	OFF
Porta aberta	OFF	ON
INCONSISTENTE	ON	ON

Semelhantemente, o estado de cada trem é definido de acordo com a Tabela 6.2.

Tabela 6.2. Estados dos trens.

<i>Estado do trem</i>	<i>Sensor trem retraído</i>	<i>Sensor trem estendido</i>
Trem retraído	ON	OFF
Trem em movimento	OFF	OFF
Trem estendido	OFF	ON
INCONSISTENTE	ON	ON

Nível 2: Consistência entre os estados de uma porta e do respectivo trem.

Tendo como base o estado de cada porta e do respectivo trem, o estado do conjunto porta-trem é determinado de acordo com Tabela 6.3. Os sete estados desta tabela são organizados em 3 classes principais: 1 – Trem retraído, 2 – Porta aberta, 3 – Trem estendido.

Tabela 6.3. Estados do conjunto porta-trem.

<i>Estado do conjunto</i>	<i>Porta</i>	<i>Trem</i>	<i>Classe</i>
Estado 1	Fechada	Retraído	1
Estado 2	Em movimento	Retraído	1
Estado 3	Aberta	Retraído	1 e 2
Estado 4	Aberta	Em movimento	2
Estado 5	Aberta	Estendido	2 e 3
Estado 6	Em movimento	Estendido	3
Estado 7	Fechada	Estendido	3
INCONSISTENTE	Em movimento	Em movimento	-
INCONSISTENTE	Fechada	Em movimento	-

Nível 3: Consistência entre os estados dos três conjuntos porta-trem.

Os estados dos três conjuntos são considerados consistentes se pertencentes à mesma classe.

Outra função do Sistema Supervisório é executar a sequência de extensão dos trens (*down*) e de retração (*up*) em um tempo máximo de K_{θ_down} e K_{θ_up} , respectivamente.

No primeiro caso (*down*) as atividades a serem realizadas são:

1. Abrir a eletro-válvula geral.
2. Abrir a eletro-válvula de abertura de portas.
3. Fechar a eletro-válvula de abertura de portas.
4. Abrir a eletro-válvula de extensão de trens.
5. Fechar a eletro-válvula de extensão de trens.
6. Abrir a eletro-válvula de fechamento de portas.
7. Fechar a eletro-válvula de fechamento de portas.

8. Fechar a eletro-válvula geral.

A seqüência de atividades para a retração (*up*) são :

1. Abrir a eletro-válvula geral.
2. Abrir a eletro-válvula de abertura de portas.
3. Fechar a eletro-válvula de abertura de portas.
4. Abrir a eletro-válvula de retração de trens.
5. Fechar a eletro-válvula de retração de trens.
6. Abrir a eletro-válvula de fechamento de portas.
7. Fechar a eletro-válvula de fechamento de portas.
8. Fechar a eletro-válvula geral.

Além destas funções, o Sistema Supervisório deve ainda detectar falhas nos seguintes casos:

- Quando as portas não estão abertas após de um intervalo de K_{01} a partir do instante que uma ordem para abertura de portas é emitida, ou não estão fechadas após K_{01} da emissão de uma ordem para fechamento de portas.
- Semelhantemente, quando os trens não estão estendidos após um intervalo de K_{01} a partir do instante que uma ordem para extensão de trens é emitida, ou não estão retraídos após K_{01} da emissão de uma ordem para retração de trens.
- Quando o sensor de pressão não detecta pressão no circuito hidráulico após um intervalo de K_{01} a partir do instante que uma ordem para pressurização do circuito é emitida, ou detecta pressão após K_{01} da emissão de uma ordem para despressurização.

Observa-se que, apesar de se incluir entre as funções do Sistema Supervisório a detecção de falhas, o seu diagnóstico e tratamento não é considerado neste trabalho, pois, neste caso, envolve a colaboração com um segundo Sistema Supervisório (backup implementado em outro computador) e a consideração dos estados de outros dois conjuntos de sensores (backups), que estão fora do escopo deste estudo de caso.

6.2. Modelagem do Sistema Supervisório e seu Objeto de Controle

Uma vez que a aplicação do procedimento proposto para modelagem já foi ilustrada para o estudo de caso do Capítulo 5, no caso do Sistema de Aterrissagem, o detalhamento das diversas **atividades** deste procedimento é colocado no Anexo A.

No que se refere a modelagem, apresenta-se a seguir apenas os objetos e classes relacionados ao sistema de acionamento das portas, que são posteriormente utilizados na Seção 6.3. A lista completa de objetos e classes do Sistema de Aterrissagem, assim como o modelo em redes PTD-OO das demais classes encontram-se no Anexo A.

6.2.1. Exemplos de Classes e Objetos

O conjunto de objetos e classes que modelam o acionamento das portas é formado por:

Objeto de Controle

- C_1 – Equipamento 1 pistão: $O_{1,1} = \underline{\text{Porta Frontal}}$, $O_{2,1} = \underline{\text{Porta Direita}}$, $O_{3,1} = \underline{\text{Porta Esquerda}}$;
- C_7 – Eletro-válvula de Pressão Positiva: $O_{1,7} = \underline{\text{EV Abertura de Portas}}$;
- C_8 – Eletro-válvula de Pressão Negativa: $O_{1,8} = \underline{\text{EV Fechamento de Portas}}$;
- C_9 – Circuito Hidráulico Dedicado: $O_{1,9} = \underline{\text{CH Portas}}$;
- C_{12} – Circuito Elétrico Dedicado: $O_{1,12} = \underline{\text{CE Abertura de Portas}}$, $O_{2,12} = \underline{\text{CE Fechamento de Portas}}$;

Sistema Supervisório

- C_{19} – Interface EV Dedicada: $O_{1,19} = \underline{\text{Interface EV Portas}}$.

O modelo em redes PTD-OO de cada classe é apresentado a seguir.

C_1 – Equipamento 1 Pistão (Fig. 6.5)

Esta classe modela os equipamentos cujo estado é determinado pela posição de um único pistão: as portas e o trem frontal. A posição deste pistão depende da pressão no circuito hidráulico correspondente, de acordo com o ilustrado na Fig. 6.4. Quando a porta está fechada ou o trem frontal está recolhido, e a diferença de pressão $p_{11,C9}$ no pistão é superior a K_p , inicia-se a extensão do pistão, que é realizada com

uma velocidade constante de K_v . A posição do equipamento é representada pela variável x . Se a pressão cai para um valor inferior a K_p , o movimento é interrompido e a porta permanece parcialmente aberta ou, no caso do trem, parcialmente estendido.

Fig. 6.4. Abertura e fechamento das portas.

Fig. 6.5. Modelo da classe C_1 – Equipamento 1 Pistão.

A porção do circuito hidráulico que move os pistões das portas (ou dos trens) é chamada de circuito hidráulico dedicado (modelado por C_9). Para controlar a pressão neste circuito existem duas eletro-válvulas (Fig. 6.6), chamadas de eletro-válvula de pressão positiva (modelada por C_7) e eletro-válvula de pressão negativa (modelada por C_8).

Com base na posição destas eletro-válvulas, a pressão no circuito hidráulico dedicado pode assumir 3 estados principais: pressão negativa, pressão positiva e bloqueado, ilustrados na Fig. 6.6. Se ambas as válvulas permanecerem abertas, a pressão no circuito seria nula, ocasionando uma instabilidade na posição do pistão. Esta situação não deve ocorrer durante o funcionamento do sistema.

Fig. 6.6. Circuito hidráulico dedicado e eletro-válvulas correspondentes.

Ambas as classes C_7 – *Eletro-válvula de Pressão Positiva* e C_8 – *Eletro-válvula de Pressão Negativa* são definidas como especialização de uma classe genérica C_6 – *Eletro-válvula Dedicada*.

C_6 – *Eletro-válvula Dedicada* (Fig. 6.7)

A eletro-válvula pode assumir dois estados principais: fechada (p_{1_6}) e aberta (p_{4_6}), interagindo com o circuito hidráulico dedicado de acordo com as interfaces para t_{2_6} , t_{3_6} , t_{4_6} e t_{5_6} , especificadas nas suas especializações.

Fig. 6.7. Modelo da classe C_6 - *Eletro-válvula Dedicada*.

C_7 – *Eletro-válvula de Pressão Positiva*

Neste caso as seguintes interfaces são especificadas para as transições t_{2_6} , t_{3_6} , t_{4_6} e t_{5_6} :

- $t_{2_7} \rightarrow t_{3_9.11}$ – Bloquear pressão positiva

- $t_{3_7} \rightarrow t_{4_9,11}$ – Colocar pressão positiva
- $t_{4_7} \rightarrow t_{5_9,11}$ – Anular pressão negativa

C_8 – Eletro-válvula de Pressão Negativa

Neste caso as seguintes interfaces são especificadas para as transições t_{2_6} , t_{3_6} , t_{4_6} e t_{5_6} :

- $t_{2_8} \rightarrow t_{2_9,11}$ – Bloquear pressão negativa
- $t_{3_8} \rightarrow t_{1_9,11}$ – Colocar pressão negativa
- $t_{4_8} \rightarrow t_{6_9,11}$ – Anular pressão positiva

C_9 – Circuito Hidráulico Dedicado (Fig. 6.8)

O circuito hidráulico dedicado tem sua pressão variada de acordo com as posições das eletro-válvulas e com a pressão no circuito hidráulico geral ($p_{g,11,C5}$).

Fig. 6.8. Modelo da classe C_9 – Circuito Hidráulico Dedicado.

A abertura e o fechamento das eletro-válvulas do circuito hidráulico dedicado são realizados de acordo com o estado do respectivo circuito elétrico, que corresponde a um objeto da classe C_{12} – Circuito Elétrico Dedicado, que é definida como especialização de uma classe genérica C_{10} – Circuito Elétrico Genérico.

C_{10} – Circuito Elétrico Genérico (Fig. 6.9)

O estados dos circuitos elétricos dependem não apenas do sinal enviado pelo Sistema Supervisório, mas também da posição do relé analógico (Fig. 6.3). Basicamente, a eletro-válvula correspondente ao circuito elétrico é aberta (t_{1_10}) quando o circuito é energizado (t_{4_10}) pelo Sistema Supervisório. Isto só pode ocorrer quando o circuito deixou de ser isolado (t_{7_10}) pelo relé analógico. As transições

t_{1_10} , t_{5_10} e t_{6_10} correspondem a interface com a respectiva eletro-válvula, que é especificada nas classes C_{11} e C_{12} .

Fig. 6.9. Modelo da classe C_{10} – Circuito Elétrico Genérico.

C_{12} – Circuito Elétrico Dedicado

Neste caso as seguintes interfaces são especificadas para as transições t_{1_10} , t_{5_10} e t_{6_10} :

- $t_{1_12} \rightarrow t_{1_6.11}$ – Abrir eletro-válvula dedicada
- $t_{5_12} \rightarrow t_{5_6.11}$ – Fechar eletro-válvula dedicada
- $t_{6_12} \rightarrow t_{5_6.11}$ – Fechar eletro-válvula dedicada

O objeto do Sistema Supervisório responsável por interagir com os circuitos elétricos dedicados das eletro-válvulas é modelado pela classe C_{19} – Interface EV Dedicadas.

C_{19} – Interface EV Dedicadas (Fig. 6.10)

Esta classe atua sobre um par de eletro-válvulas com efeitos contrários: eletro-válvula de pressão positiva (I_2) e eletro-válvula de pressão negativa (I_1), de forma a estender e recolher os pistões conforme solicitado.

Uma lâmpada é acesa no painel do piloto quando os pistões referentes às portas ou aos trens não estão recolhidos.

Fig. 6.10. Modelo da classe C_{19} – Interface EV Dedicadas.

Considerou-se como estado inicial do Sistema de Aterrissagem a situação na qual ele está completamente estendido (posição *down*), que corresponde a seguinte marcação:

- $O_{1,1}$ = Porta Frontal; $X_{1,1} = \{x = 0, K_p = 10, K_v = 1, K_x = 0,5, I_1 = \underline{\text{CH Portas}}, I_2 = \underline{\text{Porta Frontal Fechada}}, I_3 = \underline{\text{Porta Frontal Aberta}}\}$; $m_{1,1} = \{p_{1_1}\}$;
- $O_{2,1}$ = Porta Direita; $X_{2,1} = \{x = 0, K_p = 10, K_v = 1, K_x = 0,5, I_1 = \underline{\text{CH Portas}}, I_2 = \underline{\text{Porta Direita Fechada}}, I_3 = \underline{\text{Porta Direita Aberta}}\}$; $m_{2,1} = \{p_{1_1}\}$;
- $O_{3,1}$ = Porta Esquerda; $X_{3,1} = \{x = 0, K_p = 10, K_v = 1, K_x = 0,5, I_1 = \underline{\text{CH Portas}}, I_2 = \underline{\text{Porta Esquerda Fechada}}, I_3 = \underline{\text{Porta Esquerda Aberta}}\}$; $m_{3,1} = \{p_{1_1}\}$;
- $O_{1,7}$ = EV Abertura de Portas; $X_{1,7} = \{I_1 = \underline{\text{CH Portas}}\}$; $m_{1,7} = \{p_{1_7}\}$;
- $O_{1,8}$ = EV Fechamento de Portas; $X_{1,8} = \{I_1 = \underline{\text{CH Portas}}\}$; $m_{1,8} = \{p_{1_8}\}$;
- $O_{1,9}$ = CH Portas; $X_{1,9} = \{p = -9,6, I_1 = \underline{\text{EV/CH Geral}}\}$; $m_{1,9} = \{p_{1_9}\}$;
- $O_{1,12}$ = CE Abertura de Portas; $X_{1,12} = \{I_1 = \underline{\text{EV Abertura de Portas}}\}$; $m_{1,12} = \{p_{7_12}\}$;

- $O_{2.12} = \underline{\text{CE Fechamento de Portas}}$; $X_{2.12} = \{I_1 = \underline{\text{EV Fechamento de Portas}}\}$; $m_{2.12} = \{p_{7.12}\}$;
- $O_{1.19} = \underline{\text{Interface EV Portas}}$; $X_{1.19} = \{\theta = \text{ind}, K_{\square 1} = 2, K_{\square 2} = 1, I_1 = \underline{\text{CE Fechamento de Portas}}, I_2 = \underline{\text{CE Abertura de Portas}}, I_3 = \underline{\text{Porta Frontal Aberta}}, I_4 = \underline{\text{Porta Direita Aberta}}, I_5 = \underline{\text{Porta Esquerda Aberta}}, I_6 = \underline{\text{Porta Frontal Fechada}}, I_7 = \underline{\text{Porta Direita Fechada}}, I_8 = \underline{\text{Porta Esquerda Fechada}}\}$; $m_{1.19} = \{p_{1.19}\}$;

6.3. Análise dos Modelos em redes PTD-OO

A validação do Sistema de Aterrissagem implica na verificação de uma série de propriedades de segurança e alcançabilidade. Uma vez que, para o estudo de caso do Capítulo 5, foram detalhados exemplos de verificação de propriedades de alcançabilidade, apresenta-se a seguir um exemplo de verificação de propriedade de segurança.

6.3.1. Propriedade 1

6.3.1.1. Etapa 1 - Definição do enunciado da propriedade

O enunciado da **Propriedade 1** é definido de acordo com o tipo de enunciado PS1 (apresentado no Capítulo 4, Seção 4.3.4.1):

- **Propriedade 1** - Os circuitos hidráulicos dedicados nunca podem estar sem pressão: os estados $p_{4.9.01}=1$ (do objeto CH Portas) e $p_{4.9.02}=1$ (do objeto CH Trens) nunca são alcançados.

6.3.1.2. Etapa 2 - Definição do conjunto de restrições da propriedade

Nenhuma restrição é imposta, a **Propriedade 1** deve ser verdadeira em qualquer circunstância.

6.3.1.3. Etapa 3 – Construção dos Diagramas de Colaboração Estáticos

A Fig. 6.11 apresenta o Diagrama de Colaboração Estático dos objetos referentes ao acionamento das portas. Nesta figura destacam-se as comunicações entre os objetos que geram obrigações de análise para a **Propriedade 1**.

Fig. 6.11. Interações relevantes para **Propriedade 1**.

Para facilitar a compreensão do procedimento de verificação da **Propriedade 1**, apresenta-se uma breve discussão sobre os objetos a serem analisados e os resultados esperados destas análises.

Resumidamente, o estado ‘Sem pressão’ ($p_{4.9.01}$) é atingido se ambas as válvulas EV Abertura de Portas ($O_{1.7}$) e EV Fechamento de Portas ($O_{1.8}$) estão simultaneamente abertas. A análise de CH Portas ($O_{1.9}$) determina dois possíveis cenários que levam a este estado: abrir EV Fechamento de Portas quando EV Abertura de Portas está aberta (**Cenário 1p**), ou abrir EV Abertura de Portas quando EV Fechamento de Portas está aberta (**Cenário 2p**).

Para provar que estes cenários proibidos são falsos, verifica-se que sempre que EV Abertura de Portas é aberta, ela deve ser fechada *antes* ($\Delta\theta > 0$) que EV Fechamento de Portas possa ser aberta (**Cenários 1c**), e que sempre que EV Fechamento de Portas é aberta, ela deve ser fechada antes que EV Abertura de Portas possa ser aberta (**Cenários 2c**).

As eletro-válvulas são acionadas pelo respectivos circuitos elétricos ($O_{1.12}$ e $O_{2.12}$), que são ativados pelo objeto Interface EV Portas ($O_{1.19}$) do Sistema Supervisório. Assim, a verificação da **Propriedade 1** deve envolver a análise de todos estes objetos, e inicia-se pela análise de CH Portas ($O_{1.9}$).

6.3.1.4. **Etap**a 4.1 – Parte Discreta – Busca de Cenários ($O_{1.9}$ - CH Portas)

Para determinar os cenários que resultam em $p_{4.9.01}$, o seguinte seqüente é analisado, resultando nos **Cenário 1p** e **2p**:

- Dado um disparo qualquer de $t_{1_9.O1/3_8.O1}$, $t_{2_9.O1/2_8.O1}$ deve disparar *antes* ($\Delta\theta > 0$) da habilitação de $t_{5_9.O1/4_7.O1}$ em $O_{1.7}$.

A Fig. 6.12 ilustra a ordem a parcial de disparos dos cenários considerados nesta prova. Em cada caso são apresentadas as duas possíveis variações para a evolução do cenário: ‘p’, em vermelho e ‘c’ em azul. Em preto são representados eventos em comum entre ‘p’ e ‘c’.

Fig. 6.12. Ordem parcial de disparos – Cenários 1p, 1c, 2p e 2c – Propriedade 1.

6.3.1.5. *Etapla 4.2 – Elaboração de Hipóteses ($O_{1.9}$ - CH Portas)*

Nenhuma hipótese é elaborada.

6.3.1.6. *Etapla 4.3 – Parte Contínua – Evolução de variáveis contínuas e datas de disparos ($O_{1.9}$ - CH Portas)*

Não existem funções de habilitação associadas às transições deste objeto. Para que as datas de habilitação das transições sejam determinadas e a propriedade seja verificada, os objetos $O_{1.7}$ e $O_{1.8}$ devem ser analisados.

6.3.1.7. *Etapla 5.1 – Parte Discreta – Busca de Cenários ($O_{1.8}$ - EV Fechamento de Portas)*

Apresenta-se a seguir o detalhamento de cada cenário.

- **Cenário 1p** - o único evento deste cenário referente a interface entre $O_{1.8}$ e $O_{1.9}$ é o disparo de $t_{4_8.O1/6_9.O1}$, tem-se então:

- *Busca 1* (após o disparo de $t_{4_8.O1/6_9.O1}$): esta busca é considerada irrelevante para a propriedade analisada.
- *Busca 2* – (até o disparo de $t_{4_8.O1/6_9.O1}$): $\Gamma_0 = p_{2_8.O1}$ e $\Gamma_f = \emptyset$

$$\frac{p_{2_8.O1} \text{ — } p_{2_8.O1} \quad \Gamma_0, !t_{1_8.O1}, !t_{5_8.O1} \text{ — } p_{1_8.O1}}{\Gamma_0, !t_{1_8.O1}, !t_{5_8.O1} \text{ — } p_{2_8.O1}} \text{ — } o \text{ L } (t_{1_8.O1})$$

- *Definição de cenários:*

- **Cenário 1p:** $t_{4_8.O1/6_9.O1}$; $t_{1_12.O2/1_8.O1}$

- **Cenário 1c** - não contém disparo de transições da interface deste objeto.
- **Cenário 2p** - o único evento a ser considerado é o disparo de $t_{3_8.01/1_9.01}$:
 - *Busca 1* (após o disparo de $t_{3_8.01/1_9.01}$): esta busca é considerada irrelevante para a propriedade analisada.
 - *Busca 2* (até o disparo de $t_{3_8.01/1_9.01}$): $\Gamma_0 = p_{1_8.01}$ e $\Gamma_f = \emptyset$.

$$\frac{p_{2_8.01} \multimap p_{2_8.01} \quad \Gamma_0, !t_{1_8.01}, !t_{5_8.01} \multimap p_{1_8.01}, \Gamma_f}{\Gamma_0, !t_{1_8.01}, !t_{5_8.01} \vdash p_{2_8.01}, \Gamma_f} \multimap L (t_{1_8.01})$$

- *Definição de cenários:*
 - **Cenário 2p:** $t_{3_8.01/1_9.01}$; $t_{1_12.02/1_8.01}$
- **Cenário 2c** - os eventos a serem considerados são o disparo de $t_{2_8.01/2_9.01}$ e o disparo de $t_{3_8.01/1_9.01}$:
 - *Busca 1* (após o disparo de $t_{2_8.01/2_9.01}$): esta busca é considerada irrelevante para a propriedade analisada.
 - *Busca 2* (do disparo de $t_{3_8.01/1_9.01}$ até o disparo de $t_{2_8.01/2_9.01}$): $\Gamma_0 = p_{4_8.01}$ e $\Gamma_f = \emptyset$.

$$\frac{p_{3_8.01} \multimap p_{3_8.01} \quad \Gamma_0, !t_{1_8.01}, !t_{5_8.01} \multimap p_{4_8.01}, \Gamma_f}{\Gamma_0, t_{3_8.01}, !t_{1_8.01}, !t_{5_8.01} \vdash p_{3_8.01}, \Gamma_f} \multimap L (t_{5_8.01})$$

- *Busca 2 – Verificação de outros cenários concorrentes:* a partir do disparo de $t_{3_8.01/1_9.01}$ ($p_{4_8.01}$) o único cenários possível é o **Cenário 2c**.
- *Busca 3* (até o disparo de $t_{3_8.01/1_9.01}$): semelhante à *Busca 2* do **Cenário 2c**.
- *Definição de cenários:*
 - **Cenário 2c:** $t_{2_8.01/2_9.01}$; $t_{5_12.02/5_8.01}$; $t_{3_8.01/1_9.01}$; $t_{1_12.02/1_8.01}$

6.3.1.8. *Etapa 5.2 – Elaboração de Hipóteses ($O_{1.8}$ - EV Fechamento de Portas)*

É feita a seguinte hipótese, que corresponde ao tipo de hipótese H1 (apresentado no Capítulo 4, Seção 4.3.3.6):

- Hipótese 1A: No intervalo de tempo considerado, as chamada de métodos solicitadas pelo objeto são imediatamente executadas: após o disparo de $t_{1_12.02/1_8.01}$, $t_{3_8.01/1_9.01}$ ou $t_{4_8.01/6_9.01}$ disparam em $\Delta\theta = 0$, e, após o disparo de $t_{5_12.02/5_8.01}$, $t_{2_8.01/2_9.01}$ dispara em $\Delta\theta = 0$.

6.3.1.9. Etapa 5.3 – Parte Contínua – Evolução de variáveis contínuas e datas de disparos ($O_{1.8}$ - EV Fechamento de Portas)

Não existem funções de habilitação associadas as transições. De acordo com a hipótese feita:

- **Cenário 1p:**
 - A transição $t_{4_8.01/6_9.01}$ é habilitada em $O_{1.8}$ em $\theta_{4_8} = \theta_{1_12.02/1_8.01}$. Além disso, se esta transição é disparada (**Cenário 1p**) $\theta_{4_8.01/6_9.01} = \theta_{1_12.02/1_8.01}$.
- **Cenário 2c:**
 - A transição $t_{2_8.01/2_9.01}$ é habilitada em $O_{1.8}$ em $\theta_{2_8} = \theta_{5_12.02/5_8.01}$. Além disso, se esta transição é disparada (**Cenário 2c**) $\theta_{2_8.01/2_9.01} = \theta_{5_12.02/5_8.01}$.
- **Cenários 2p e 2c:**
 - $\theta_{3_8.01/1_9.01} = \theta_{1_12.02/1_8.01}$.

6.3.1.10. Etapa 5.1 – Parte Discreta – Busca de Cenários ($O_{2.8}$ - EV Abertura de Portas)

A análise deste objeto é semelhante a do objeto EV Fechamento de Válvulas.

Após a análise dos objetos $O_{1.7}$ e $O_{1.8}$, a ordem parcial dos disparos dos cenários considerados é ilustrada na Fig. 6.13.

Fig. 6.13. Ordem parcial de disparos – Cenários 1p, 1c, 2p e 2c – Propriedade 1.

6.3.1.11. Etapa 5.2 – Elaboração de Hipóteses ($O_{2.8}$ - EV Abertura de Portas)

A seguinte hipótese é elaborada:

- Hipótese 1B (correspondente a H1): No intervalo de tempo considerado, as chamadas de métodos solicitadas pelo objeto são imediatamente executados: após o disparo de $t_{1_12.01/1_7.01}$, $t_{3_7.01/4_9.01}$ ou $t_{4_7.01/5_9.01}$ disparam em $\Delta\theta = 0$, e, após o disparo de $t_{5_12.01/5_7.01}$, $t_{2_7.01/3_9.01}$ dispara em $\Delta\theta = 0$.

6.3.1.12. Etapa 5.3 – Parte Contínua – Evolução de variáveis contínuas e datas de disparos ($O_{2.8}$ - EV Abertura de Portas)

Não existem funções de habilitação associadas as transições. De acordo com a hipótese feita:

- **Cenário 1c:**
 - A transição $t_{2_7.01/3_9.01}$ é habilitada em $O_{1.7}$ em $\theta_{2_7} = \theta_{5_12.01/5_7.01}$. Além disso, se esta transição é disparada (**Cenário 1c**) $\theta_{2_7.01/3_9.01} = \theta_{5_12.01/5_7.01}$.
- **Cenário 2p:**
 - A transição $t_{4_7.01/5_9.01}$ é habilitada em $O_{1.7}$ em $\theta_{4_7} = \theta_{1_12.01/1_7.01}$. Além disso, se esta transição é disparada (**Cenário 2p**) $\theta_{4_7.01/5_9.01} = \theta_{1_12.01/1_7.01}$.
- **Cenários 1p e 1c:**
 - Para o disparo de $t_{3_7.01/4_9.01}$ (**Cenários 1c e 1p**): $\theta_{3_7.01/4_9.01} = \theta_{1_12.01/1_7.01}$.
- **Condições para Propriedade 1** – Baseando-se na análise de $O_{1.7}$ e $O_{1.8}$, a condição para veracidade da **Propriedade 1** é rescrita como:
 - Dado um disparo qualquer de $t_{4_9.01/3_7.01}$, $t_{5_12.01/5_7.01}$ deve disparar *antes* ($\Delta\theta > 0$) do disparo de $t_{1_12.02/1_8.01}$. Além disso, para que $t_{6_9.01/4_8.01}$ não esteja habilitada em no momento de disparo de $t_{4_9.01/3_7.01}$, o disparo de $t_{1_12.02/1_8.01}$ deve ocorrer *após* o disparo de $t_{4_9.01/3_7.01}$.
 - Dado um disparo qualquer de $t_{1_9.01/3_8.01}$, $t_{5_12.02/5_8.01}$ deve disparar *antes* ($\Delta\theta > 0$) do disparo de $t_{1_12.01/1_7.01}$. Além disso, para que $t_{5_9.01/4_7.01}$ não esteja habilitada em no momento de disparo de $t_{1_9.01/3_8.01}$, o disparo de $t_{1_12.01/1_7.01}$ deve ocorrer *após* o disparo de $t_{1_9.01/3_8.01}$.

Para que as datas de disparo sejam calculadas e a propriedade seja verificada, os objetos $O_{1.12}$ e $O_{2.12}$ devem ser analisados.

6.3.1.13. **Etapa 5.1 – Parte Discreta – Busca de Cenários** ($O_{2.12}$ - CE Fechamento de Portas)

São realizadas as seguintes buscas para cada cenário:

- **Cenário 1p:**

- *Busca 1* (após o disparo de $t_{1_12.O2/1_8.O1}$): esta busca é considerada irrelevante para a propriedade analisada.
- *Busca 2* (até o disparo de $t_{1_12.O2/1_8.O1}$): considerando apenas um último disparo tem-se $\Gamma_0 = p_{6_12.O2}$ e $\Gamma_f = \emptyset$.

$$\frac{p_{3_12.O2} \text{ — } p_{3_12.O2} \quad \Gamma_0, !t_{2_12.O2}, \dots, !t_{8_12.O2} \text{ — } p_{6_12.O2}, \Gamma_f}{\Gamma_0, !t_{2_12.O2}, !t_{3_12.O2}, !t_{4_12.O2}, !t_{6_12.O2}, !t_{7_12.O2}, !t_{8_12.O2} \text{ — } p_{3_12.O2}, \Gamma_f} \text{ — } O \text{ L } (t_{4_12.O2})$$

- *Definição de cenários:*

- **Cenário 1p:** $t_{1_12.O2/1_8.O1}$; $t_{16_19.O1/4_12.O1}$

- **Cenário 1c:** não contém disparo de transições da interface deste objeto.

- **Cenário 2p:**

- *Busca 1* (após o disparo de $t_{1_12.O2/1_8.O1}$): esta busca é considerada irrelevante para a propriedade analisada.
- *Busca 2* (até o disparo de $t_{1_12.O2/1_8.O1}$): semelhante à *Busca 2* realizada para o **Cenário 1p**.
- *Definição de cenários:*

- **Cenário 2p:** $t_{1_12.O2/1_8.O1}$; $t_{16_19.O1/4_12.O1}$

- **Cenário 2c:**

- *Busca 1* (após o disparo de $t_{5_12.O2/5_8.O1}$): esta busca é considerada irrelevante para a propriedade analisada.
- *Busca 2* (do disparo de $t_{1_12.O2/1_8.O1}$ até o disparo de $t_{5_12.O2/5_8.O1}$): $\Gamma_0 = p_{2_12.O2}$ e $\Gamma_f = \emptyset$.

$$\frac{p_{4_12.O2} \text{ — } p_{4_12.O2} \quad \Gamma_0, t_{2_12.O2}, \dots, !t_{8_12.O2} \text{ — } p_{2_12.O2}, \Gamma_f}{\Gamma_0, !t_{2_12.O2}, !t_{3_12.O2}, !t_{4_12.O2}, !t_{7_12.O2}, !t_{8_12.O2} \text{ — } p_{4_12.O2}, \Gamma_f} \text{ — } O \text{ L } (t_{2_12.O2})$$

- *Busca 2 – Verificação de cenários concorrentes:* a partir do disparo de $t_{1_12.O2/1_8.O1}$ ($p_{2_12.O2}$) o único cenário possível é o **Cenário 2c**.
- *Busca 3* (até o disparo de $t_{1_12.O2/1_8.O1}$): semelhante à *Busca 2* realizada para o **Cenário 1p**.

- *Definição de cenários:*

- **Cenário 2c:** $t_{5_12.02/5_8.01}$; $t_{5_19.01/2_12.01}$; $t_{1_12.02/1_8.01}$; $t_{16_19.01/4_12.01}$

6.3.1.14. **Etapa 5.2** – *Elaboração de Hipóteses* ($O_{2.12}$ - CE Fechamento de Portas)

A seguinte hipótese é elaborada:

- Hipótese 1C (correspondente a H1): No intervalo de tempo considerado, as chamadas de métodos solicitadas pelo objeto são imediatamente executados: após o disparo de $t_{4_12.02/16_19.01}$, $t_{1_12.02/1_8.01}$ dispara em $\Delta\theta = 0$, e, após o disparo de $t_{2_12.02/5_19.01}$, $t_{5_12.02/5_8.01}$ dispara em $\Delta\theta = 0$.

6.3.1.15. **Etapa 5.3** – *Parte Contínua – Evolução de variáveis contínuas e datas de disparos* ($O_{2.12}$ - CE Fechamento de Portas)

Não existem funções de habilitação associadas as transições. De acordo com a hipótese feita:

- **Cenário 1p:**

- A transição $t_{4_8.01/6_9.01}$ é habilitada em $O_{1.8}$ em $\theta_{4_8} = \theta_{1_12.02/1_8.01} = \theta_{16_19.01/4_12.02}$. Além disso, se esta transição é disparada (**Cenário 1p**) $\theta_{4_8.01/6_9.01} = \theta_{1_12.02/1_8.01} = \theta_{16_19.01/4_12.02}$.

- **Cenário 2c:**

- A transição $t_{2_8.01/2_9.01}$ é habilitada em $O_{1.8}$ em $\theta_{2_8} = \theta_{5_12.02/5_8.01} = \theta_{5_19.01/2_12.02}$. Além disso, se esta transição é disparada (**Cenário 2c**) $\theta_{2_8.01/2_9.01} = \theta_{5_12.02/5_8.01} = \theta_{5_19.01/2_12.02}$.

- **Cenários 2p e 2c:**

- Para o disparo de $t_{3_8.01/1_9.01}$ (**Cenários 2c e 2p**): $\theta_{3_8.01/1_9.01} = \theta_{1_12.02/1_8.01} = \theta_{16_19.01/4_12.02}$.

6.3.1.16. **Etapa 5.1** – *Parte Discreta – Busca de Cenários* ($O_{1.12}$ - CE Abertura de Portas)

A análise deste objeto é semelhante a do objeto CE Fechamento de Portas.

Após a análise dos objetos $O_{1.12}$ e $O_{2.12}$, a ordem parcial dos disparos dos cenários é ilustrada na Fig. 6.14.

Fig. 6.14. Ordem parcial de disparos – Cenários 1p, 1c, 2p e 2c – Propriedade 1.

6.3.1.17. *Etapa 5.2 – Elaboração de Hipóteses ($O_{1.12}$ - CE Abertura de Portas)*

A seguinte hipótese é elaborada:

- Hipótese 1D (correspondente a H1): No intervalo de tempo considerado, as chamadas de métodos solicitadas pelo objeto são imediatamente executados: após o disparo de $t_{4_12.O1/6_19.O1}$, $t_{1_12.O1/1_7.O1}$ dispara em $\Delta\theta = 0$, e, após o disparo de $t_{2_12.O1/15_19.O1}$, $t_{5_12.O1/5_7.O1}$ dispara em $\Delta\theta = 0$.

6.3.1.18. *Etapa 5.3 – Parte Contínua – Evolução de variáveis contínuas e datas de disparos ($O_{1.12}$ - CE Abertura de Portas)*

Não existem funções de habilitação associadas as transições. De acordo com a hipótese feita:

- **Cenário 1c:**

- A transição $t_{2_7.O1/3_9.O1}$ é habilitada em $O_{1.7}$ em $\theta_{2_7} = \theta_{5_12.O1/5_7.O1} = \theta_{15_19.O1/2_12.O1}$. Além disso, se esta transição é disparada (**Cenário 1c**) $\theta_{2_7.O1/3_9.O1} = \theta_{5_12.O1/5_7.O1} = \theta_{15_19.O1/2_12.O1}$.

- **Cenário 2p:**

- A transição $t_{4_7.O1/5_9.O1}$ é habilitada em $O_{1.7}$ em $\theta_{4_7} = \theta_{1_12.O1/1_7.O1} = \theta_{6_19.O1/4_12.O1}$. Além disso, se esta transição é disparada (**Cenário 2p**) $\theta_{4_7.O1/5_9.O1} = \theta_{1_12.O1/1_7.O1} = \theta_{6_19.O1/4_12.O1}$.

- **Cenários 1p e 1c:**

- Para o disparo de $t_{3_7.O1/4_9.O1}$ (Cenários 1c e 1p): $\theta_{3_7.O1/4_9.O1} = \theta_{1_12.O1/1_7.O1} = \theta_{6_19.O1/4_12.O1}$.

- *Condições para Propriedade 1* – Baseando-se na análise de $O_{1.12}$ e $O_{2.12}$, a condição para veracidade da **Propriedade 1** é rescrita como:

- Dado um disparo qualquer de $t_{4_9.O1/3_7.O1}$ (**Cenário 1p** ou **1c**), para que $t_{5_12.O1/5_7.O1}$ dispare *antes* de $t_{1_12.O2/1_8.O1}$, $t_{15_19.O1/2_12.O1}$ deve disparar em $\theta_{15_19.O1/2_12.O1} < \theta_{16_19.O1/4_12.O2}$. Além disso, para que o disparo de $t_{1_12.O2/1_8.O1}$ ocorra *após* o de $t_{4_9.O1/3_7.O1}$, $\theta_{16_19.O1/4_12.O2} > \theta_{6_19.O1/4_12.O1}$.
- Dado um disparo qualquer de $t_{1_9.O1/3_8.O1}$ (**Cenário 2p** ou **2c**), para que $t_{5_12.O2/5_8.O1}$ dispare *antes* de $t_{1_12.O1/1_7.O1}$, $t_{5_19.O1/2_12.O2}$ deve disparar em $\theta_{5_19.O1/2_12.O2} < \theta_{6_19.O1/4_12.O1}$. Além disso, para que o disparo de $t_{1_12.O1/1_7.O1}$ ocorra *após* o disparo de $t_{1_9.O1/3_8.O1}$, $\theta_{6_19.O1/4_12.O1} > \theta_{16_19.O1/4_12.O2}$.

Para que as datas de disparo sejam calculadas e a propriedade seja verificada, o objeto $O_{1.19}$ deve ser analisado.

6.3.1.19. ***Etap**a 5.1 – Parte Discreta – Busca de Cenários ($O_{1.19}$ - Interface EV Portas)*

Em $O_{1.19}$, a diferença dos demais objetos analisados, os métodos associados a $t_{1_19.O1}$, $t_{2_19.O1}$, $t_{17_19.O1}$ e $t_{18_19.O1}$ podem ser chamados por mais de uma transição, resultando na duplicação destas transições quando a rede deste objeto é desdobrada (de acordo com o apresentado na Seção 2.5.3). Uma vez duplicadas, estas transições são nomeadas como $t_{1_19.O1a}$ (chamada por $t_{16_17.O1}$), $t_{1_19.O1b}$ (chamada por $t_{29_17.O1}$), $t_{2_19.O1a}$ (chamada por $t_{14_17.O1}$), $t_{2_19.O1b}$ (chamada por $t_{31_17.O1}$), $t_{17_19.O1}$ (chamada por $t_{19_17.O1}$), $t_{17_19.O1b}$ (chamada por $t_{26_17.O1}$), $t_{18_19.O1a}$ (chamada por $t_{17_17.O1}$) e $t_{18_19.O1b}$ (chamada por $t_{28_17.O1}$).

No caso dos **Cenários 1p** e **2p**, a ordem de disparo das transições da interface $O_{1.19}$ - $O_{1.12}$ em relação as transições da interface com $O_{1.19}$ - $O_{2.12}$ não é conhecida. Assim, todas as possibilidades devem ser consideradas, resultando na decomposição de cada cenário. Apresenta-se a seguir um resumo dos resultados obtidos:

• **Cenário 1p-1** ($t_{16_19.O1/4_12.O2}$ antes de $t_{6_19.O1/4_12.O1}$):

- *Busca 1* (após o disparo de $t_{6_19.O1/4_12.O1}$): esta busca é considerada irrelevante para a propriedade analisada.
- *Busca 2* (do disparo de $t_{16_19.O1/4_12.O2}$ até o disparo de $t_{6_19.O1/4_12.O1}$): este cenário só é possível se considerarmos um disparo de $t_{5_19.O1/2_12.O2}$ entre os disparos de $t_{16_19.O1/4_12.O2}$ e $t_{6_19.O1/4_12.O1}$. Neste caso são obtidos 4 cenários (**Cenários 1p-1-1 a 1p-1-4**). A inclusão de $t_{5_19.O1/2_12.O2}$ significa que o objeto $O_{2.12}$ deve ser analisado novamente para incluir este disparo (após o disparo de $t_{1_12.O1/1_7.O1}$). A nova ordem parcial de disparos resultante desta análise é ilustrada na Fig. 6.15 para o caso **Cenário 1p-1-1** (para os demais cenários a ordem é semelhante, trocando apenas as transições $t_{1_19.O1a}$ e/ou $t_{2_19.O1a}$ pelas correspondentes $t_{1_19.O1b}$ e $t_{2_19.O1b}$).

Fig. 6.15. Ordem parcial de disparos – **Cenário 1p-1-1 – Propriedade 1.**

- *Busca 3* (até o disparo de $t_{16_19.O1/4_12.O2}$): esta busca é considerada irrelevante para a propriedade analisada.
- *Definição de cenários:*
 - **Cenário 1p-1-1:** $t_{6_19.O1/4_12.O1}$; $t_{4_19.O1}$; $t_{2_19.O1a}$; $t_{1_19.O1a}$; $t_{3_19.O1}$; $t_{5_19.O1/2_12.O2}$; $t_{11_19.O1}$; $t_{12_19.O1}$; $t_{13_19.O1}$; $t_{16_19.O1/4_12.O2}$; ($\Gamma_0 = p_{22_19.O1}$ e $\Gamma_f = \emptyset$)
 - **Cenário 1p-1-2 a 1p-1-4:** semelhantes a **Cenário 1p-1-1** trocando apenas as transições $t_{1_19.O1a}$ e/ou $t_{2_19.O1a}$ pelas correspondentes $t_{1_19.O1b}$ e $t_{2_19.O1b}$
- **Cenário 1p-2** ($t_{6_19.O1/4_12.O1}$ antes de $t_{16_19.O1/4_12.O2}$):
 - *Busca 1* (após o disparo de $t_{16_19.O1/4_12.O2}$): esta busca é considerada irrelevante para a propriedade analisada.

- *Busca 2* (do disparo de $t_{6_19.O1/4_12.O1}$ até a habilitação de $t_{16_19.O1/4_12.O2}$): semelhantemente à *Busca 2* do **Cenário 1p-1**, este cenário só é possível se considerarmos um disparo de $t_{15_19.O1/2_12.O1}$ entre $t_{6_19.O1/4_12.O1}$ e $t_{16_19.O1/4_12.O2}$. Neste caso são obtidos 4 cenários (**Cenários 1p-2-1 a 1p-2-4**) e o objeto $O_{1.12}$ deve ser analisado novamente para incluir este disparo. A nova ordem parcial de disparos resultante desta análise é ilustrada na Fig. 6.16 para o caso **Cenário 1p-2-1** (para os demais cenários a ordem é semelhante, trocando apenas as transições $t_{17_19.O1a}$ e/ou $t_{18_19.O1a}$ pelas correspondentes $t_{17_19.O1b}$ e $t_{18_19.O1b}$). Nesta figura, são representados em preto os eventos em comum entre todos **Cenários 1p** e **1c** e em cinza os eventos em comum apenas entre os **Cenários 1p-1** e **1c**.

Fig. 6.16. Ordem parcial de disparos – **Cenário 1p-2-1 – Propriedade 1.**

- *Busca 3* (até o disparo de $t_{6_19.O1/4_12.O1}$): esta busca é considerada irrelevante para a propriedade analisada.
- *Definição de cenários:*
 - o **Cenário 1p-2-1**: $t_{16_19.O1/4_12.O2}$; $t_{17_19.O1a}$; $t_{18_19.O1a}$; $t_{15_19.O1/2_12.O1}$; $t_{8_19.O1}$; $t_{9_19.O1}$; $t_{10_19.O1}$; $t_{6_19.O1/4_12.O1}$; ($\Gamma_0 = p_{5_19.O1}$ e $\Gamma_f = \emptyset$)
 - o **Cenário 1p-2-2 a 1p-2-4**: semelhantes a **Cenário 1p-1-1** trocando apenas as transições $t_{17_19.O1a}$ e/ou $t_{18_19.O1a}$ pelas correspondentes $t_{17_19.O1b}$ e $t_{18_19.O1b}$
- **Cenário 1c:**
 - *Busca 1* (após o disparo de $t_{15_19.O1/2_12.O1}$): esta busca é considerada irrelevante para a propriedade analisada.
 - *Busca 2* (do disparo de $t_{6_19.O1/4_12.O1}$ até o disparo de $t_{15_19.O1/2_12.O1}$): semelhantemente à realizada para o **Cenários 1p-2**.

- *Busca 2 – Verificação de cenários concorrentes:* a partir do disparo de $t_{6_19.O1/4_12.O1}$, o disparo de $t_{7_19.O2}$ consiste em um possível cenário conflitante, pois inviabiliza o disparo de $t_{15_19.O1/2_12.O1}$. No entanto, como o disparo $t_{15_19.O1/2_12.O1}$ também faz parte dos **Cenários 1p**, ambos os cenários são inviabilizados, o que faz com que a **Propriedade 1** ainda seja verdadeira (neste caso o objeto $O_{1,9}$ estará em ‘deadlock’).
- *Busca 3 (até o disparo de $t_{6_19.O1/4_12.O1}$):* esta busca é considerada irrelevante para a propriedade analisada.
- *Definição de cenários –* A ordem parcial de disparos para o **Cenário 1c** é apresentada na Fig. 6.17:
 - **Cenário 1c:** $t_{15_19.O1/2_12.O1}$; $t_{8_19.O1}$; $t_{9_19.O1}$; $t_{10_19.O1}$; $t_{6_19.O1/4_12.O1}$; ($\Gamma_0 = p_{5_19.O1}$ e $\Gamma_f = \emptyset$)

Fig. 6.17. Ordem parcial de disparos – **Cenários 1c – Propriedade 1.**

- **Cenário 2p-1** (seqüência $t_{16_19.O1/4_12.O2}$; $t_{6_19.O1/4_12.O1}$):
 - *Busca 1* (após o disparo de $t_{6_19.O1/4_12.O1}$): esta busca é considerada irrelevante para a propriedade.
 - *Busca 2* (do disparo de $t_{16_19.O1/4_12.O2}$ até o disparo de $t_{6_19.O1/4_12.O1}$): semelhante a realizada para o **Cenário 1p-1**. Neste caso também $O_{2,12}$ é novamente analisado para incluir o disparo de $t_{5_19.O1/2_12.O2}$ (após o disparo de $t_{1_12.O2/1_8.O1}$) e resulta na seguinte ordem parcial ilustrada na Fig. 6.18, para o caso do **Cenário 2p-1-1**.

Fig. 6.18. Ordem parcial de disparos – **Cenários 2p-1 – Propriedade 1.**

- *Busca 3* (até o disparo de $t_{16_19.O1/4_12.O2}$): esta busca é considerada irrelevante para a propriedade analisada.
- *Definição de cenários*: semelhante a realizada para os **Cenários 1p-1**.
- **Cenário 2p-2** (seqüência $t_{6_19.O1/4_12.O1}$; $t_{16_19.O1/4_12.O2}$):
 - *Busca 1* (após o disparo de $t_{16_19.O1/4_12.O2}$): esta busca é considerada irrelevante para a propriedade analisada.
 - *Busca 2* (do disparo de $t_{6_19.O1/4_12.O1}$ a $t_{16_19.O1/4_12.O2}$): semelhante à realizada para o **Cenários 1p-2**, resultando em uma nova análise de $O_{2.12}$ para incluir o disparo de $t_{15_19.O1/2_12.O1}$ (após o disparo de $t_{1_12.O2/1_8.O1}$). A ordem parcial obtida é ilustrada na Fig. 6.19 para o caso do **Cenário 2p-2-1**.

Fig. 6.19. Ordem parcial de disparos – **Cenários 2p-2-1 – Propriedade 1.**

- *Busca 3* (até o disparo de $t_{6_19.O1/4_12.O1}$): esta busca é considerada irrelevante para a propriedade analisada.
- *Definição de cenários*: semelhante a realizada para os **Cenários 1p-2**.
- **Cenário 2c**:
 - *Busca 1* (após o disparo de $t_{5_19.O1/2_12.O2}$): esta busca é considerada irrelevante para a propriedade analisada.

- *Busca 2* (do disparo de $t_{16_19.O1/4_12.O2}$ a $t_{5_19.O1/2_12.O2}$): semelhante à realizada para o **Cenários 2p-1**.
- *Busca 2 – Verificação de cenários concorrentes*: a partir do disparo de $t_{16_19.O1/4_12.O2}$, o disparo de $t_{14_19.O2}$ consiste em um possível cenário conflitante, pois inviabiliza o disparo de $t_{5_19.O1/2_12.O2}$. Neste caso também este disparo faz parte do **Cenário 2p**, não comprometendo a veracidade da **Propriedade 1**.
- *Busca 3* (até o disparo de $t_{16_19.O1/4_12.O2}$): esta busca é considerada irrelevante para a propriedade analisada.
- *Definição de cenários*: A ordem parcial de disparos para o **Cenário 2c** é apresentada na Fig. 6.20.
 - Cenário 2c: $t_{5_19.O1/2_12.O2}$; $t_{11_19.O1}$; $t_{12_19.O1}$; $t_{13_19.O1}$; $t_{16_19.O1/4_12.O2}$; ($\Gamma_0 = p_{22_19.O1}$ e $\Gamma_f = \emptyset$)

Fig. 6.20. Ordem parcial de disparos – **Cenários 2c** – **Propriedade 1**.

6.3.1.20. **Etapla 5.2** – *Elaboração de Hipóteses* ($O_{1.19}$ - Interface EV Portas)

Nenhuma hipótese é elaborada. Sendo assim:

- Caso alguma das transições $t_{8_19.O1/4_4.O12}$, $t_{9_19.O1/4_4.O10}$ ou $t_{10_19.O1/4_4.O11}$ não seja habilitada, ambos os **Cenários 1p-2** e **1c** se tornam impossíveis.
- Caso alguma das transições $t_{11_19.O1/4_4.O9}$, $t_{12_19.O1/4_4.O7}$ ou $t_{13_19.O1/4_4.O8}$ não seja habilitada, ambos os **Cenários 2p-1** e **2c** se tornam impossíveis.
- Caso alguma das transições $t_{1_19.O1a(b)}$ ou $t_{2_19.O1a(b)}$ não seja habilitada, os **Cenários 1p-1** e **2p-1** se tornam impossíveis.

6.3.1.21. **Etapa 5.3 – Parte Contínua – Evolução de variáveis contínuas e datas de disparos** ($O_{1.19}$ - Interface EV Portas)

• **Cenários 1p-1:**

A data de disparo das transições de interface com objetos não analisados não é conhecida. No entanto, analisando as funções de habilitação, de junção e os sistemas de equações do objeto $O_{1.19}$, tem-se que, para todos os cenários:

$$\begin{aligned} - \quad \theta_{6_19.O1/4_12.O1} \geq \theta_{4_19.O1} = \theta_{2_19.O1a(b)} &\geq (\theta_{1_19.O1a(b)} + K_{\theta 2}) \geq \theta_{3_19.O1} = \theta_{5_19.O1/2_12.O2} \\ &\geq \max(\theta_{11_19.O1/4_4.O9}, \theta_{12_19.O1/4_4.O7}, \theta_{13_19.O1/4_4.O8}) \geq \theta_{16_19.O1/4_12.O2} \Rightarrow \\ \theta_{6_19.O1/4_12.O1} &\geq (\theta_{16_19.O1/4_12.O2} + K_{\theta 2}) \Rightarrow \theta_{6_19.O1/4_12.O1} > \theta_{16_19.O1/4_12.O2}. \end{aligned}$$

No entanto, de acordo com a análise dos outros objetos e as hipóteses feitas, tem-se que:

$$\begin{aligned} - \quad \theta_{4_8.O1/6_9.O1} &= \theta_{1_12.O1/1_8.O1} = \theta_{16_19.O1/4_12.O2}. \\ - \quad \theta_{3_7.O1/4_9.O1} &= \theta_{1_12.O1/1_7.O1} = \theta_{6_19.O1/4_12.O1}. \end{aligned}$$

Isto resulta em $\theta_{3_7.O1/4_9.O1} > \theta_{4_8.O1/6_9.O1}$, o que torna o cenário *impossível* uma vez que $t_{3_7.O1/4_9.O1}$ é condição para o disparo de $t_{4_8.O1/6_9.O1}$.

Interpretando o resultado obtido, os **Cenários 1p-1** consideram os casos em que as duas ordens emitidas pela Interface EV Portas (neste caso $t_{16_19.O1/4_12.O2}$ e $t_{6_19.O1/4_12.O1}$) para abrir as válvulas são executadas na seqüência inversa a sua emissão. As hipóteses realizadas e as análises dos objetos anteriores levaram a conclusão que uma ordem emitida pela Interface EV Portas sempre é executada em um intervalo de tempo $\Delta\theta = 0$. A análise de Interface EV Portas leva a conclusão de que sempre existe um intervalo de tempo $\Delta\theta > 0$ entre a emissão das duas ordens destes cenários, o que implica na execução das ordens na seqüência em que são emitidas e, portanto, os **Cenários 1p-1** são impossíveis.

• **Cenários 2p-2:**

Por uma razão semelhante à dos **Cenários 1p-1**, os **Cenários 2p-2** também são impossíveis.

• **Cenários 1p-2:**

Analisando as funções de habilitação, de junção e os sistemas de equações do objeto $O_{1.19}$, tem-se que, para todos os cenários:

$$\begin{aligned} - \quad \theta_{16_19.O1/4_12.O2} \geq \theta_{17_19.O1a(b)} &\geq (\theta_{18_19.O1a(b)} + K_{\theta 2}) \geq \theta_{15_19.O1/2_12.O1} \geq \\ \max(\theta_{8_19.O1/4_4.O12}, \theta_{9_19.O1/4_4.O10}, \theta_{10_19.O1/4_4.O11}) &\geq \theta_{6_19.O1/4_12.O1} \Rightarrow \geq \end{aligned}$$

$$(\theta_{16_19.01/4_12.02} + K_{\theta 2}) \Rightarrow \theta_{16_19.01/4_12.02} > \theta_{15_19.01/2_12.01} \text{ e } \theta_{16_19.01/4_12.02} > \theta_{6_19.01/4_12.01}$$

De acordo com o resultado acima apresentado, no caso dos eventos da parte em comum entre os **Cenários 1p-2** e **1c** ocorrerem, todas as condições anteriormente estabelecidas para a ocorrência do Cenário 1c no lugar dos **Cenários 1p-1** são satisfeitas, portanto os **Cenários 1p-2** também são impossíveis.

Interpretando o resultado obtido, os **Cenários 1p-2** consideram os casos em que as duas ordens emitidas pela Interface EV Portas são executadas na sequência da sua emissão. No entanto a análise deste objeto indica que sempre que uma ordem para abrir a EV Abertura de Portas é emitida, uma ordem para fechar esta válvula também deve ser emitida antes que uma ordem para abrir EV Fechamento de Portas possa ser emitida. Além disso, sempre existe um intervalo de tempo não nulo ($K_{\theta 2}$) entre as duas últimas ordens, o que indica que a EV Abertura de Portas está efetivamente fechada quando uma ordem para abrir EV Fechamento de Portas é eventualmente emitida.

- **Cenários 2p-1:**

Por uma razão semelhante à dos **Cenários 1p-2**, os **Cenários 2p-1** também são impossíveis.

- **Cenários 1c e 2c:**

Como os eventos deste cenários também fazem parte dos **Cenários 1p-2** e **2p-1**, nenhuma condição adicional é imposta para sua viabilidade.

Para que os resultados obtidos com a análise destes objetos sejam válidos, as Hipóteses 1A a 1D devem ser provadas.

6.3.1.22. ***Etapas 7 – Verificação das Hipóteses***

A verificação das Hipóteses 1A e 1B é realizada através da composição dos objetos $O_{1.7}$, $O_{1.8}$ e $O_{1.9}$.

Para a verificação das Hipóteses 1C e 1D, é realizada a composição dos objetos $O_{1.7}$ e $O_{2.12}$, e $O_{1.8}$ e $O_{1.12}$, respectivamente. Observa-se no entanto que, nestes casos, deve-se introduzir uma nova hipótese (Hipótese 1E) onde supõe-se que o relé analógico ($O_{1.13}$ - Relé Analógico, cujo modelo é apresentado no Anexo A) nunca

está isolando os circuitos elétricos quando um comando é emitido pelo Sistema Supervisório.

A verificação da Hipótese 1E pode ser dividida em duas propriedades de alcançabilidade:

1. O relé analógico sempre está fechado num intervalo de $[0, 15]$ após a modificação do estado da alavanca ‘Up/Down’ do piloto.
2. As seqüência *up* ou *down* sempre são completamente executadas num intervalo de $[0, 14]$ após a modificação do estado da alavanca, garantindo que os circuitos elétricos só estarão energizados neste intervalo.

Por sua vez, esta segunda propriedade pode ser decomposta em uma série de propriedades de alcançabilidade, referentes a duração máxima de cada etapa das seqüências *up* e *down* (pressurizar circuito hidráulico geral, abrir portas, estender ou retrain trens, fechar portas despressurizar circuito hidráulico geral). Para cada uma das propriedades um conjunto restrito de objetos deve ser analisado, garantindo assim a viabilidade da aplicação do procedimento proposto para análise.

6.4. Observações

Os aspectos a serem ressaltados da modelagem deste estudo de caso são:

- A parte contínua dos modelos é relativamente simples, quando comparada aos demais estudos de caso. Em alguns casos se reduz a um temporizador entre dois eventos.
- Não existem muitos compartilhamentos de variáveis contínuas. O caso principal se refere as variáveis relacionadas às pressões nos circuitos hidráulicos.
- Em contrapartida, existem muitas comunicações discretas em ciclo fechado (um objeto chama métodos de outro objeto e após algumas interações recebe uma chamada de método), de forma que o comportamento de um objeto afeta, e é afetado pelo comportamento de muitos ou até mesmo de todos os objetos do sistema.
- O sistema é formado por blocos que se repetem: os modelos para os três conjuntos de porta/trem de pouso são praticamente idênticos, os modelos da parte referente ao circuito hidráulico/eletro-válvulas para as portas é idêntica àquele dos trens de pouso. Isto é particularmente interessante do ponto de vista da

análise porque o que foi determinado para um bloco pode ser estendido para os demais.

Entre os aspectos evidenciados por este estudo de caso está a importância da introdução de hipóteses adequadas, em particular para os casos onde existem comunicações discretas em ciclo fechado. No caso da Propriedade 1, através da introdução das Hipóteses 1C e 1D (e posteriormente da Hipótese 1E) a verificação de uma propriedade que de outra forma envolveria muitos objetos do sistema, é decomposta na verificação de uma série de propriedades envolvendo pouco objetos. Se tais hipóteses não fossem introduzidas, o grande número de cenários a serem analisados poderia tornar inviável a aplicação do procedimento proposto.

Além disso, a verificação da propriedade apresentada ilustra como a explosão de estados pode ser evitada usando um enfoque local e considerando a causalidade entre os eventos (ordem parcial). Considerando por exemplo **Propriedade 1**, a sua verificação envolve cenários da duração de segundos, com cerca de 10 a 15 disparos de transições e 6 objetos. A mesma prova, se fosse realizada considerando uma abordagem global, deveria considerar o estado dos outros 41 objetos e resultaria em cenários com milhares de disparos de transições pois o Sistema Supervisório verifica a coerência do estado dos sensores em intervalos de poucos milissegundos. Estes eventos, apesar de não serem relevantes para a verificação da propriedade, seriam considerados numa abordagem global, e a indeterminação da ordem destes em relação aos demais eventos resultaria em um número muito grande de cenários possíveis a serem analisados.

Este mesmo estudo de caso foi utilizado para testar e analisar as seguintes ferramentas de verificação: ‘NP-Tools + Lucifer translator’ (Ljung, 1999), ‘Lesar’ (Halbwachs, 1992; Lesar, 2003), SMV (Clarke et al., 1993; SMV, 2003), e UPPAAL (Pettersson; Larsen, 2000; UPPAAL, 2003). Os resultados obtidos foram publicados em (Boniol; Carcenac, 2002). Nos primeiros três casos, o sistema de aterrissagem foi descrito usando a linguagem Lustre, no último caso usando autômatos temporizados. Em todos os casos, a dinâmica continua do sistema foi simplificada para modelos temporizados.

Com exceção do SMV, todas as outras ferramentas de verificação apresentaram problemas e não foram capazes de verificar as propriedades

considerando o sistema com 3 trens de pousos e um contexto geral (o comportamento do piloto não é conhecido). Em alguns casos, resultados melhores foram obtidos considerando um ou dois trens de pouso e um contexto particular.

Estes resultados ilustram as limitações das ferramentas existentes e salientam a importância do desenvolvimento de técnicas de análise modular, como a proposta neste trabalho. Apesar de algumas ferramentas, como UPPAAL, permitirem uma modelagem modular do sistema, a análise é feita de forma global. O processo de análise, em geral, enumera todas as possíveis seqüências de eventos em um tempo global, resultando em uma explosão do número de cenários e estados.

7 ESTUDO DE CASO 3 – USINA DE CANA DE AÇÚCAR

O terceiro estudo de caso considerado é de supervisão da produção de açúcar em uma usina. A usina em questão é a Usina Cruz Alta do Grupo Açúcar Guarani S/A, localizada no município de Olímpia - SP.

A escolha deste estudo de caso foi motivada pela diversidade dos processos que compõem a produção industrial de açúcar, oferecendo assim, uma grande variedade de situações para validação do que foi proposto nos Capítulos 2, 3 e 4. Do ponto de vista de sua dinâmica, alguns processos são essencialmente contínuos, outros são classificados como de bateladas ('batch processes') e alguns podem ainda serem considerados discretos.

A Seção 7.1. apresenta uma descrição da Usina Cruz Alta e dos requisitos de seu Sistema Supervisório. Em seguida, para ilustrar a diversidade dos tipos de processos e das características dos fluxos de materiais na Usina Cruz Alta, a Seção 7.2. apresenta a **Atividade 1** do procedimento de modelagem caso. Esta seção apresenta também alguns exemplos de objetos e classes que compõem o sistema. Semelhantemente ao estudo de caso do Capítulo 6, as demais **atividades** do procedimento de modelagem e os demais modelos em redes PTD-OO das classes são apresentados no Anexo B.

No que se refere a análise do sistema, a Seção 7.3. apresenta como exemplo a verificação de uma propriedade de segurança. Diferentemente da propriedade de segurança apresentada no Capítulo 6, cuja verificação se baseava predominantemente na análise da dinâmica discreta dos objeto, neste exemplo aspectos relacionados à dinâmica contínua devem ser considerados.

7.1. Descrição do Sistema

7.1.1. Objeto de Controle

A produção de açúcar na Usina Cruz Alta consiste em uma série de processos mecânicos ou químicos que podem ser organizados nas seguintes etapas (Hugot, 1986):

- **Recepção** – A cana de açúcar chega a usina em caminhões, e pode ser destinada diretamente para a produção ou pode ser armazenada em um fosso para ser posteriormente processada. A cana enviada à produção é lavada e despejada numa esteira transportadora.
- **Preparo** – O preparo consiste essencialmente em passar a cana que está sendo transportada na esteira por um picador e um desfibrador. Após o desfibrador, uma segunda esteira é responsável por levar a cana até o processo de extração.
- **Extração** – Ao contrário de muitas usinas de cana de açúcar no Brasil que utilizam moendas, na Usina Cruz Alta a extração do caldo é realizada através de difusão. A difusão é o processo pelo qual a cana picada e desfibrada é mergulhada em uma solução menos concentrada que o caldo nelas contido e cede à esta solução uma parte ou a totalidade do açúcar que constitui o excedente de concentração de seu caldo. A difusão é realizada no difusor, um equipamento formado por um transportador horizontal sobre o qual se coloca a cana a ser processada. Durante todo o seu trajeto dentro do difusor esta camada de cana é abundantemente regada com solução, extraindo assim o caldo da cana.
- **Tratamento do caldo** – O caldo extraído passa por um processo de sulfitação (adição de dióxido de enxofre – SO_2), calagem (adição de cal – CaO) e aquecimento. O objetivo destes processos é esterilizar, regular o pH, e ajustar a coloração do caldo.
- **Clarificação** – O caldo proveniente dos aquecedores é enviado aos clarificadores, que são decantadores na forma de tanques onde se faz chegar de modo regular e contínuo o caldo a ser decantado. Eles são suficientemente grandes para que a velocidade de escoamento e de circulação do caldo seja lenta o bastante para permitir a decantação.

- **Evaporação** – O caldo clarificado contém cerca de 85% de água. A evaporação deve eliminar a maior parte desta água. Ela é realizada em evaporadores do tipo múltiplo-efeito. O produto resultante, de alta densidade, é chamado de xarope.
- **Cozimento ou Cristalização** – A viscosidade do xarope inviabiliza uma maior concentração nos evaporadores. Para tanto, são utilizados cozedores à vácuo onde ocorre o crescimento dos cristais (cristalização).
- **Centrifugação** – A massa produzida pelo cozedor é destinada as centrífugas, onde o restante da água é retirada.
- **Secagem e Empacotamento** – O açúcar em cristais obtido após a centrifugação é enviado ao secador e por fim ao empacotamento, onde o açúcar produzido é armazenado em sacos.

7.1.2. Requisitos do Sistema Supervisório

A gama de serviços sob responsabilidade do sistema supervisório de uma usina de cana é extremamente vasta, incluindo desde de funções relacionadas ao monitoramento de equipamentos ou processos específicos até os serviços que afetam o funcionamento de toda a usina.

A seleção das funções incluídas neste estudo de caso não objetiva constituir um sistema supervisório completo, que responda à todas as necessidades de uma usina, mas sim compor um conjunto significativo de funções para ilustrar e avaliar os métodos/procedimentos propostos neste trabalho.

Do ponto de vista de gerenciamento da usina como um todo, o sistema supervisório deve:

- Permitir a um operador iniciar e finalizar os diferentes processos da usina – esta função é utilizada por exemplo no caso de paradas semanais.
- Permitir a um operador selecionar entre três níveis de volumes de produção para os diferentes processos da usina de acordo com a demanda e com estoques intermediários.

As demais funções consideradas estão diretamente relacionadas a supervisão de cada uma das etapas do processo (podendo no entanto resultar também na atuação sobre equipamentos de outras etapas).

No caso do recebimento de cana, o sistema supervisório deve:

- Decidir o destino dos caminhões que chegam a usina – se devem ser enviados ao fosso ou a produção.
- Solicitar a transferência de cana do fosso para a produção quando necessário (particularmente durante o período noturno).
- Interromper o fornecimento de cana, desligando as mesas alimentadoras e os respectivos chuveiros em caso de alarme.

No caso do preparo da cana, o sistema supervisório deve:

- Interromper o processo de preparo da cana, desligando as esteiras e demais equipamentos em caso de alarme.
- Solicitar a interrupção do fornecimento de cana no caso de sobrecarregamento do picador ou do desfibrador.

No caso da difusão não foi considerada nenhuma função específica, uma vez que funções de supervisão já estão incorporadas no sistema de controle fornecido com o difusor.

No caso dos processos relacionados ao tratamento do caldo, considerou-se necessário:

- Supervisionar os processos evitando o transbordamento de tanques ou o funcionamento de bombas em vazio.
- Supervisionar o fornecimento de enxofre ao forno rotativo.
- Supervisionar a renovação da cal virgem utilizada para secagem de ar na sulfitação.
- Solicitar a manutenção dos aquecedores.

No caso da evaporação também foi considerada a seguinte função:

- Supervisionar os processos evitando o transbordamento de tanques ou o funcionamento de bombas em vazio.

Para a cristalização e o cozimento considerou-se as seguintes funções:

- Determinar o tipo de massa (A, B ou C) a ser produzida em cada cozedor e configurá-lo adequadamente.
- Evitar transbordamento ou esvaziamento dos tanques de produtos intermediários.
- Providenciar a saída da usina do mel resultante da produção de massa do tipo C.

Para secagem e empacotamento, o sistema supervisório deve:

- Registrar a produção de açúcar.

7.2. Modelagem do Sistema Supervisório e seu Objeto de Controle

Esta seção inicia-se apresentando uma descrição dos processos da usina através da modelagem do fluxo de materiais em PFS (**Atividade 1**), que é fundamental para a compreensão da abrangência deste estudo de caso. Em seguida apresenta-se como exemplo objetos e classes relativos à Recepção e ao Preparo e que são usados na verificação da propriedade de segurança da Seção 7.3.

7.2.1. Atividade 1 – Modelagem do Fluxo de Materiais

Devido à complexidade e ao grande número de processos, utiliza-se neste estudo de caso as técnicas de refinamento sucessivo do PFS. A Fig. 7.1 apresenta o PFS geral do sistema. As atividades estão relacionadas às etapas de produção e são detalhada na seqüência.

Fig. 7.1. PFS para a produção de açúcar cristal.

O vapor utilizado no [Aquecimento] e na [Extração] pode ser proveniente tanto da [Evaporação] quanto da queima do bagaço, diferentemente do processo de cozimento, onde utiliza-se sempre vapor vegetal (gerado na [Extração]). A utilização ou não do vapor vegetal residual influencia apenas no processo de queima de bagaço, que deverá ou não produzir mais vapor. Uma vez que este processo não foi incluído neste estudo de caso, do ponto de vista da supervisão o reaproveitamento do vapor não é considerado na modelagem.

Refinamento de [Recepção]

Na Usina Cruz Alta, o descarregamento dos caminhões de cana é realizado por dois guindastes fixos ao solo, um ao lado do fosso e outro ao lado da produção (Fig. 7.2). Em ambos os casos existem duas formas de descarregar a cana: por tombamento da caçamba do caminhão ou através de um sistemas de correntes. Para transportar a cana do fosso para a produção utiliza-se um transportador (com garras) que não necessita de guindaste para carregar e descarregar a cana.

Fig. 7.2. Recepção da cana.

A cana retirada do caminhão é colocada nas duas mesas de alimentação (Fig. 7.3): a primeira recebe a cana proveniente do fosso e a segunda recebe cana diretamente dos caminhões de cana que chegam à usina. Em cada uma das mesas a cana é lavada através do acionamento de chuveiros.

Fig. 7.3. Recepção e lavagem da cana.

Com base nesta descrição, o refinamento da atividade [Recepção] é apresentado na Fig. 7.4.

Fig. 7.4. Refinamento de [Recepção]

Refinamento de [Preparo]

Um esquema do [Preparo] da cana é representado na Fig. 7.5. Para modelagem, a Esteira 1, que recebe a cana da [Recepção] está dividida em duas partes: Esteira 1A, antes do picador, e Esteira 1B, após o picador. Após o desfibrador, uma segunda esteira (Esteira 2) é responsável por levar a cana até o processo de difusão. A cana em excesso na entrada da difusão é devolvida para a saída do desfibrador por uma terceira esteira rolante (Esteira 3). O refinamento da atividade [Preparo] é apresentado na Fig. 7.6.

Fig. 7.5. Instalações para o preparo da cana.

Fig. 7.6. Refinamento de [Preparo]

Refinamento de [Extração]

Um esquema do processo de difusão é apresentado na Fig. 7.7. A camada de cana que atravessa o difusor é abundantemente regada com o líquido de extração do açúcar através de 14 difusores. Por baixo da camada, o fundo do difusor é formado por 14 recipientes justapostos, os quais recebem o caldo que atravessou a camada de cana (o estrado do transportador é formado por uma grade que deixa passar apenas o caldo).

Uma bomba coleta o caldo retido no recipiente e o envia ao distribuidor anterior, de modo que o caldo retrocede de recipiente em recipiente desde a extremidade de saída até a extremidade de entrada da cana no difusor. Neste processo, o bagaço que sai do difusor ainda está encharcado, assim ele passa ainda por uma moenda que tem como finalidade retirar o excesso de água de modo que o bagaço possa ser utilizado nas caldeiras para geração de energia. O caldo enviado à sulfitação corresponde a uma parcela do caldo coletado no primeiro recipiente. O restante do caldo do primeiro recipiente é despejado sobre a cana do transportador.

Fig. 7.7. Esquema de um difusor.

O refinamento da atividade [Extração] é apresentado na Fig. 7.8.

Fig. 7.8. Refinamento de [Extração]

Refinamento de [Sulfitação]

Um esquema da sulfitação é apresentado na Fig. 7.9. O caldo proveniente da difusão é armazenado em um tanque. O SO₂ utilizado na sulfitação é obtido através da combustão em um forno rotativo de enxofre em pó: $S + O_2 \rightarrow SO_2$. Um compressor é responsável pela produção do ar comprimido utilizado nesta combustão. Antes de ser introduzido no forno, o ar comprimido atravessa uma câmara onde entra em contato com cal virgem, cujo objetivo é secar o ar de combustão, evitando a formação de anidrido sulfúrico (SO₃). O SO₂ produzido na combustão atravessa uma serpentina de resfriamento, seguindo para a coluna de sulfitação, ou sulfitador, que contém em seu interior placas inclinadas. O caldo que está no tanque é introduzido pela parte superior do sulfitador e as placas reduzem a velocidade do caldo. Na parte inferior, os gases resultantes da combustão do enxofre são introduzidos em contra-corrente. O refinamento da atividade [Sulfitação] é apresentado na Fig. 7.10.

Fig. 7.11. Esquema da calagem.

Fig. 7.12. Refinamento de [Calagem]

Refinamento de [Aquecimento]

O aquecimento consiste em passar o caldo proveniente da calagem por uma série de 3 aquecedores. As instalações da Usina Cruz Alta possuem 3 séries de 4 aquecedores. Normalmente, pelo menos um aquecedor de cada série se encontra em manutenção. A inclusão/exclusão de um aquecedor na série é determinada pela posição de uma válvula de 2 entradas/2 saídas (V_{2E2S}). Um esquema das instalações é apresentado na Fig. 7.13. O refinamento da atividade [Calagem] é apresentado na Fig. 7.14.

Fig. 7.13. Séries de aquecedores.

Fig. 7.14. Refinamento de [Aquecimento]

Refinamento de [Clarificação]

A clarificação é ilustrada na Fig. 7.15. O caldo proveniente dos aquecedores é destinado a um tanque de armazenagem (T_{CL}), de onde é enviado aos 3 clarificadores da Usina Cruz Alta. Os clarificadores são decantadores na forma de tanques onde o caldo a ser decantado chega com um fluxo regular e contínuo. Os clarificadores são de dimensão suficientes para que a velocidade de escoamento e de circulação do caldo seja lenta o bastante para permitir a decantação e obtenção do caldo para evaporação. O lodo resultante da decantação é extraído por uma bomba e enviado aos filtros. O caldo resultante da filtragem do lodo é enviado de volta ao tanque T_{CL} , enquanto a torta extraída nos filtros é um sub-produto comercializável como adubo.

A Fig. 7.16 apresenta o refinamento da atividade [Clarificação]

Fig. 7.15. Esquema da Clarificação.

Fig. 7.16. Refinamento de [Clarificação]

Refinamento de [Evaporação]

O processo de evaporação ocorre em um evaporador múltiplo-efeito (Benne et al; 2000), onde a cada efeito aumenta-se gradualmente a concentração do caldo até a obtenção do xarope. Cada efeito envolve um ou mais corpos. Em cada corpo, caldo e vapor são introduzidos simultaneamente, o vapor então condensa cedendo energia ao caldo, que tem sua temperatura elevada e parte da água nele presente é evaporada, gerando vapor, que é utilizado no efeito seguinte. Uma parte do vapor gerado no 2º Efeito é utilizada no cozimento, enquanto o vapor residual dos demais efeitos pode ser utilizado em outros processos da usina. No caso da Usina Cruz Alta, o 1º efeito é composto de 3 corpos, o 2º efeito de 4 corpos, e o 3º, o 4º e o 5º efeitos de 1 corpo. Um esquema é apresentado na Fig. 7.17.

Fig. 7.17. Esquema da evaporação.

A Fig. 7.18 apresenta o refinamento da atividade [Evaporação]

Fig. 7.18. Refinamento de [Evaporação]

Refinamento de [Cozimento e Centrifugação]

Os cozedores (cristalizadores) são equipamentos semelhantes aos corpos do evaporador mas funcionam por bateladas (*batch*) de acordo com um determinado ciclo de operação. O produto resultante do cozimento é chamado de massa. Esta massa é destinada às centrifugas, que também são equipamentos que operam por bateladas, resultando na produção de magma ou açúcar, e mel.

Existem diversas configurações possíveis para a planta, envolvendo a produção de massas de diversas qualidades. No caso da Usina Cruz Alta são produzidos três tipos de massa diferentes: A, B e C (Fig. 7.19). Após a centrifugação a massa A resulta em açúcar e mel A, a massa B em magma B e mel B, e a massa C em magma C e mel C. A massa A é produzida a partir do xarope proveniente da evaporação e utiliza na semeadura o magma B (maiores informações sobre o processo de cozimento são fornecidas no Anexo B). A massa B é produzida a partir do mel A e utiliza como semente o magma C. A massa C é produzida a partir do mel B e utiliza

sementes adquiridas pela usina. O mel C é um sub-produto comercializável utilizado na produção de álcool.

Fig. 7.19. Configuração da planta de cristalização.

O refinamento da atividade [Cozimento e Centrifugação] é apresentado na Fig. 7.20.

Fig. 7.20. Refinamento de [Cozimento e Centrifugação]

No PFS da Fig. 7.20, cada atividade correspondente ao cozimento ou centrifugação de um tipo de massa e pode ser detalhado de forma a especificar o cozedor que está sendo utilizado. A Usina Cruz Alta possui 10 cozedores que podem ser utilizados para produzir massa A, B ou C. Como exemplo, a Fig. 7.21 apresenta o refinamento da atividade [Cozimento Massa A]

Fig. 7.21. Refinamento de [Cozimento Massa A]

Refinamento de [Secagem e Empacotamento]

O açúcar resultante da centrifugação é enviado a um reservatório de açúcar, de onde segue para o secador, transportado através de esteiras. Do secador o açúcar é enviado ao empacotamento, onde é armazenado em sacos. Um esquema é apresentado na Fig. 7.22. O refinamento da atividade [Secagem e Empacotamento] é apresentado na Fig. 7.23.

Fig. 7.22. Esquema da secagem e empacotamento.

Fig. 7.23. Refinamento de [Secagem e Empacotamento]

7.2.2. Exemplos de Classes e Objetos

Alguns dos objetos e classes correspondentes aos processos de recepção e preparo são:

Objeto de Controle

- C_7 – *Mesa* – Mesa 1, Mesa 2.
- C_{13} – *Esteira 1-Picador* – Esteira 1-Picador.

Sistema Supervisório

- C_{74} – *Interface Mesas* – Interface Mesas
- C_{75} – *Supervisor Fosso* – Supervisor Fosso
- C_{76} – *Supervisor Picador* – Supervisor Picador

A seguir apresenta-se os modelos em redes PTD-OO destas classes. Observa-se que a lista completa dos objetos e classes da Usina Cruz Alta, assim como o modelo em redes PTD-OO das demais classes encontram-se no Anexo B.

C_7 - *Mesa* (Fig. 7.24)

Esta classe modela as mesas que recebem a cana proveniente dos caminhões e do transportador.

A parte esquerda do modelo corresponde ao descarregamento da cana. O volume total de cana acumulado na *Mesa* é dado por V_M . Quando a *Mesa* é acionada, a vazão de cana é aproximadamente constante e é dado por ' $q_M * v_{VV.I3.C9}$ ', onde $v_{VV.I3.C9}$ é a velocidade imposta pelo respectivo *Variador de Velocidade* (C_9). Quando o volume total de cana acumulado na *Mesa* excede um determinado limite (K_{V_M}), tem-se uma situação de falha, pois o excesso de cana sobrecarrega o motor da esteira. Quando a mesa se esvazia (disparo de t_{9_7}), q_M torna-se nulo. O controle da *Mesa* atua sobre o respectivo *Chuveiro* (C_8), acionando-o (t_{7_7}) e desligando-o (t_{11_7}) de acordo com o seu estado.

Fig. 7.24. Modelo da classe C7 - Mesa.

A modelagem do transporte da cana na esteira é realizada considerando a aproximação apresentada em Beek; Rooda; Trienekens (1999) para atraso de tempo. Neste caso, quando ocorre um transporte contínuo, o valor de uma variável y , a uma distância L do início do transporte ($x=L$) é aproximado através da discretização de L em n intervalos. A constante de tempo τ depende da velocidade de transporte do material v : $\tau = L/v$. Calcula-se então o valor de y nos n pontos resultantes ($x=L/n$, $x=2L/n$, etc) através das expressões abaixo, onde $y_0 = y(x=0)$ e $y_n = y(x=L)$

$$\begin{cases} \dot{y}_1 = -n/\tau * (y_1 - y_0) \\ \dot{y}_n = -n/\tau * (y_n - y_{n-1}) \\ \text{para } i=2 \text{ até } n-1: \dot{y}_i = -n/(6*\tau) * (2*y_{i+1} + 3*y_i - 6*y_{i-1} + y_{i-2}) \end{cases}$$

A partir desta aproximação é definida a classe C_{11} – Esteira Bipartida. A classe C_{12} – Preparador modela ambos o picador e o desfibrador. A classe C_{13} – Esteira 1 – Picador é resultado da composição de uma C_{11} e uma C_{12} .

C_{13} - Esteira 1- Picador (Fig. 7.25)

A Esteira Bipartida pode assumir três estados discretos: ‘On’ ($p_{1.13}$), ‘Off’ ($p_{3.13}$) e ‘Falha’ ($p_{2.13}$). A ‘Falha’ ocorre quando a esteira está desligada e recebe cana. A vazão de cana em peso (m_{E1A}) na saída da parte 1A da Esteira 1 (entrada do Preparador) é função da vazão na entrada da esteira sobre a qual tem-se um atraso (τ_{E1A}) que corresponde ao tempo que a cana leva para ir da entrada da esteira até o Preparador. Este atraso é inversamente proporcional a velocidade da Esteira

Bipartida ($v_{VV.I3.C9}$). A modelagem da parte 1B da esteira é semelhante a modelagem da parte 1A. Considera-se que a densidade do feixe de cana sobre a esteira é constante (K_{p_E1}).

A vazão na saída do *Preparador* (m_P) é igual a vazão de entrada quando esta é inferior a um determinado limite K_{m_P1} , correspondente ao limite de processamento do *Preparador*. Se a vazão na entrada ($m_{E1B.I2.C13}$) for superior a este limite, acumula-se cana na entrada do *Preparador*. O peso de cana acumulado é dado por M_P . Este volume de cana deve ser processado tão logo a quantidade de cana que chega ao *Preparador* seja inferior a K_{m_P1} . Entretanto, se M_P ultrapassa um determinado limite K_{M_P} , tem-se uma situação de falha no *Preparador* devido ao sobre carregamento. Quando o *Preparador* está ‘Desligado’, a vazão em massa na saída é igual a vazão na entrada. Se houver cana acumulada na entrada do picador, esta é consumida de acordo com a constante K_{m_P2} . Em função do estado ‘Ligado’ ou ‘Desligado’ do picador o coeficiente de preparo do picador (C_P) assume os valores ‘ K_{C_P} ’ ou ‘0’.

Fig. 7.25. Modelo da classe C₁₃ - Esteira 1 - Picador.

C₇₄ – Interface Mesas (Fig. 7.26)

Esta classe é responsável por fazer a interface com as mesas (C₇), decidindo qual dentre elas deve fornecer cana para a produção (Mesa 1 ou Mesa 2) e onde deve ser feito o descarregamento (Mesa 1 ou Fosso) dos caminhões de cana que chegam a usina. Ela é também responsável por estimar o volume de cana em cada mesa (V_{M1} e V_{M2}) de acordo com o volume de produção da usina, e solicitar a transferência de cana do Fosso para a Mesa 1 quando necessário (t_{11_74}).

Fig. 7.26. Modelo da classe C₇₄ - Interface Mesas.

7.2.2.1. C_{76} - Interface Picador (Fig. 7.27)

Esta classe faz a interface com o Picador, iniciando (t_{1_76}) e suspendendo (t_{14_76}) o preparo da cana quando solicitado. Quando é detectada sobrecarga neste equipamento, suspende-se (t_{12_76}) o fornecimento de cana até que não haja mais cana acumulada na entrada do equipamento ($M_{P.I1.C13} \leq 0$).

Fig. 7.27. Modelo da classe C_{76} - Interface Picador.

Apresenta-se a seguir o estado inicial destes objetos:

- $O_{1.7} = \underline{\text{Mesa 1}}; X_{1.7} = \{V_M = ind, V_{CM} = 0, K_{q_M} = 1, K_{V_M} = ind, I_1 = ind, I_2 = \underline{\text{Chuveiro 1}}, I_3 = \underline{\text{VV Mesa 1}}, q_M = 0\}; m_{1.7} = \{p_{2_7}, p_{4_7}\};$
- $O_{2.7} = \underline{\text{Mesa 2}}; X_{2.7} = \{V_M = ind, V_{CM} = 0, K_{q_M} = 1, K_{V_M} = ind, I_1 = ind, I_2 = \underline{\text{Chuveiro 2}}, I_3 = \underline{\text{VV Mesa 2}}, q_M = 0\}; m_{2.7} = \{p_{2_7}, p_{4_7}\};$
- $O_{1.13} = \underline{\text{Esteira 1 - Picador}}; X_{1.13} = \{m_{E1B} = 0, m_{E1A} = 0, \tau_{E1A} = 0, \tau_{E1B} = 0, K_{\tau_E1A} = 1, K_{\tau_E1B} = 1, x_{0A} = 0, x_{1A} = 0, x_{2A} = 0, x_{3A} = 0, x_{4A} = 0, x_{0B} = 0, x_{1B} = 0, x_{2B} = 0, x_{3B} = 0, x_{4B} = 0, K_{_E1} = ind, I_1 = \underline{\text{VV Esteira 1}}, I_2 = \underline{\text{Mesa 1}}, I_3 = \underline{\text{Mesa 2}}, V_{CM} = 0, m_P = 0, C_P = 0, M_P = 0, K_{m_P1} = 1, K_{m_P2} = ind, K_{M_P} = 15\}; m_{1.13} = \{p_{1_13}, p_{4_13}\};$
- $O_{1.74} = \underline{\text{Interface Mesas}}; X_{1.74} = \{V_{M1} = ind, V_{M2} = ind, K_V = ind, V_C = 0, q = 0, I_1 = \underline{\text{Mesa 1}}, I_2 = \underline{\text{Mesa 2}}, I_3 = \underline{\text{Supervisor Fosso}}\}; m_{1.74} = \{p_{1_74}, p_{8_74}, p_{9_74}\};$
- $O_{1.76} = \underline{\text{Interface Picador}}; X_{1.76} = \{K_M = 10, I_1 = \underline{\text{Esteira 1 - Picador}}, I_2 = \underline{\text{Desfibrador}}, I_3 = \underline{\text{Interface Mesas}}\}; m_{1.76} = \{p_{1_76}\};$

7.3. Análise dos Modelos em redes PTD-OO

Detalha-se a seguir a verificação de propriedade de segurança envolvendo aspectos relacionados à dinâmica contínua dos objetos. Um exemplo de verificação de propriedade de alcançabilidade é apresentado no Anexo B.

No que se refere as buscas de cenários para análise da parte discreta, uma vez que a construção das árvores dos seqüentes já foi ilustrada nos Capítulos 4, 5 e 6, estas são omitidas neste capítulo. Nas **Etapas 4.1** e **5.1** apresenta-se apenas os seqüentes referente às buscas e os resultados obtidos pela construção das respectivas árvores.

7.3.1. Propriedade 1

7.3.1.1. *Etapas 1 - Definição do enunciado da propriedade*

O enunciado da **Propriedade 1** é definido de acordo com o tipo de enunciado PS1 definido para propriedades de segurança (apresentado no Capítulo 4, Seção 4.3.4.1):

- **Propriedade 1** - O objeto Esteira 1- Picador ($O_{1,13}$) não atinge o estado de falha (evento e_f), referente à sobrecarga no picador: o estado $p_{7_13.01} = 1$ nunca é alcançado.

7.3.1.2. *Etapas 2 - Definição do conjunto de restrições da propriedade*

É imposta a seguinte restrição para a **Propriedade 1**:

- Restrição 1A (correspondente a R5, p.113) – O Gerenciador da Produção de Caldo permanece ligado quando o Picador está no estado c/ excesso: $p_{20_77} = 1$ se $p_{6_13} = 1$.

7.3.1.3. *Etapas 3 – Construção dos Diagramas de Colaboração Estáticos*

As interações entre os objetos relevantes para esta propriedade são apresentadas na Fig. 7.28.

A verificação desta propriedade inicia-se pelo objeto Esteira 1 + Picador, cujo estado é proibido.

Resumidamente, para provar esta propriedade, verifica-se que a cana acumulada na entrada do Picador nunca é suficiente para causar falha (a transição $t_{9_13.O1}$ nunca está habilitada). O objeto responsável por monitorar o Picador e executar a ação de controle necessária para evitar a falha é o Interface Picador ($O_{1.76}$). Esta ação de controle é tomada quando a cana acumulada no Picador atinge um determinado valor (K_M). Neste caso é enviada ao objeto Interfaces Mesas uma solicitação para suspender o fornecimento de cana, isto é, desligar Mesa 1 ou Mesa 2, até que o Picador tenha consumido toda a cana acumulada na sua entrada ($M_P = 0$).

Fig. 7.28. Diagrama de Colaboração das interações relevantes p/ a **Propriedade 1**.

7.3.1.4. *Etapa 4.1 – Parte Discreta – Busca de Cenários ($O_{1.13}$ - Esteira 1 + Picador)*

Para determinar os cenários que resultam em $p_{7_13.O1}$ (Fig. 7.25), o seguinte seqüente é analisado, resultando em infinitos cenários:

- *Busca 1* (até o estado proibido $p_{7_13.O1}$): $\Gamma_0, ! t_{13.O1}, \dots, ! t_{13.O1} \mid \text{--- } p_{13.O1} \otimes \Gamma_f$
- *Definição dos cenários proibidos* – Se retrocedermos na ocorrência de eventos até que o Picador tenha sido ativado, a construção da árvore resulta em infinitos cenários que variam entre si pelo número de disparo das transições $t_{8_13.O1}$ e $t_{7_13.O1}$, correspondente ao número de vezes que o Picador esteve no estado ‘c/ excesso’ de cana. A seqüência de disparos para cada cenário é apresentada a seguir, onde i pode variar de 0 a ∞ , e onde $\Gamma_0 = p_{4_13.O1} \wp p_{8_13.O1}$ e $\Gamma_f = p_{8_13.O1}$:
 - **Cenário i :** $t_{9_13.O1}; t_{7_13.O1}^{(i+1)}; i^*(t_{8_13.O1}^0; t_{7_13.O1}^0); t_{2_76.O1/4_13.O1}$.
- *Condições para Propriedade 1* – Para provar que a **Propriedade 1** é verdadeira, verifica-se que a transição $t_{9_13.O1}$ (Fig. 7.25) nunca é disparada. Para tanto a

condição definida por $e_{9_13.O1}$ ($M_P \geq K_{M_P}$) nunca deve ser satisfeita. Esta situação corresponde ao Caso 1, descrito na Seção 4.3.4.5 (Fig. 4.24 do Capítulo 4).

7.3.1.5. Etapa 4.2 – Elaboração de Hipóteses ($O_{1.13}$ - Esteira 1 + Picador)

Nenhuma hipótese é elaborada.

7.3.1.6. Etapa 4.3 – Parte Contínua – Evolução de variáveis contínuas e datas de disparos ($O_{1.13}$ - Esteira 1 + Picador)

A partir da análise das funções de habilitação, junção e dos sistemas de equações, conclui-se que:

• **Cenários i:**

- Em $\theta_{2_76.O1/4_13.O1}$ e em $\theta_{8_13.O1}$, $M_P = 0$, portanto, em $\theta_{7_13.O1}^{i+1}$, $M_P = 0$.
- Em $\theta_{9_13.O1}$ $M_P = K_{M_P}$, portanto $\theta_{9_13.O1} > \theta_{7_13.O1}^{i+1}$.
- No estado $p_{6_13.O1}=1$ (entre $\theta_{7_13.O1}^{i+1}$ e $\theta_{9_13.O1}$), $m_P = K_{m_P1}$.
- Quando o Picador está no estado $p_{6_13.O1}$, o valor da cana acumulada na entrada do Picador (M_P) é dado por F_{6_13} , portanto:

$$M_P(\theta_{9_13.O1}) = \int_{\theta_{7_13.O1}^{i+1}}^{\theta_{9_13.O1}} (m_{1EA} - m_P) \cdot d\theta \geq K_{M_P}$$

- m_{1EA} e m_P podem ser calculados por:

$$m_P = K_{m_P1}$$

$$m_{1EA} = x_{4A} = -\dot{x}_{4A} \cdot \tau_{E1A}/4 + x_{3A}$$

$$x_{3A} = -\dot{x}_{3A} \cdot \tau_{E1A}/2 + (-2 \cdot x_{4A} + 6 \cdot x_{2A} + x_{1A})/3$$

$$x_{1A} = -\dot{x}_{1A} \cdot \tau_{E1A}/4 + x_{0A}$$

$$x_{2A} = -\dot{x}_{2A} \cdot \tau_{E1A}/2 + (-2 \cdot x_{3A} + 6 \cdot x_{1A} + x_{0A})/3$$

$$x_{0A} = (q_{M.O1.C7} + q_{M.O2.C7}) \cdot K_{p_E1}$$

- Resolvendo o sistema acima, temos a seguinte expressão para m_{1EA} :

$$m_{1EA} = \tau_{E1A}/36 \cdot (-7 \cdot \dot{x}_{4A} - 6 \cdot \dot{x}_{3A} - 12 \cdot \dot{x}_{2A} - 13 \cdot \dot{x}_{1A}) + 15 \cdot (q_{M.O1.C7} + q_{M.O2.C7}) \cdot K_{p_E1}$$

- Dividindo o intervalo $[\theta_{7_13.O1}^{i+1}, \theta_{9_13.O1}]$ em $[\theta_{7_13.O1}^{i+1}, \theta_C]$ e $[\theta_C, \theta_{9_13.O1}]$, onde θ_C é o instante em que a ação de controle para evitar falhas é iniciada, tem-se que:

$$M_P(\theta_{9_13.O1}) = M_P(\theta_C) + \int_{\theta_{7_13.O1}^{i+1}}^{\theta_{9_13.O1}} (m_{1EA} - m_P) \cdot d\theta = M_P(\theta_C) - K_{m_P1} * (\theta_{9_13.O1} - \theta_C) + \tau_{E1A}/36 * (7 * (x_{4A}(\theta_C) - x_{4A}(\theta_{9_13.O1})) + 6 * (x_{3A}(\theta_C) - x_{3A}(\theta_{9_13.O1})) + 12 * (x_{2A}(\theta_C) - x_{2A}(\theta_{9_13.O1})) + 13 * (x_{1A}(\theta_C) - x_{1A}(\theta_{9_13.O1})) + 15 * K_{p_E1} * \int_{\theta_C}^{\theta_{9_13.O1}} (q_{M.O1.C7} + q_{M.O2.C7})$$

- Considerando o pior caso, isto é, onde $x_{0A}(\theta_C) = \max(q_{M.O1.C7} + q_{M.O2.C7})$ e onde $x_{0A}(\theta_{9_13.O1}) = \min(q_{M.O1.C7} + q_{M.O2.C7}) = 0$, a condição para $p_{7_13.O1}$ ser atingido é dada por:

$$M_P(\theta_{9_13.O1}) \leq M_P(\theta_C) - K_{m_P1} * (\theta_{9_13.O1} - \theta_C) + \tau_{E1A}/36 * 38 * \max(q_{M.O1.C7} + q_{M.O2.C7}) + 15 * K_{p_E1} * \int_{\theta_C}^{\theta_{9_13.O1}} (q_{M.O1.C7} + q_{M.O2.C7}) \geq K_{M_P}$$

Para verificar a expressão acima, os objetos Mesa 1 ($O_{1.7}$) e Mesa 2 ($O_{2.7}$) devem ser analisados. Além do compartilhamento das variáveis $q_{M.O1.C7}$ e $q_{M.O2.C7}$, estes objetos interagem com o objeto Esteira 1 – Picador através dos objetos Interface Mesas e Interface Picador ($O_{1.76}$). Uma vez que a ação de controle para evitar a falha é tomada pelo objeto Interface Picador ($O_{1.76}$), inicia-se a análise por este objeto.

7.3.1.7. *Etapa 5.1 – Parte Discreta – Busca de Cenários ($O_{1.76}$ - Interface Picador)*

Apresenta-se a seguir o detalhamento dos cenários relativos a **Propriedade 1**.

- **Cenários i:** A princípio qualquer estado atingível por este objeto (Fig. 7.27) é um possível estado no instante de disparo de $t_{9_13.O1}$. Estes estados são: $\{p_{1_76.O1}\}$; $\{p_{2_76.O1}, p_{5_76.O1}\}$; $\{p_{3_76.O1}, p_{5_76.O1}\}$; $\{p_{4_76.O1}, p_{5_76.O1}\}$; $\{p_{2_76.O1}, p_{6_76.O1}\}$; $\{p_{3_76.O1}, p_{6_76.O1}\}$; $\{p_{4_76.O1}, p_{6_76.O1}\}$. Para cada estado deve-se então fazer a busca dos possíveis cenários que, a partir do disparo de $t_{2_76.O1/4_13.O1}$ resultam neste estado, verificando em seguida eventuais restrições impostas pela parte contínua. Resumem-se a seguir os resultados obtidos:
 - **Estado final $\{p_{1_76.O1}\}$:** não existe sequência possível de disparo que a partir do disparo de $t_{2_76.O1/4_13.O1}$ resulte em $p_{1_76.O1}$ sem disparar outras transições da interface entre $O_{1.13}$ e $O_{1.76}$.
 - **Estado final $\{p_{2_76.O1}, p_{5_76.O1}\}$:** não existe sequência possível de disparo.

- **Estado final $\{p_{2_76.O1}, p_{6_76.O1}\}$:** não existe sequência possível de disparo.
- **Estado final $\{p_{3_76.O1}, p_{5_76.O1}\}$:**
 - *Busca 1* (após o disparo de $t_{2_76.O1/4_13.O1}$): $\Gamma_0, !\downarrow_{76.O1}, !\downarrow_{76.O1}, !\downarrow_{76.O1}, !\downarrow_{76.O1}, t_{2_76.O1} \mid \text{---} p_{2_76.O1}, p_{5_76.O1}$.
 - *Busca 2* (até o disparo de $t_{2_76.O1/4_13.O1}$): esta busca é considerada irrelevante para a verificação da propriedade.
 - *Definição de cenários:* são encontrados infinitos cenários que variam entre si pelo número de disparos de ' $t_{6_76.O1/2_74.O1}, t_{5_76.O1/4_74.O1}$ '. A sequência de disparos destes cenários é apresentada a seguir, onde i e j podem variar de 0 a ∞ :
 - **Cenário i-1-j:** $j^*(t_{6_76.O1/2_74.O1}^0; t_{5_76.O1/4_74.O1}^0); t_{2_76.O1/4_13.O1}$.
- **Estado final $\{p_{3_76.O1}, p_{6_76.O1}\}$:** semelhantemente ao caso do estado final $\{p_{3_76.O1}, p_{5_76.O1}\}$ são encontrados infinitos cenários que variam entre si pelo número de disparos de ' $t_{6_76.O1/2_74.O1}, t_{5_76.O1/4_74.O1}$ '. A sequência de disparos destes cenários é apresentada a seguir, onde i e j podem variar de 0 a ∞ :
 - **Cenário i-2-j:** $t_{18_77.O1/7_76.O1} // (j^*(t_{6_76.O1/2_74.O1}^0; t_{5_76.O1/4_74.O1}^0); t_{2_76.O1/4_13.O1})$.
- **Estado final $\{p_{4_76.O1}, p_{5_76.O1}\}$:** semelhantemente ao caso do estado final $\{p_{3_76.O1}, p_{5_76.O1}\}$ são encontrados infinitos cenários que variam entre si pelo número de disparos de ' $t_{6_76.O1/2_74.O1}, t_{5_76.O1/4_74.O1}$ '. A sequência de disparos destes cenários é apresentada a seguir, onde i e j podem variar de 0 a ∞ :
 - **Cenário i-3-j:** $t_{5_76.O1/4_74.O1}; j^*(t_{6_76.O1/2_74.O1}^0; t_{5_76.O1/4_74.O1}^0); t_{2_76.O1/4_13.O1}$.
- **Estado final $\{p_{4_76.O1}, p_{6_76.O1}\}$:** são encontrados infinitos cenários que variam entre si pelo número de disparo de ' $t_{6_76.O1/2_74.O1}, t_{5_76.O1/4_74.O1}$ '. A sequência de disparos destes cenários é apresentada a seguir, onde i e j podem variar de 0 a ∞ :
 - **Cenário i-4-j:** $t_{18_77.O1/7_76.O1} // (t_{5_76.O1/4_74.O1}; j^*(t_{6_76.O1/2_74.O1}^0; t_{5_76.O1/4_74.O1}^0); t_{2_76.O1/4_13.O1})$.

7.3.1.8. *Etapa 5.2 – Elaboração de Hipóteses ($O_{1.76}$ - Interface Picador)*

São elaboradas a seguinte hipótese, que corresponde ao tipo de hipótese H1 (apresentado no Capítulo 4, Seção 4.3.3.6, p.113):

- Hipótese 1A – O Picador (Fig. 7.25) responde imediatamente a qualquer chamada de método emitida pelo objeto Interface Picador (Fig. 7.27): as transições $t_{2_76.O1/4_13.O1}$, $t_{3_76.O1/10_13.O1}$ e $t_{4_76.O1/10_13.O1}$ disparam em $\Delta\theta=0$ após suas habilitações em $O_{1.76}$.
- Hipótese 1B – O objeto Interface Mesas (Fig. 7.26) responde imediatamente a qualquer chamada de método emitida pelo objeto Interface Picador (Fig. 7.27): as transições $t_{5_76.O1/4_74.O1}$ e $t_{6_76.O1/2_74.O1}$ disparam em $\Delta\theta=0$ após suas habilitações em $O_{1.76}$.

7.3.1.9. Etapa 5.3 – Parte Contínua – Evolução de variáveis contínuas e datas de disparos ($O_{1.76}$ - Interface Picador)

A consideração das hipóteses apresentadas e a análise da parte contínua resulta então nas seguintes conclusões:

- Os **Cenários i-1-j** e **i-2-j** são impossíveis porque, de acordo com a Hipótese 1B, $t_{5_76.O1/4_74.O1}$ está habilitada e dispara em $\theta_{7_13.O1}^{i+1} < \theta_{5_76.O1/4_74.O1} < \theta_{9_13.O1}$, consumindo a marca em p_{3_76} .
- Para os **Cenários i-4-j**, $\theta_{18_77.O1/7_76.O1} = \theta_{9_13.O1}$, pois caso contrário $t_{3_76.O1/10_13.O1}$ ou $t_{4_76.O1/10_13.O1}$ teria sido disparada.
- Considerando o compartilhamento da variável M_P , tem-se que, para os **Cenários i-3-j** e **i-4-j**:
 - $\theta_{7_13.O1}^{i+1} < \theta_{5_76.O1/4_74.O1} < \theta_{9_13.O1}$, onde o disparo de $t_{5_76.O1/4_74.O1}$ é a ação de controle considerada na análise do objeto Esteira 1 – Picador (Fig. 7.25).
 - $M_P(\theta_C) = M_P(\theta_{5_76.O1/4_74.O1}) = K_M$.
 - A condição a ser satisfeita para que $p_{7_13.O1}$ possa ser atingido é então:

$$K_M - K_{m_P1} * (\theta_{9_13.O1} - \theta_{5_76.O1/4_74.O1}) + \tau_{E1A}/36 * 38 * \max(q_{M.O1.C7} + q_{M.O2.C7}) + 15 * K_{p_E1} * \int_{\theta_{5_76.O1/4_74.O1}}^{\theta_{9_13.O1}} (q_{M.O1.C7} + q_{M.O2.C7}) \geq K_{M_P}$$

7.3.1.10. Etapa 5.1 – Parte Discreta – Busca de Cenários ($O_{1.74}$ - Interface Mesas)

• **Cenários i-3-j e i-4-j:**

A busca dos cenários deste objeto é semelhante para os **Cenários i-3-j** e **i-4-j**. Como no caso do objeto Interface Picador (Fig. 7.27), a princípio qualquer estado

atingível por este objeto é um possível estado no instante de disparo de $t_{9_13.O1}$. Estes estados são (Fig. 7.26): $\{p_{1_74.O1}\}$, $\{p_{3_74.O1}, p_{4_74.O1}\}$, $\{p_{4_74.O1}, p_{5_74.O1}\}$, $\{p_{4_74.O1}, p_{6_74.O1}\}$, $\{p_{4_74.O1}, p_{7_74.O1}\}$, $\{p_{2_74.O1}, p_{3_74.O1}\}$, $\{p_{2_74.O1}, p_{5_74.O1}\}$, $\{p_{2_74.O1}, p_{6_74.O1}\}$, $\{p_{2_74.O1}, p_{7_74.O1}\}$.

Como exemplo, considera-se a busca dos cenários que conduzem a $\{p_{1_74.O1}\}$, a partir do disparo de $t_{5_76.O1/4_74.O1}$. Do ponto de vista discreto, existem infinitos cenários, pois antes que $p_{1_74.O1}$ seja atingido pelo disparo de $t_{3_74.O1}$, $t_{5_74.O1/12_7.O1}$ ou $t_{10_74.O1/12_7.O2}$, $O_{1.74}$ pode alternar indefinidamente entre $\{p_{3_74.O1}, p_{4_74.O1}\}$, $\{p_{4_74.O1}, p_{5_74.O1}\}$, $\{p_{4_74.O1}, p_{6_74.O1}\}$ e $\{p_{4_74.O1}, p_{7_74.O1}\}$. Alguns exemplos são apresentados abaixo:

- **Cenário i-3 ou 4-j-1:** $t_{3_74.O1}, t_{12_76.O1/4_74.O1}$
- **Cenário i-3 ou 4-j-2:** $t_{5_74.O1/12_7.O1}, t_{12_76.O1/4_74.O1}$
- **Cenário i-3 ou 4-j-3:** $t_{10_74.O1/12_7.O2}, t_{12_76.O1/4_74.O1}$
- **Cenário i-3 ou 4-j-4:** $t_{3_74.O1}, t_{7_74.O1/12_7.O1}, t_{12_76.O1/4_74.O1}$
- **Cenário i-3 ou 4-j-5:** $t_{3_74.O1}, t_{9_74.O1/12_7.O2}, t_{12_76.O1/4_74.O1}$
- **Cenário i-3 ou 4-j-6:** $t_{5_74.O1/12_7.O1}, t_{6_74.O1/5_7.O2}, t_{12_76.O1/4_74.O1}$
- **Cenário i-3 ou 4-j-7:** $t_{10_74.O1/12_7.O2}, t_{8_74.O1/5_7.O2}, t_{12_76.O1/4_74.O1}$

7.3.1.11. *Etapa 5.2 – Elaboração de Hipóteses ($O_{1.74}$ - Interface Mesas)*

São feitas as seguintes hipóteses sobre a interface deste objeto:

- Hipótese 1C (correspondente a H1, p.113) – Mesa 1 (Fig. 7.24) responde imediatamente a qualquer chamada de método emitida pelo objeto Interface Mesas (Fig. 7.26): as transições $t_{5_74.O1/12_7.O1}$, $t_{6_74.O1/5_7.O1}$ e $t_{7_74.O1/12_7.O1}$ disparam em $\Delta\theta=0$ após suas habilitações em $O_{1.74}$.
- Hipótese 1D (correspondente a H1, p.113) – Mesa 2 (Fig. 7.24) responde imediatamente a qualquer chamada de método emitida pelo objeto Interface Mesas (Fig. 7.26): as transições $t_{9_74.O1/12_7.O1}$, $t_{8_74.O1/5_7.O2}$ e $t_{10_74.O1/12_7.O1}$ disparam em $\Delta\theta=0$ após suas habilitações em $O_{1.74}$.
- Hipótese 1E (correspondente a H1, p.113) – Supervisor Fosso responde imediatamente a qualquer chamada de método emitida pelo objeto Interface Mesas: as transições $t_{11_74.O1/1_75.O1}$, $t_{6_75.O1/12_74.O1}$ e $t_{3_75.O1/13_74.O1}$ disparam em $\Delta\theta=0$ após suas habilitações em $O_{1.74}$.

7.3.1.12. Etapa 5.3 – Parte Contínua – Evolução de variáveis contínuas e datas de disparos ($O_{1.74}$ - Interface Mesas)

A consideração das hipóteses apresentadas e a análise da parte contínua resulta que o único estado possível quando $t_{9_13.O1}$ (Fig. 7.25) dispara é o estado $\{p_{1_74.O1}\}$ (Fig. 7.26). As seguintes conclusões são obtidas:

- Os cenários onde o estado em θ_{9_13} inclui $p_{2_74.O1}=1$ são impossíveis porque não podem ser atingidos a partir do disparo de $t_{5_76.O1/4_74.O1}$ a menos que $t_{6_76/2_74.O1}$ ou $t_{16_77.O1/2_74.O1}$ disparem. No entanto $t_{6_76/2_74.O1}$ não faz parte dos cenários definidos e, de acordo com a Restrição 1A (p.224), $t_{13_77.O1/2_74.O1}$ não dispara em $O_{1.77}$.
- Os cenários onde o estado em θ_{9_13} inclui $p_{4_74.O1}=1$ são impossíveis porque $t_{3_74.O1}$, $t_{5_74.O1/12_7.O1}$ ou $t_{10_74.O1/12_7.O2}$ está habilitada e dispara em $\theta_{5_76.O1/4_74.O1}$, consumindo $p_{4_74.O1}$.
- Para os cenários terminados com o disparo de $t_{3_74.O1}$, $\theta_{3_74.O1} = \theta_{5_76.O1/4_74.O1}$.
- Para os cenários terminados com o disparo de $t_{5_74.O1/12_7.O1}$, $\theta_{5_74.O1/12_7.O1} = \theta_{5_76.O1/4_74.O1}$.
- Para os cenários terminados com o disparo de $t_{5_74.O1/12_7.O1}$, $\theta_{10_74.O1/12_7.O2} = \theta_{5_76.O1/4_74.O1}$.

7.3.1.13. Etapa 5.1 – Parte Discreta – Busca de Cenários ($O_{1.7}$ - Mesa 1 e $O_{2.7}$ - Mesa 2)

Estes objetos influenciam a verificação da **Propriedade 1** apenas no que se refere aos valores de $q_{M.O1.C7}$ e $q_{M.O2.C7}$, o que é limitado pelo estado discreto dos respectivos objetos.

Como simplificação, no lugar de determinar todos os possíveis cenários (que são infinitos), considera-se que no intervalo $[\theta_{7_13.O1i+1}, \theta_{9_13.O1}]$ as mesas podem estar em qualquer estado e no intervalo $[\theta_{5_76.O1/4_74.O1}, \theta_{9_13.O1}]$ seu estado é limitado pela Hipótese 1F, apresentada a seguir.

7.3.1.14. Etapa 5.2 – Elaboração de Hipóteses ($O_{1.7}$ - Mesa 1 e $O_{2.7}$ - Mesa 2)

São feitas as seguintes hipóteses:

- Hipótese 1F (correspondente a H5, p.113) – Após o disparo de $t_{3_74.O1}$, $t_{5_74.O1/12_7.O1}$ ou $t_{10_74.O1/12_7.O2}$ o estado Mesa 1 ‘desligada’ ($p_{4_7.O1}=1$) e Mesa 2 ‘desligada’ ($p_{4_7.O2}=1$) são atingidos em $\Delta\theta=0$ se as transições $t_{6_76/2_74.O1}$ e $t_{16_77.O1/2_74.O1}$ não disparam.
- Hipótese 1G (correspondente a H8, p.113) – $v_{VV.O1.C9} \in [1; 2]$ $v_{VV.O2.C9} \in [1; 2]$.
- Hipótese 1H (correspondente a H8, p.113) – $v_{VV.O3.C9} \in [0,5; 1]$.

7.3.1.15. Etapa 5.3 – Parte Contínua – Evolução de variáveis contínuas e datas de disparos ($O_{1.7}$ – Mesa 1 e $O_{2.7}$ – Mesa 2)

De acordo com as hipóteses realizadas tem-se que:

- $q_{M.O1.C7}(\theta \geq \theta_{5_76.O1/4_74.O1}) = 0$ e $q_{M.O1.C7}(\theta < \theta_{5_76.O1/4_74.O1}) \leq K_{q_M} * \max(v_{VV.O1.C9}) = 2$
- $q_{M.O2.C7}(\theta \geq \theta_{5_76.O1/4_74.O1}) = 0$ e $q_{M.O2.C7}(\theta < \theta_{5_76.O1/4_74.O1}) \leq K_{q_M} * \max(v_{VV.O2.C9}) = 2$
- Como resultado:

$$K_M - K_{m_P1} * (\theta_{9_13.O1} - \theta_{5_76.O1/4_74.O1}) + 4,2 * \max(\tau_{E1A}) < K_M + 4,2 * \max(v_{VV.O3.C9}) = 14,2 < K_{M_P} = 15$$
- Portanto a **Propriedade 1** é verdadeira com base nas hipóteses realizadas.

7.3.1.16. Etapa 7 – Verificação das Hipóteses

Resumidamente, as hipóteses podem ser verificadas através da fusão dos objetos envolvidos:

- Hipótese 1A (p.229) é verificada através da fusão dos objetos Picador e Interface Picador.
- Hipótese 1B (p.229) é verificada através da fusão dos objetos Interface Mesas e Interface Picador.
- Hipótese 1C (p.230) é verificada através da fusão dos objetos Interface Mesas e Mesa 1.
- Hipótese 1D (p.230) é verificada através da fusão dos objetos Interface Mesas e Mesa 2.
- Hipótese 1E (p.230) é verificada através da fusão dos objetos Interface Mesas e Supervisor Fosso.
- Hipótese 1F (p.232) é verificada através da fusão dos objetos Interface Mesas, Mesa 1 e Mesa 2.

- Hipótese 1G (p.232) é verificada através da análise dos objetos VV Mesa 1 e VV Mesa 2.
- Hipótese 1H (p.232) é verificada através da análise do objeto VV Esteira 1.

7.4. Observações

Entre os três estudos de caso apresentados nesta tese, este é sem dúvida aquele de maior porte e com maior diversidade de processos, o que resulta em modelos com diferentes características, incluindo classes puramente contínuas ou discretas e classes híbridas. Entre alguns objetos existe grande interação, incluindo compartilhamento de variáveis contínuas e muitas chamadas de métodos em um breve intervalo de tempo. Outros objetos, no entanto, estão relativamente isolados, e, neste caso, a comunicação se restringe a eventuais chamadas de métodos.

Esta grande variedade de situações permite uma melhor avaliação dos métodos e procedimentos propostos para modelagem e análise de Sistemas Supervisórios Híbridos. Em relação à modelagem, a principal conclusão obtida é de que a introdução dos conceitos de orientação a objetos às redes PTD é essencial para viabilizar a construção racional e sistemática do modelo. Sem a adoção de uma abordagem modular, onde o comportamento de cada componente do sistema é considerado separadamente dos demais, a complexidade da modelagem seria intratável. No entanto, de acordo com a abordagem proposta, o problema de modelagem se reduziu a uma série de problemas de menor complexidade (como modelar um tanque, um cozedor, etc.). Quanto à construção do PFS, este propicia uma visão geral dos processos e do fluxo de material entre eles, o que é usado para definição de objetos através da relação de composição, em especial quando existe ciclo fechado de compartilhamento de variáveis. Finalmente, os diversos Diagramas da UML propiciam uma visualização voltada aos Casos de Uso, enfocando diferentes aspectos em cada diagrama, o que facilita a definição e modelagem dos objetos do Sistema Supervisório.

No que se refere à análise, a verificação de algumas propriedades salienta a importância para sistemas complexos da definição de hipóteses adequadas, o que significa que o sucesso da verificação de uma propriedade depende em maior grau do conhecimento de quem está realizando a análise e da sua capacidade de introduzir

hipóteses que simplifiquem a análise. Isto ocorre principalmente para propriedades de segurança, onde não existe um evento inicial (e_0) e final (e_f) que delimitam o intervalo de tempo a ser considerado. O número de cenários a serem analisados pode se tornar demasiadamente grande de acordo com as escolhas realizadas. No caso da **Propriedade 1**, por exemplo, é particularmente útil a suposição, durante a análise do objeto Esteira 1+Picador, de que existe uma ação de controle que evita o transbordamento do tanque, e que os comportamentos do sistema antes e após esta ação devem ser considerados separadamente (decomposição da integral de $\theta_{7_13.O1}$ a $\theta_{9_13.O1}$ em duas integrais de $\theta_{7_13.O1}$ a θ_C e de θ_C a $\theta_{9_13.O1}$). Outro exemplo é a Hipótese 1F, sem a qual os o número de cenário a serem analisados para o comportamento da Mesa 1 e da Mesa 2 poderia inviabilizar a verificação da propriedade.

8 CONCLUSÃO

Este trabalho tratou do desenvolvimento de Sistemas Supervisórios Híbridos, onde o termo híbrido se refere a presença simultânea de características de Sistemas a Eventos Discretos e de Sistema de Variáveis Contínuas, e onde o termo Supervisório se refere a um sistema de controle inserido em uma estrutura hierárquica.

Uma possível abordagem para o desenvolvimento de Sistema Supervisórios Híbridos é sua divisão em duas fases. Na primeira etapa é gerado um modelo do comportamento do Sistema Supervisório e do seu Objeto de Controle (o sistema controlado). Este modelo é construído usando um formalismo de modelagem que permita de algum modo a validação do sistema supervisório através da análise das características do modelo construído. Na segunda fase, este modelo, já devidamente validado, é então convertido para a linguagem na qual o Sistema Supervisório é implementado.

Considerando esta dicotomia no desenvolvimento de Sistemas Supervisórios Híbridos, este trabalho abordou o problema de como gerar e validar o modelo do Sistema Supervisório e seu Objeto de Controle.

8.1. Principais Contribuições

As principais contribuições deste trabalho podem ser resumidas em três pontos: a introdução de um formalismo para modelagem do Sistema Supervisório e seu Objeto de Controle, a proposta de um procedimento para a construção do modelo usando o formalismo desenvolvido, e a proposta de um procedimento para verificação de propriedades no modelo construído.

As contribuições apresentadas foram avaliadas através da sua aplicação em estudos de casos de diferentes características: um sistema de ar condicionado, o trem de pouso de um avião militar, e uma usina de cana de açúcar.

No que se refere ao formalismo proposto, este é o resultado da incorporação dos conceitos de orientação a objetos a um formalismo já existente, o das redes Predicado-Transição Diferenciais. A principal vantagem desta incorporação é a adoção de uma estrutura modular, que permite o enfoque em apenas uma parte do sistema de cada vez, facilitando a modelagem de sistemas complexos e de grande porte.

Quanto ao procedimento para desenvolvimento do modelo, este consiste na construção sistematizada de uma série de diagramas auxiliares, que têm como finalidade proporcionar um detalhamento gradual das características do Sistema Supervisório e seu Objeto de Controle. Eles representam o mesmo sistema sob diferentes óticas, ressaltando diferentes aspectos do modelo construído. Com exceção do ‘Production Flow Schema’ (PFS), todos os demais diagramas pertencem a ‘Unified Modeling Language’, conhecida como UML, que é um padrão no que se refere a orientação a objetos não apenas para a comunidade científica mas também no âmbito industrial. Desta forma, estes diagramas auxiliam na compreensão do sistema por pessoas que não participaram do processo de modelagem, e na comunicação com pessoas que não conheçam o formalismo de modelagem proposto.

Em relação à análise do modelo construído para validação do Sistema Supervisório, este é baseado na verificação de propriedades. Foram considerados dois tipos de propriedades: de alcançabilidade e de segurança. A primeira consiste em verificar que um estado será atingido em certas circunstâncias e a segunda em verificar que um estado jamais será atingido. A principal vantagem do procedimento proposto para verificação de propriedades é que a estrutura modular do modelo é explorada de forma a decompor um problema de análise complexo, que envolveria o modelo de todo o sistema, em uma série de problemas mais simples, onde considera-se apenas um ou poucos objetos de cada vez.

É importante salientar que este procedimento não garante uma solução. Entre os principais fatores que influenciam a aplicação do procedimento para análise está a comunicação entre os objetos do sistema. Além disso, uma das principais desvantagens deste procedimento é a dependência da interferência do usuário (quem o realiza). Se hipóteses adequadas não forem realizadas, o número de cenários a serem considerados pode tornar inviável sua aplicação.

Através dos estudos de caso, foram analisadas as contribuições realizadas neste trabalho. Entre as conclusões obtidas, considera-se que a aplicação da abordagem e do formalismo proposto para modelagem é mais bem sucedida e enfrenta menores dificuldades, se comparada a aplicação do procedimento proposto para análise. Enquanto a modelagem de sistemas tão complexos como da Usina Cruz Alta pode ser realizada tão facilmente como a modelagem de sistemas mais simples (como os Sistemas de Ar Condicionado A e B), o mesmo não pode ser dito para análise.

Isto advém do fato de que o problema de modelagem de Sistemas Híbridos usando redes de Petri e equações diferenciais vem sendo estudado a vários anos e por diferentes pesquisadores. Um exemplo é a tese de Andreu (1996), defendida há 8 anos, e que já introduzia os conceitos básicos das redes Predicado-Transição Diferencial. Assim, no que se refere a modelagem, este trabalho considerou várias contribuições anteriores. No entanto, do que se tem conhecimento, até o início deste trabalho, não existiam propostas para solucionar o problema de análise de modelos de Sistemas Híbridos usando redes de Petri e equações diferenciais. De fato, atualmente, além do presente trabalho, identifica-se um tema similar apenas na tese de Khalfaoui (2003), que trata do problema de detecção de cenários críticos em sistemas mecatrônicos.

8.2. Trabalhos Futuros

Como a maioria das pesquisas científicas, esta tese não pode, de forma alguma, ser considerada como um trabalho conclusivo, sem perspectivas de aprimoramento, detalhamento ou prosseguimento. As possibilidades de trabalhos futuros deixadas em aberto são inúmeras. Entre elas, destacam-se as seguintes, consideradas de maior relevância.

Durante a modelagem, um ponto particularmente crítico é a definição dos objetos do Sistema Supervisório – isto é, qual a melhor forma de decompor o modelo do Sistema Supervisório. Enquanto os candidatos a classes e objetos do Objeto de Controle em geral podem ser facilmente identificados através da observação do sistema real, o mesmo não pode ser feito para o Sistema Supervisório. No presente trabalho, este problema foi rapidamente abordado. Propõe-se que os candidatos a

objetos do Sistema Supervisório correspondam a objetos, ou grupo de objetos do Objeto de Controle. Neste sentido, cada objeto do Sistema Supervisório é responsável por interagir e armazenar as informações relativas ao seu correspondente no Objeto de Controle. Tal proposta pode ser aprimorada através da introdução de ‘bibliotecas’ de objetos básicos relacionadas ao tipo de sistema ou às funções do Sistema Supervisório, que possam servir como ponto de partida para a construção do modelo do Sistema Supervisório.

Quanto a análise, as possibilidades de trabalhos futuros são muitas. Um ponto ainda não tratado se refere ao uso da simulação e a construção de um simulador. Neste sentido é interessante explorar a decomposição do modelo para realizar uma simulação distribuída. Entre os problemas a serem abordados neste caso está como agrupar os modelos dos objetos de forma a minimizar as interações, como sincronizar a simulação distribuída, etc.

O procedimento proposto para verificação de propriedades também pode ser aprimorado através da sua aplicação a outros estudos de caso. O objetivo é definir uma maior variedade de enunciados para as propriedades, restrições e hipóteses, e de detalhar o procedimento para cada caso, de forma a torná-lo mais automático e menos dependente da pessoa que realiza a análise. Além disso, um ponto ainda em aberto é como, a partir dos requisitos do sistema, definir o conjunto de propriedades a serem verificadas no modelo construído.

Finalmente, um tópico ainda não abordado, referente ao prosseguimento deste trabalho, é o que foi denominado de 2ª Fase do desenvolvimento de Sistemas Supervisórios Híbridos, isto é, como implementar fisicamente o Sistema Supervisório a partir do modelo construído, garantindo que as propriedades verificadas neste modelos sejam conservadas após a efetiva operação do Sistema Supervisório.

ANEXO A - DADOS COMPLEMENTARES DO ESTUDO DE CASO 2 – SISTEMA DE ATERRISSAGEM

Este anexo apresenta a aplicação do procedimento proposto no Capítulo 3 para modelagem, para o Estudo de Caso 2 – Sistema de Aterrisagem do avião Rafale. Além de exemplos dos diagramas resultantes de cada **atividade** do procedimento, é apresentada a lista completa dos objetos que compõem o modelo do Sistema de Aterrisagem (Objeto de Controle e Sistema Supervisor). São ainda apresentados os modelos em redes PTD-OO das classes que não foram apresentados no Capítulo 6.

Apesar de não serem necessários para a compreensão do que foi apresentado no Capítulo 6, os modelos deste anexo documentam o trabalho desenvolvido e comprovam a viabilidade da utilização do procedimento de modelagem para o Estudo de Caso 2. Além disso, a apresentação integral dos modelos do sistema permite que os mesmos sejam utilizados em trabalhos futuros.

A.1. Modelagem do Sistema Supervisor e seu Objeto de Controle

A.1.1. Atividade 1 – Modelagem do Fluxo de Materiais

De acordo com a descrição do sistema apresentada na Seção 6.2.1 do Capítulo 6, o único fluxo de material existente no sistema se refere ao óleo que percorre os circuitos hidráulicos. A Fig. A.1 apresenta a modelagem em PFS deste fluxo.

Fig. A.1. PFS para o fluxo de óleo nos circuitos do Sistema de Aterrisagem.

A.1.2. Atividade 2 – Definição dos Casos de Uso

Considerando os requisitos do Sistema Supervisor descritos na Seção 6.2.2, o Diagrama de Casos de Uso para o Sistema de Aterrisagem é apresentado na Fig. A.2.

Fig. A.2. Diagrama de Casos de Uso para o Sistema de Aterrissagem.

A.1.3. Atividade 3 – Construção dos Diagramas de Atividades

Para ilustrar a **Atividade 3**, seleciona-se o Caso de Uso ‘Executar seqüência Up’, cujo Diagrama de Atividades é apresentado na Fig. A.3.

Fig. A.3. Diagrama de Atividades do Caso de Uso ‘Executar seqüência Up’.

Neste diagrama foram usadas as seguintes siglas: AP para Abertura das Portas, FP para Fechamento das Portas, ET para Extensão dos Trens e RT para Retração dos Trens. Além disso, este diagrama considera que o sistema estava na posição ‘Down’ (todas as

portas fechadas e os trens estendidos) quando a sequência foi solicitada pelo piloto. As *atividades* desenhadas com traço mais espesso ‘—’ (em relação ao traço ‘—’ das demais *atividades*) correspondem ao agrupamento de um conjunto de *atividades* e são detalhadas na sequência. O detalhamento das *atividades* ‘Pressuriza circuito hidráulico geral’ e ‘Despressuriza circuito hidráulico geral’ é apresentado na Fig. A.4. O detalhamento de ‘Abre portas’ é apresentado na Fig. A.5, onde a sigla AP indica Abertura de Portas. O detalhamento de ‘Estende trens’ e ‘Fecha portas’ é semelhante ao de ‘Abre portas’.

Fig. A.4. Detalhamento de ‘Pressuriza’ e ‘Despressuriza circuito hidráulico geral’.

Fig. A.5. Detalhamento de ‘Abre portas’.

Observa-se que, de acordo com a Fig. A.5, a próxima *atividade* da Fig. A.3 ('Acende lâmpada no painel do piloto') é executada tão logo a ordem para não-energização do circuito elétrico de abertura das portas é emitida. Isto ocorre porque o Sistema Supervisório não tem como confirmar o efetivo fechamento da eletro-válvula de abertura de portas.

A.1.4. *Atividade 4 – Definição das Classes e Objetos*

Objeto de Controle

Através da aplicação das 1ª e 2ª Regras de Decomposição (apresentadas na Seção 3.1.4 do Capítulo 3), foram definidos os seguintes objetos e classes:

- C_1 – *Equipamento 1 pistão*: $O_{1,1}$ = Porta Frontal, $O_{2,1}$ = Porta Direita, $O_{3,1}$ = Porta Esquerda, $O_{4,1}$ = Trem Frontal;
- C_2 – *Equipamento 2 pistões*: $O_{1,2}$ = Trem Direito, $O_{2,2}$ = Trem Esquerdo;
- C_3 – *Alavanca Up/Down*: $O_{1,3}$ = Alavanca Up/Down;
- C_4 – *Sensor Discreto*: $O_{1,4}$ = Trem Direito Estendido, $O_{2,4}$ = Trem Esquerdo Estendido, $O_{3,4}$ = Trem Frontal Estendido, $O_{4,4}$ = Trem Direito Retraído, $O_{5,4}$ = Trem Esquerdo Retraído, $O_{6,4}$ = Trem Frontal Retraído, $O_{7,4}$ = Porta Direita Fechada, $O_{8,4}$ = Porta Esquerda Fechada, $O_{9,4}$ = Porta Frontal Fechada, $O_{10,4}$ = Porta Direita Aberta, $O_{11,4}$ = Porta Esquerda Aberta, $O_{12,4}$ = Porta Frontal Aberta, $O_{13,4}$ = Circuito Geral Pressurizado;
- C_5 – *Eletro-válvula / Circuito Hidráulico Geral*: $O_{1,5}$ = EV/CH Geral;
- C_7 – *Eletro-válvula de Pressão Positiva*: $O_{1,7}$ = EV Abertura de Portas, $O_{2,7}$ = EV Extensão de Trens;
- C_8 – *Eletro-válvula de Pressão Negativa*: $O_{1,8}$ = EV Fechamento de Portas, $O_{2,8}$ = EV Retração de Trens;
- C_9 – *Circuito Hidráulico Dedicado*: $O_{1,9}$ = CH Portas, $O_{2,9}$ = CH Trens;
- C_{11} – *Circuito Elétrico Geral*: $O_{1,11}$ = CE Geral;
- C_{12} – *Circuito Elétrico Dedicado*: $O_{1,12}$ = CE Abertura de Portas, $O_{2,12}$ = CE Fechamento de Portas, $O_{3,12}$ = CE Extensão de Trens, $O_{4,12}$ = CE Retração de Trens;
- C_{13} – *Relé Analógico*: $O_{1,13}$ = Relé Analógico.

Sistema Supervisório

Através da aplicação da 1ª Regra de Decomposição, foram definidos os seguintes objetos e classes para o Sistema Supervisório:

- C_{14} – *Supervisor de Equipamento*: $O_{1,14}$ = Supervisor Porta Frontal, $O_{2,14}$ = Supervisor Porta Direita, $O_{3,14}$ = Supervisor Porta Esquerda, $O_{4,14}$ = Supervisor Trem Frontal, $O_{5,14}$ = Supervisor Trem Direito, $O_{6,14}$ = Supervisor Trem Esquerdo;

- C_{15} – *Supervisor de Conjunto*: $O_{1.15}$ = Supervisor Conjunto Frontal, $O_{2.15}$ = Supervisor Conjunto Direito, $O_{3.15}$ = Supervisor Conjunto Esquerdo;
- C_{16} – *Supervisor do Sistema*: $O_{1.16}$ = Supervisor do Sistema;
- C_{17} – *Interface Alavanca*: $O_{1.17}$ = Interface Alavanca;
- C_{18} – *Interface EV Geral*: $O_{1.18}$ = Interface EV Geral;
- C_{19} – *Interface EV Dedicada*: $O_{1.19}$ = Interface EV Portas, $O_{2.19}$ = Interface EV Trens.

A.1.5. *Atividade 5 – Construção dos Diagramas de Seqüência ou Colaboração*

Considerando o mesmo Caso de Uso selecionado para ilustrar a **Atividade 3**, isto é o Caso de Uso ‘Executar seqüência Up’, apresenta-se na Fig. A.6 e na Fig. A.7 alguns dos Diagramas de Seqüência correspondentes.

Fig. A.6. Diagrama de Seqüência p/ Caso de Uso 'Executar Seqüência Up' – Parte 1.

A Fig. A.6 apresenta as chamadas de métodos desde o início do cenário até a finalização da pressurização do circuito hidráulico geral. Foram utilizadas as seguintes siglas para os nomes dos objetos neste diagrama: CE AP para CE Abertura de Portas, CE FP para CE Fechamento de Portas, CE ET para CE Extensão de Trens, CE RT para CE Retração de Trens.

Na seqüência, as chamadas de métodos relativas à abertura das portas são apresentadas na Fig. A.7. O procedimento para extensão dos trens e fechamento das portas é semelhante ao de abertura das portas. Foram usadas as seguintes siglas para os nomes dos objetos: CE AP para CE Abertura de Portas, EV AP para EV Abertura de Portas, PF Ab., PD

Ab. e PE Ab. para os sensores Porta Frontal Aberta, Porta Direita Aberta e Porta Esquerda Aberta, PF Fec., PD Fec. e PE Fec. para os sensores Porta Frontal Fechada, Porta Direita Fechada e Porta Esquerda Fechada.

Fig. A.7. Diagrama de Sequência p/ Caso de Uso 'Executar Sequência Up' – Parte 2.

A.1.6. Atividade 6 – Modelagem das Classes em redes PTD-OO

São apresentados aqui apenas os modelos em redes PTD-OO das classes que não constam no Capítulo 6. São portanto omitidos os modelos das classes C_1 , C_7 , C_8 , C_9 , C_{10} , C_{12} e C_{19} .

C_2 – Equipamento 2 Pistões (Fig. A.8)

Esta classe modela os trens laterais, que têm sua posição determinada por dois pistões, cujas posições são representadas por x_1 e x_2 . O primeiro pistão é responsável por bloquear o trem na posição estendida e o segundo por estender e recolher o trem. A variável K_p indica a pressão necessária para a movimentação dos pistões. As variáveis K_{x_1} e K_{x_2} indicam os cursos dos pistões enquanto K_v corresponde a velocidade de movimentação quando a diferença de pressão no circuito hidráulico correspondente $p_{11.C9}$ atinge K_p .

Fig. A.8. Modelo da classe C₂- Equipamento 2 Pistões.**C₃ – Alavanca Up/Down (Fig. A.9)**

Através da alavanca, o piloto solicita a execução das sequencias ‘Up’ ($t_{8,3}$) e ‘Down’ ($t_{1,3}$).

Quando a posição da alavanca é modificada, o estado do relé analógico é atualizado ($t_{3,3}$ e $t_{4,3}$) e o sistema supervisão é notificado ($t_{2,3}$ e $t_{6,3}$).

Fig. A.9. Modelo da classe C₃- Alavanca Up/Down.**C₄ – Sensor Discreto (Fig. A.10)**

Os diversos sensores discretos do Sistema de Aterrissagem podem assumir dois estados: ‘Off’ ($p_{1,4}$) e ‘On’ ($p_{2,4}$). Os métodos associados a $t_{3,4}$ e $t_{4,4}$ são utilizados pelo Sistema Supervisão para verificar o estado dos sensores.

Fig. A.10. Modelo da classe C₄- Sensor Discreto.

C₅ – Eletro-válvula / Circuito Hidráulico Geral (Fig. A.12)

A pressão no circuito hidráulico geral é determinada pela eletro-válvula geral, que pode assumir duas posições (Fig. A.11). Quando a eletro-válvula geral está aberta, a pressão no circuito hidráulico (p_g) aumenta a uma taxa constante de K_{v_g} até atingir a pressão de K_{p_g} . Quando a válvula é fechada, o circuito hidráulico é conectado ao escape e a pressão do circuito decai para zero.

Fig. A.11. Posições da eletro-válvula geral.

Fig. A.12. Modelo da classe *C₅- Eletro-válvula / Circuito Hidráulico Geral*.

C₁₁ – Circuito Elétrico Geral

Esta classe, responsável pelo acionamento da eletro-válvula geral é definida como uma especialização da classe *C₁₀ – Circuito Elétrico Genérico*, apresentada no Capítulo 6. Considerando a definição de *C₁₀*, o modelo desta classe é dado pela especificação das seguintes interfaces para as transições t_{1_10} , t_{5_10} e t_{6_10} :

- $t_{1_11} \rightarrow t_{1_5.11}$ – Abrir eletro-válvula geral
- $t_{5_11} \rightarrow t_{2_5.11}$ – Fechar eletro-válvula geral
- $t_{6_11} \rightarrow t_{2_5.11}$ – Fechar eletro-válvula geral

C₁₃ – Relé Analógico (Fig. A.13)

O relé analógico é aberto após K_0 da última chamada do método associado a t_{14_13} (o que ocorre sempre que a Alavanca Up/Down tem seu estado modificado). O relé analógico interage com os seguintes circuitos elétricos: CE Geral, CE Abertura de Portas, CE Fechamento de Portas, CE Extensão de Trens e CE Retração de Trens.

Fig. A.13. Modelo da classe C_{13} – Relé Analógico. **C_{14} – Supervisor de Equipamento (Fig. A.14)**

Esta classe do Sistema Supervisório é responsável por verificar os sensores e determinar o estado da porta ou trem, de acordo com as Tabelas 6.1 e 6.2, apresentadas na Seção 6.2.2 do Capítulo 6.

A informação sobre o estado do equipamento é transmitida ao objeto solicitante através das transições t_{6_14} , t_{7_14} e t_{8_14} . Se o estado dos sensores é inconsistente, um alarme é acionado e o objeto atinge um estado de ‘deadlock’.

 C_{15} – Supervisor de Conjunto (Fig. A.15)

Esta classe é responsável por determinar o estado dos conjuntos porta-trem, de acordo com a Tabela 6.3 apresentada na Seção 6.2.2 do Capítulo 6. A informação sobre o estado do equipamento é transmitida ao objeto solicitante através das transições t_{10_15} a t_{16_15} . Se o estado do conjunto é inconsistente, um alarme é acionado e o objeto atinge um estado de ‘deadlock’.

Fig. A.16. Modelo da classe C₁₆ – Supervisor do Sistema.**C₁₇ – Interface Alavanca (Fig. A.17)**

Esta classe executa as seqüências ‘Up’ ou ‘Down’ de acordo com o solicitado pela Alavanca Up/Down (chamada dos métodos t_{1_17} e t_{2_17}). Quando o método ‘Executar seqüência Up’ (t_{2_17}) é chamado, esta seqüência só é executada se os amortecedores do avião não estiverem pressionados (t_{5_17}). Se a alavanca vai para a posição ‘Down’ enquanto o Sistema Supervisor está executando a seqüência ‘Up’, esta é interrompida e inicia-se com a seqüência ‘Down’.

C₁₈ – Interface EV Geral (Fig. A.18)

Quando solicitado, esta classe atua sobre o circuito elétrico geral (C₁₁), de forma a abrir ou fechar a eletro-válvula geral. A abertura ou fechamento da válvula são confirmados pelo estado do sensor discreto Circuito Geral Pressurizado.

Fig. A.17. Modelo da classe C₁₇ – Interface Alavanca. Fig. A.18. Modelo da classe C₁₈ – Interface EV Geral.

As relações entre as classes previamente descritas são apresentadas no Diagrama de Classes da Fig. A.19.

Fig. A.19. Diagrama de Classes para o Sistema de Aterrissagem.

Conforme apresentado no Capítulo 6, considerou-se como estado inicial o Sistema de Aterrissagem na completamente estendido (posição ‘Down’), que corresponde a seguinte marcação:

Objeto de Controle

- $O_{1,1} = \text{Porta Frontal}$; $X_{1,1} = \{x = 0, K_p = 10, K_v = 1, K_x = 0,5, l_1 = \text{CH Portas}, l_2 = \text{Porta Frontal Fechada}, l_3 = \text{Porta Frontal Aberta}\}$; $m_{1,1} = \{p_{1,1}\}$;
- $O_{2,1} = \text{Porta Direita}$; $X_{2,1} = \{x = 0, K_p = 10, K_v = 1, K_x = 0,5, l_1 = \text{CH Portas}, l_2 = \text{Porta Direita Fechada}, l_3 = \text{Porta Direita Aberta}\}$; $m_{2,1} = \{p_{1,1}\}$;
- $O_{3,1} = \text{Porta Esquerda}$; $X_{3,1} = \{x = 0, K_p = 10, K_v = 1, K_x = 0,5, l_1 = \text{CH Portas}, l_2 = \text{Porta Esquerda Fechada}, l_3 = \text{Porta Esquerda Aberta}\}$; $m_{3,1} = \{p_{1,1}\}$;
- $O_{4,1} = \text{Trem Frontal}$; $X_{4,1} = \{x = 0, K_p = 10, K_v = 0,5, K_x = 1, l_1 = \text{CH Trens}, l_2 = \text{Trem Frontal Retraído}, l_3 = \text{Trem Frontal Estendido}\}$; $m_{4,1} = \{p_{5,1}\}$;
- $O_{1,2} = \text{Trem Direito}$; $X_{1,2} = \{x_1 = 0, x_2 = 0, K_p = 10, K_v = 0,5, K_{x,1} = 1, K_{x,2} = 0,2, l_1 = \text{CH Trens}, l_2 = \text{Trem Direito Retraído}, l_3 = \text{Trem Direito Estendido}\}$; $m_{1,2} = \{p_{8,2}\}$;
- $O_{2,2} = \text{Trem Esquerdo}$; $X_{2,2} = \{x_1 = 0, x_2 = 0, K_p = 10, K_v = 0,5, K_{x,1} = 1, K_{x,2} = 0,2, l_1 = \text{CH Trens}, l_2 = \text{Trem Esquerdo Retraído}, l_3 = \text{Trem Esquerdo Estendido}\}$; $m_{2,2} = \{p_{8,2}\}$;
- $O_{1,3} = \text{Alavanca Up/Down}$; $X_{1,3} = \{l_1 = \text{Interface Alavanca}, l_2 = \text{Relé Analógico}\}$; $m_{1,3} = \{p_{10,3}\}$;
- $O_{1,4} = \text{Trem Direito Estendido}$; $m_{1,4} = \{p_{2,4}\}$;
- $O_{2,4} = \text{Trem Esquerdo Estendido}$; $m_{2,4} = \{p_{2,4}\}$;

- $O_{3,4} = \text{Trem Frontal Estendido}; m_{3,4} = \{p_{2,4}\};$
- $O_{4,4} = \text{Trem Direito Retraído}; m_{4,4} = \{p_{2,4}\};$
- $O_{5,4} = \text{Trem Esquerdo Retraído}; m_{5,4} = \{p_{1,4}\};$
- $O_{6,4} = \text{Trem Frontal Retraído}; m_{6,4} = \{p_{1,4}\};$
- $O_{7,4} = \text{Porta Direita Fechada}; m_{7,4} = \{p_{1,4}\};$
- $O_{8,4} = \text{Porta Esquerda Fechada}; m_{8,4} = \{p_{2,4}\};$
- $O_{9,4} = \text{Porta Frontal Fechada}; m_{9,4} = \{p_{2,4}\};$
- $O_{10,4} = \text{Porta Direita Aberta}; m_{10,4} = \{p_{1,4}\};$
- $O_{11,4} = \text{Porta Esquerda Aberta}; m_{11,4} = \{p_{1,4}\};$
- $O_{12,4} = \text{Porta Frontal Aberta}; m_{12,4} = \{p_{1,4}\};$
- $O_{13,4} = \text{Circuito Geral Pressurizado}; m_{13,4} = \{p_{1,4}\};$
- $O_{1,5} = \text{EV/CH Geral}; X_{1,5} = \{p_g = 0, K_{p_g} = 12, K_v = 4, l_1 = \text{Circuito Geral Pressurizado}\};$
 $m_{1,5} = \{p_{1,5}, p_{5,5}\};$
- $O_{1,7} = \text{EV Abertura de Portas}; X_{1,7} = \{l_1 = \text{CH Portas}\}; m_{1,7} = \{p_{1,7}\};$
- $O_{2,7} = \text{EV Extensão de Trens}; X_{2,7} = \{l_1 = \text{CH Trens}\}; m_{2,7} = \{p_{1,7}\};$
- $O_{1,8} = \text{EV Fechamento de Portas}; X_{1,8} = \{l_1 = \text{CH Portas}\}; m_{1,8} = \{p_{1,8}\};$
- $O_{2,8} = \text{EV Retração de Trens}; X_{2,8} = \{l_1 = \text{CH Trens}\}; m_{2,8} = \{p_{1,8}\};$
- $O_{1,9} = \text{CH Portas}; X_{1,9} = \{p = -9,6, l_1 = \text{EV/CH Geral}\}; m_{1,9} = \{p_{1,9}\};$
- $O_{2,9} = \text{CH Trens}; X_{2,9} = \{p = 9,6, l_1 = \text{EV/CH Geral}\}; m_{2,9} = \{p_{1,9}\};$
- $O_{1,11} = \text{CE Geral}; X_{1,11} = \{l_1 = \text{EV/CH Geral}\}; m_{1,11} = \{p_{7,11}\};$
- $O_{1,12} = \text{CE Abertura de Portas}; X_{1,12} = \{l_1 = \text{EV Abertura de Portas}\}; m_{1,12} = \{p_{7,12}\};$
- $O_{2,12} = \text{CE Fechamento de Portas}; X_{2,12} = \{l_1 = \text{EV Fechamento de Portas}\}; m_{2,12} =$
 $\{p_{7,12}\};$
- $O_{3,12} = \text{CE Extensão de Trens}; X_{3,12} = \{l_1 = \text{EV Extensão de Trens}\}; m_{3,12} = \{p_{7,12}\};$
- $O_{4,12} = \text{CE Retração de Trens}; X_{4,12} = \{l_1 = \text{EV Retração de Trens}\}; m_{4,12} = \{p_{7,12}\};$
- $O_{1,13} = \text{Relé Analógico}; X_{1,13} = \{\theta = \text{ind}, K_0 = 15, l_1 = \text{CE Geral}, l_2 = \text{CE Abertura de}$
 $\text{Portas}, l_3 = \text{CE Fechamento de Portas}, l_4 = \text{CE Extensão de Trens}, l_5 = \text{CE Retração de}$
 $\text{Trens}\}; m_{4,12} = \{p_{23,13}, p_{24,13}\};$

Sistema Supervisor

- $O_{1,14} = \text{Supervisor Porta Frontal}; X_{1,14} = \{l_1 = \text{Porta Frontal Fechada}, l_2 = \text{Porta Frontal}$
 $\text{Aberta}\}; m_{1,14} = \{p_{1,14}\};$
- $O_{2,14} = \text{Supervisor Porta Direita}; X_{2,14} = \{l_1 = \text{Porta Direita Fechada}, l_2 = \text{Porta Direita}$
 $\text{Aberta}\}; m_{2,14} = \{p_{1,14}\};$

- $O_{3,14} = \text{Supervisor Porta Esquerda}$; $X_{3,14} = \{l_1 = \text{Porta Esquerda Fechada}, l_2 = \text{Porta Esquerda Aberta}\}$; $m_{3,14} = \{p_{1,14}\}$;
- $O_{4,14} = \text{Supervisor Trem Frontal}$; $X_{4,14} = \{l_1 = \text{Trem Frontal Retraído}, l_2 = \text{Trem Frontal Estendido}\}$; $m_{4,14} = \{p_{1,14}\}$;
- $O_{5,14} = \text{Supervisor Trem Direito}$; $X_{5,14} = \{l_1 = \text{Trem Direito Retraído}, l_2 = \text{Trem Direito Estendido}\}$; $m_{5,14} = \{p_{1,14}\}$;
- $O_{6,14} = \text{Supervisor Trem Esquerdo}$; $X_{6,14} = \{l_1 = \text{Trem Esquerdo Retraído}, l_2 = \text{Trem Esquerdo Estendido}\}$; $m_{6,14} = \{p_{1,14}\}$;
- $O_{1,15} = \text{Supervisor Conjunto Frontal}$; $X_{1,15} = \{l_1 = \text{Supervisor Porta Frontal}, l_2 = \text{Supervisor Trem Frontal}\}$; $m_{1,15} = \{p_{1,15}\}$;
- $O_{2,15} = \text{Supervisor Conjunto Direito}$; $X_{2,15} = \{l_1 = \text{Supervisor Porta Direita}, l_2 = \text{Supervisor Trem Direito}\}$; $m_{2,15} = \{p_{1,15}\}$;
- $O_{3,15} = \text{Supervisor Conjunto Esquerdo}$; $X_{3,15} = \{l_1 = \text{Supervisor Porta Esquerda}, l_2 = \text{Supervisor Trem Esquerdo}\}$; $m_{3,15} = \{p_{1,15}\}$;
- $O_{1,16} = \text{Supervisor do Sistema}$; $X_{1,16} = \{\theta = ind, K_{\theta} = 40.10^{-3}, l_1 = \text{Supervisor Conjunto Frontal}, l_2 = \text{Supervisor Conjunto Direito}, l_3 = \text{Supervisor Conjunto Esquerdo}\}$; $m_{1,16} = \{p_{1,16}\}$;
- $O_{1,17} = \text{Interface Alavanca}$; $X_{1,17} = \{l_1 = \text{Interface EV Geral}, l_2 = \text{Interface EV Portas}, l_3 = \text{Interface EV Trens}\}$; $m_{1,17} = \{p_{2,17}, p_{6,17}, p_{26,17}\}$;
- $O_{1,18} = \text{Interface EV Geral}$; $X_{1,18} = \{\theta = ind, K_{\theta 1} = 4, K_{\theta 2} = 1, l_1 = \text{Circuito Geral Pressurizado}, l_2 = \text{CE Geral}\}$; $m_{1,18} = \{p_{1,18}\}$;
- $O_{1,19} = \text{Interface EV Portas}$; $X_{1,19} = \{\theta = ind, K_{\theta 1} = 2, K_{\theta 2} = 1, l_1 = \text{CE Fechamento de Portas}, l_2 = \text{CE Abertura de Portas}, l_3 = \text{Porta Frontal Aberta}, l_4 = \text{Porta Direita Aberta}, l_5 = \text{Porta Esquerda Aberta}, l_6 = \text{Porta Frontal Fechada}, l_7 = \text{Porta Direita Fechada}, l_8 = \text{Porta Esquerda Fechada}\}$; $m_{1,19} = \{p_{1,19}\}$;
- $O_{2,19} = \text{Interface EV Trens}$; $X_{2,19} = \{\theta = ind, K_{\theta 1} = 2, K_{\theta 2} = 1, l_1 = \text{CE Retração de Trens}, l_2 = \text{CE Extensão de Trens}, l_3 = \text{Trem Frontal Estendido}, l_4 = \text{Trem Direito Estendido}, l_5 = \text{Trem Esquerdo Estendido}, l_6 = \text{Trem Frontal Retraído}, l_7 = \text{Trem Direito Retraído}, l_8 = \text{Trem Esquerdo Retraído}\}$; $m_{2,19} = \{p_{24,19}\}$;

A.1.7. *Atividade 7 – Verificação dos Modelos*

Modelo em redes PTD-OO e Diagramas de Seqüência e/ou Colaboração

Para ilustrar a **Atividade 7**, a Fig. A.20 e a Fig. A.21 apresentam a relação entre as interação dos Diagramas de Seqüência para o Caso de Uso ‘Executar Seqüência Up’ (Fig. A.6 e Fig. A.7) e as transições dos modelos em redes PTD das classes.

Fig. A.20. Correspondência entre Diagrama de Sequência da Fig. A.6 e o modelo em redes PTD-OO.

Fig. A.21. Correspondência entre Diagrama de Sequência da Fig. A.7 e o modelo em redes PTD-OO.

Modelo em redes PTD-OO e Diagrama de Atividade

A Fig. A.22, a Fig. A.23 e a Fig. A.24 apresentam o detalhamento dos Diagramas de Atividades da Fig. A.3, da Fig. A.4 e da Fig. A.5, respectivamente, considerando agora as atividades específicas das comunicações entre os objetos.

Estes diagramas são então convertidos para redes de Petri. A Fig. A.25 apresenta a conversão desde o início do cenário até a atividade ‘EV/CH Geral modifica posição do Circuito Pressurizado para On’, do conjunto de atividades ‘Pressuriza circuito hidráulico geral’ (Fig. A.23). A Fig. A.26 apresenta a conversão das atividades que vão desde ‘Interface Alavanca solicita abertura de portas à Interface EV Portas’ até ‘EV Abertura de Portas bloqueia pressão positiva em CH Portas’, do conjunto de atividades ‘Abre Portas’ (Fig. A.24).

Fig. A.22. Detalhamento do Diagrama de Atividades da Fig. A.3.

Fig. A.23. Detalhamento do Diagrama de Atividades da Fig. A.4.

Fig. A.24. Detalhamento do Diagrama de Atividades da Fig. A.5.

Destaca-se na rede da Fig. A.26 que não existe equivalente nos modelos das classe PTD-OO à transição que segue o lugar p_{3_9} . Isto ocorre porque a relação de pré-condição entre p_{3_9} e o disparo das transições $t_{1_1} \rightarrow t_{2_4}$ é fornecida através do compartilhamento da variável p do objeto da classe C_9 com os objetos da classe C_1 . De fato, a presença de uma marca em p_{3_9} indica que ' $p = p_g = K_p$ ' e portanto a função de habilitação ' $p \geq K_p$ ' das três transições t_{1_1} , correspondentes a cada uma das portas, está satisfeita.

A.2. Observações

Para ilustrar a complexidade das interações discretas entre os diversos objetos apresentam-se a seguir os Diagramas de Colaborações Estáticos que ilustram as possíveis interações entre os objetos do Sistema de Aterrissagem são apresentados.

Fig. A.25. Conversão para redes de Petri do Diagrama de Atividades da Fig. A.22 e da Fig. A.23.

A Fig. A.27 apresenta as comunicações entre o relé analógico, os circuitos elétricos, as eletro-válvulas, os circuitos hidráulicos, os trens e as portas. Continuando, a Fig. A.28 apresenta as comunicações entre trens, portas e os respectivos sensores discretos. Estas duas figuras representam as interações entre si dos objetos do Objeto de Controle.

Se considerarmos os tipos de interações em um Sistema Produtivo, (apresentados na Fig. 1.4, da Seção 1.1.2 do Capítulo 1) a Fig. A.29 ilustra as interações relativas à *detecção*, correspondente as comunicações entre os objetos do Sistema Supervisório e os sensores discretos do Objeto de Controle, e à *atuação*, correspondente a interferência do Sistema Supervisório nos circuitos elétricos.

Por sua vez, a Fig. A.30 ilustra as relações de *comando*, isto é, como o piloto (entidade externa ao sistema) interage com os objetos do Sistema Supervisório. Finalmente, Fig. A.31 ilustra as comunicações internas entre os objetos do Sistema Supervisório. Observa-se que a *monitoração* não é apresentada nestes diagramas porque na modelagem não foram considerados objetos específicos para emissão de mensagens, alarmes, etc.

Fig. A.26. Conversão para redes de Petri do Diagrama de Atividades da Fig. A.22 e da Fig. A.24.

Fig. A.27. Diagrama de Colaboração I – Sistema de Aterrissagem.

Fig. A.28. Diagrama de Colaboração II – Sistema de Aterrissagem.

Fig. A.29. Diagrama de Colaboração III – Sistema de Aterrissagem.

Fig. A.30. Diagrama de Colaboração IV – Sistema de Aterrissagem.

Fig. A.31. Diagrama de Colaboração V – Sistema de Aterrissagem.

ANEXO B - DADOS COMPLEMENTARES DO ESTUDO DE CASO 3 – USINA DE AÇÚCAR

Este anexo apresenta a aplicação do procedimento proposto no Capítulo 3 para modelagem, para o Estudo de Caso 3 – Usina de Cana de Açúcar.

Além de exemplos dos diagramas a serem construídos para cada **atividade** do procedimento, é apresentada a lista completa dos objetos que compõem o modelo do Objeto de Controle e Sistema Supervisório e os modelos em redes PTD-OO das classes que não foram apresentados no Capítulo 7.

Apresenta-se ainda, como exemplo adicional de análise, a verificação de uma propriedade de alcançabilidade.

B.1. Modelagem do Sistema Supervisório e seu Objeto de Controle

Observa-se que a **Atividade 1** do procedimento de modelagem foi apresentada no Capítulo 7. Assim, inicia-se com a **Atividade 2**.

B.1.1. Atividade 2 – Definição dos Casos de Uso

Como exemplo, a Fig. B.1 apresenta o Diagrama de Casos de Uso, definido de acordo com os requisitos apresentados no Capítulo 7, para os processos de Recepção, Preparo e Cozimento.

Fig. B.1. Diagrama de Casos de Uso para Recepção, Preparo e Cozimento.

B.1.2. Atividade 3 – Construção dos Diagramas de Atividades

Como exemplo para este estudo de caso, considera-se o detalhamento do Caso de Uso ‘Descarregar caminhão c/ caçamba basculante’.

A sequência de atividades definida para este estudo de caso considera que cada guindaste pode fazer os seguintes movimentos (Fig. B.2): levantar e abaixar o cabo, rotacionar em torno do eixo horizontal e rotacionar em torno do eixo vertical.

Fig. B.2. Movimentação do guindaste.

Para descarregar caminhões c/ caçamba basculante, o cabo do guindaste é preso na lateral do caminhão e içado, rotacionando a caçamba e derrubando a cana (Fig. B.3). No caso de caminhões c/ correntes, a cana chega a usina amarrada em feixes c/correntes de aço. Para descarregar, o cabo do guindaste é preso às correntes, retirando o feixe do caminhão e depositando-o no local apropriado (Fig. B.4).

Fig. B.3. Descarregamento do caminhão c/ caçamba basculante.

Fig. B.4. Descarregamento do caminhão c/ correntes.

A Fig. B.5 apresenta o Diagrama de *Atividades* para o Caso de Uso ‘Descarregar caminhão c/ caçamba basculante’.

Fig. B.5. Diagrama de Atividades do Caso de Uso 'Descarregar caminhão c/ caçamba basculante'.

B.1.3. Atividade 4 – Definição das Classes e Objetos

Objeto de Controle - Recepção

Na aplicação da 1ª Regra de Decomposição (apresentadas na Seção 3.1.4 do Capítulo 3), são candidatos à objetos os caminhões c/ correntes (cuja interface com o guindaste pode ser definida de forma discreta), o Caminhão c/ Garras, o Chuveiro 1 (associado à Mesa 1) e o Chuveiro 2. No caso dos caminhões c/ correntes, o número de caminhões na usina (e portanto de objetos) varia no decorrer do dia. Para evitar oinstanciamento dinâmico de objetos, considera-se que o número máximo de caminhões presentes na usina é 10. Assim, são definidos 10 objetos: Caminhão c/ Correntes 1, Caminhão c/ Correntes 2, ..., Caminhão c/ Correntes 10, cuja chegada na usina ocorre através de uma chamada de método realizada por um elemento externo ao sistema, que define, entre outras coisas, o volume de cana a ser entregue.

A aplicação da 2ª Regra de Decomposição leva a definição de objetos relacionados aos guindastes (Guindaste Mesa e Guindaste Fosso) e aos caminhões c/ caçamba basculante (Caminhão c/ Caçamba 1, Caminhão c/ Caçamba 2, ..., Caminhão c/ Caçamba 10). A interface destes com os guindaste é continua durante o descarregamento do caminhão (diferentemente do caso dos caminhões c/ correntes onde a interface é através de eventos discretos). Outro objeto definido através da aplicação da 2ª Regra é o Fosso, que interage com o caminhões c/ caçamba de forma contínua durante um intervalo de tempo restrito (o

descarregamento) e de forma discreta com os caminhões c/ correntes ou com o caminhão c/ garra.

A aplicação da 3ª Regra de Decomposição resulta na definição dos objetos Mesa 1, Mesa 2. A velocidade das mesas e esteiras pode variar de forma discreta entre três valores (associados aos 3 volumes de produção da usina), assim, associa-se as mesas os objetos VV Mesa 1 e VV Mesa 2, responsáveis por determinar sua velocidade.

Estes objetos são organizados nas seguintes classes:

- C_2 - Caminhão c/ Caçamba Basculante – Caminhão c/ Caçamba 1, Caminhão c/ Caçamba 2, ..., Caminhão c/ Caçamba 10.
- C_3 – Caminhão c/ Correntes – Caminhão c/ Correntes 1, Caminhão c/ Correntes 2, ..., Caminhão c/ Correntes 10.
- C_4 – Transportador c/ Garras – Transportador c/ Garras.
- C_5 – Guindaste – Guindaste Mesa, Guindaste Fosso.
- C_6 – Fosso – Fosso.
- C_7 – Mesa – Mesa 1, Mesa 2.
- C_8 – Chuveiro – Chuveiro 1, Chuveiro 2.
- C_9 – Variador de Velocidade – VV Mesa 1, VV Mesa 2.

Objeto de Controle – Preparo

O fluxo de cana através das esteiras é contínuo, assim, qualquer decomposição do Objeto de Controle relacionado ao preparo da cana só é possível através da aplicação da 3ª Regra. Considerando que existe um ciclo fechado de dependência entre o picador e a Esteira 1 (o fluxo de saída do picador depende do fluxo de entrada na Esteira 1 e, simultaneamente influencia o fluxo de saída da Esteira 1) e entre a Esteira 2 e a Esteira 3, as classes e objetos definidos neste caso são.

- C_8 – Variador de Velocidade: VV Esteira 1, VV Esteira 2 (a velocidade da Esteira 3 é constante).
- C_{12} – Preparador – Esmagador.
- C_{13} – Esteira 1-Picador – Esteira 1-Picador.
- C_{15} – Esteira 2-Esteira 3 – Esteira 2-Esteira 3.

Objeto de Controle - Difusão

A aplicação da 1ª Regra de Decomposição leva ao seguinte objeto e classe:

- C_{23} – Controle Local do Difusor – Controle Local do Difusor.

Através da aplicação da 3ª Regra de Decomposição, foram definidos os seguintes objetos e classes:

- C_8 – Variador de Velocidade – VV Transportador

- C_{16} – *Válvula de Água* – Válvula de água.
- C_{22} – *Difusor* – Difusor.

Objeto de Controle – Sulfitação

A aplicação da 1ª Regra de Decomposição resulta em:

- C_{27} – *Caixa de Cal* – Caixa de Cal.
- C_{32} – *Trocador de Calor* – Trocador de Calor

A aplicação da 3ª Regra de Decomposição resulta em:

- C_{25} – *Variador de Potência* – VP Tanque-Bomba Sulfitação.
- C_{26} – *Compressor* – Compressor.
- C_{24} – *Tanque-Bomba* – *Sulfitação* – Tanque-Bomba Sulfitação.
- C_{31} – *Sulfitador* – Sulfitador.

Objeto de Controle – Calagem

A aplicação da 3ª Regra de Decomposição resulta em:

- C_{25} – *Variador de Potência* – VP Tanque Misturador.
- C_{33} – *Tanque Rotativo* – Tanque Rotativo.
- C_{37} – *Calagem* – Calagem.

Objeto de Controle – Aquecimento

A aplicação da 3ª Regra de Decomposição resulta em:

- C_{38} – *Divisor de Fluxo - Aquecimento* – DV Serie 1, DV Serie 2, DV Serie 3 e DV Serie 4.
- C_{39} – *Válvula On/Off* – VOO Serie 1, VOO Serie 2, VOO Serie 3 e VOO Serie 4.
- C_{40} – *Válvula 2 Posições - Aquecedor* – 12 objetos: V2P Serie 1.1, V2P Serie 1.2, V2P Serie 1.3, V2P Serie 1.4, V2P Serie 2.1, V2P Serie 2.2, V2P Serie 2.3, V2P Serie 2.4, V2P Serie 3.1, V2P Serie 3.2, V2P Serie 3.3 e V2P Serie 3.4.

Objeto de Controle – Clarificação

A aplicação da 3ª Regra de Decomposição resulta em:

- C_{25} – *Variador de Potência* – VP Tanque Clarificação
- C_{47} – *Clarificação* – Clarificação.

Objeto de Controle – Evaporação

A aplicação da 3ª Regra de Decomposição resulta em:

- C_{51} – *1º Efeito* – 1º. Efeito.
- C_{55} – *2º. Efeito* – 2º. Efeito.
- C_{62} – *3-4-5º. Efeitos* – 3-4-5º. Efeitos.

Objeto de Controle – Cozimento

O cozimento é um processo por bateladas, assim, a decomposição desta parte do Objeto de Controle é obtida através da aplicação da 2ª Regra de Decomposição. As classes e objetos resultantes são:

- C_{65} – *Cozedor*- Cozedor 1, Cozedor 2, ..., Cozedor 10.
- C_{66} – *Tanque Massa* – T. Massa A, T. Massa B, T. Massa C.

A aplicação da 3ª Regra de Decomposição resulta em:

- C_{64} – *Tanque Xarope* – Tanque Xarope.

Objeto de Controle – Centrifugação

Semelhantemente ao Cozimento, a aplicação da 2ª Regra de Decomposição resulta em:

- C_{67} – *Centrífuga*- N objetos: Centrífuga 1, Centrífuga 2, ..., Centrífuga 10.
- C_{68} – *Tanque Magma*- T Magma B, T. Magma C.
- C_{69} – *Tanque Mel* - T Mel A, T. Mel B, T. Mel C.
- C_{70} – *Caminhão de Mel C* – Caminhão de Mel 1, ..., Caminhão de Mel N.

Objeto de Controle – Secagem e Empacotamento

A aplicação da 3ª Regra de Decomposição resulta em:

- C_{71} – *Tanque de Açúcar*- T. Açúcar.
- C_{72} – *Secador*- Secador.
- C_{73} – *Empacotador*- Empacotador.

Sistema Supervisório

O modelo do Sistema Supervisório é composto por:

- C_{74} – *Interface Mesas* – Interface Mesas
- C_{75} – *Supervisor Fosso* – Supervisor Fosso
- C_{76} – *Supervisor Esmagador-Picador* – Supervisor Esmagador Picador
- C_{77} – *Gerenciador da Produção de Caldo* – Gerenciador da Produção de Caldo
- C_{78} – *Interface Variadores de Velocidade* – Interface VV
- C_{79} – *Interface Válvula de Caldo* – Interface Válvula de Caldo.
- C_{80} – *Supervisor Tanque Bomba Sulfitação* – Supervisor TB Sulfitação.
- C_{81} – *Interface Bandeja de Cal* – Interface Bandeja de Cal .
- C_{82} – *Interface Forno* – Interface Forno.
- C_{83} – *Gerenciador Sulfitação- Calagem* – Gerenciador Sulfitação - Calagem.
- C_{85} – *Supervisor Tanque Leite de Cal* – Supervisor Tanque Leite de Cal.
- C_{86} – *Supervisor Tanque Misturador* – Supervisor Tanque Misturador.

- *C₈₇ – Interface Variador de Potência – Interface VP Sulfitação, Interface VP Aquecimento, Interface VP Clarificação.*
- *C₈₈ – Interface Aquecedor – Interface Aquecedor 1-1, Interface Aquecedor 1-2, ..., Interface Aquecedor 3-4.*
- *C₈₉ – Série de Aquecedores – Série 1, Série 2 e Série 3.*
- *C₉₀ – Gerenciador Aquecimento – Gerenciador Aquecimento.*
- *C₉₁ – Interface Clarificador-Filtro – Interface C-F 1, Interface C-F 2 e Interface C-F 3.*
- *C₉₂ – Supervisor Tanque Bomba Clarificação – Supervisor Tanque Bomba Clarificação.*
- *C₉₃ – Gerenciador Clarificação – Gerenciador Clarificação.*
- *C₉₄ – Supervisor Tanque Bomba Evaporação – Supervisor Tanque Bomba Evaporação.*
- *C₉₅ – Interface Variadores de Potência Evaporação – Interface VP Evaporação.*
- *C₉₆ – Gerenciador Evaporação – Gerenciador Evaporação.*
- *C₉₇ – Interface Cozedor – Interface Cozedor 1, Interface Cozedor 2, ... Interface Cozedor 10.*
- *C₉₉ – Gerenciador Cozimento A – Gerenciador Cozimento A.*
- *C₁₀₀ – Gerenciador Cozimento B – Gerenciador Cozimento B.*
- *C₁₀₁ – Gerenciador Cozimento C – Gerenciador Cozimento C.*
- *C₁₀₂ – Gerenciador Cozimento Global – Gerenciador Cozimento Global.*
- *C₁₀₃ – Interface Centrífuga – Interface Centrífuga 1, Interface Centrífuga 2, ... Interface Centrífuga N.*
- *C₁₀₅ – Gerenciador Centrifugação A – Gerenciador Centrifugação A.*
- *C₁₀₆ – Gerenciador Centrifugação B – Gerenciador Centrifugação B.*
- *C₁₀₇ – Gerenciador Centrifugação C – Gerenciador Centrifugação C.*
- *C₁₀₈ – Gerenciador Centrifugação Global – Gerenciador Centrifugação Global.*
- *C₁₀₉ – Supervisor Tanque Xarope – Supervisor Tanque Xarope.*
- *C₁₁₀ – Supervisor Tanque Massa – Supervisor Tanque Massa A, Supervisor Tanque Massa B, Supervisor Tanque Massa C.*
- *C₁₁₁ – Supervisor Tanque Magma – Supervisor Tanque Magma B, Supervisor Tanque Magma C.*
- *C₁₁₂ – Supervisor Tanque Mel – Supervisor Tanque Mel A, Supervisor Tanque Mel B, Supervisor Tanque Mel C.*
- *C₁₁₃ – Interface Caminhão de Mel C – Interface CMC 1, Interface CMC 2, ..., Interface CMC N.*
- *C₁₁₄ – Interface Secador Empacotador – Interface Secador-Empacotador.*

B.1.4. Atividade 5 – Construção dos Diagramas de Seqüência ou Colaboração

Apresenta-se a seguir um possível Diagrama de Seqüência para o Caso de Uso ‘Descarregar caminhão c/ caçamba basculante’ (Fig. B.6). Considera-se o caso onde o caminhão é destinado ao fosso.

Fig. B.6. Diagrama de Seqüência do Caso de Uso ‘Descarregar caminhão c/ caçamba basculante’.

B.1.5. Atividade 6 – Modelagem das Classes em redes PTD-OO

Os modelos das classes C_7 , C_{10} , C_{13} , C_{74} , C_{75} e C_{76} foram apresentados no Capítulo 7 e portanto não estão incluídos neste anexo.

Ambas as classes C_2 - Caminhão c/ Caçamba Basculante e C_3 - Caminhão c/ Correntes são definidas como especialização da classe C_1 - Caminhão Externo.

C_1 - Caminhão Externo (Fig. B.7)

A chegada de caminhões a usina ocorre através da chamada do método associado a t_{1_1} por um elemento externo. Uma vez na usina, o Caminhão Externo informa sua chegada e seu volume ao sistema supervisor (t_{2_1}), e aguarda ordem para descarregar na Mesa (t_{3_1}) ou no Fosso (t_{4_1}). O percurso da entrada da usina até a Mesa ou Fosso tem durações de K_{0_C1} e K_{0_C2} . Quando o Caminhão estiver pronto e a Mesa ou Fosso estiver livre (disparo de t_{5_1} e t_{6_1}) inicia-se o descarregamento.

Fig. B.7. Modelo da classe C₁ - Caminhão Externo.**C₂ - Caminhão c/ Caçamba Basculante (Fig. B.8)**

Uma vez posicionado o Caminhão c/ Caçamba Basculante, solicita-se o posicionamento do respectivo Guindaste ($t_{11,2}$), abre-se a lateral ($t_{12,2}$), prende-se o gancho do Guindaste ($t_{13,2}$). A cana é então despejada. A vazão de cana despejada (Q_{CB}) é proporcional ao ângulo da caçamba (α_{CB}), que por sua vez varia na mesma velocidade do cabo do Guindaste ($V_{G,14,C5}$).

C₃ - Caminhão c/ Correntes (Fig. B.9)

A assinatura do método ‘Chegada na usina de Caminhão Externo’ ($t_{1,3}$) neste caso recebe como entrada, além do volume de cana no caminhão (V_C), também o número de feixes (n_{fCC}), a partir dos quais é possível determinar o volume de cada feixe (V_{fCC}). Durante o descarregamento, o gancho do Guindaste é preso ao feixe e retirado do caminhão ($t_{12,3}$, $n_{fCC} = n_{fCC} - 1$). Quando todos os feixes foram retirados ($n_{fCC} = 0$), encerra-se o descarregamento ($t_{13,3}$).

C₄ - Caminhão c/ Garras (Fig. B.10)

Quando solicitado pelo disparo do método ‘Transfere cana c/ Caminhão c/ Garras’ ($t_{1,4}$), o caminhão inicia o transporte de n_{fCG} feixes para produção. O número de feixes é recebido como variável de entrada do método associado a $t_{1,4}$. Cada feixe corresponde a volume de cana de $K_{V,fCG}$ (capacidade de transporte do Caminhão c/ Garras). Os trajetos estacionamento-fosso, fosso-produção, produção-fosso e produção-estacionamento tem durações de $K_{\theta,CG1}$, $K_{\theta,CG2}$, $K_{\theta,CG3}$ e $K_{\theta,CG4}$, respectivamente.

Fig. B.8. Modelo da classe C₂ - Caminhão c/ Caçamba Basculante.**C₅: Guindaste (Fig. B.11)**

Este modelo apresenta a sequência de movimentos que devem ser executados no caso do descarregamento dos dois tipos de caminhão. Uma vez realizado o descarregamento de um tipo, se o seguinte for de outro tipo, deve-se providenciar a troca das garras. Considerou-se que todos os movimentos tem a mesma duração (K_{θ_G}). A velocidade do cabo é compartilhada (v_G). No descarregamento do Caminhão c/ Correntes, o volume de cana liberado em cada feixe é V_{fG} .

C₆ - Fosso (Fig. B.12)

O Fosso pode receber cana do descarregamento de Caminhões c/ Correntes, modelado como evento discreto (disparo de $t_{1,6}$, volume despejado V_{CF}), e do descarregamento de Caminhões c/ Caçamba Basculante, modelado através do sistema de equações associado a $p_{2,6}$. A cana é retirada do Fosso pelo Caminhão c/ Garras através do método 'Carrega cana do Fosso' ($t_{3,6}$). O volume de cana no Fosso é V_F .

Fig. B.9. Modelo da classe C₃ - Caminhão com Correntes. Fig. B.10. Modelo da classe C₄ – Transportador c/ Garras.

Fig. B.11. Modelo da classe C_5 - Guindaste. Fig. B.12. Modelo da classe C_6 - Fosso. C_8 - Chuveiro (Fig. B.13)

Quando o *Chuveiro* está no estado ‘Ligado’ a cana proveniente da respectiva *Mesa* é lavada.

Fig. B.13. Modelo da classe C_8 - Chuveiro. C_9 - Variador de Velocidade (Fig. B.14)

Esta classe permite a variação da velocidade (v_{VV}) da esteira ou mesa entre três valores constantes (K_{v_VV1} , K_{v_VV2} , K_{v_VV3}).

Fig. B.14. Modelo da classe C_9 - Variador de Velocidade.

A classe C_{10} - Esteira utiliza a mesma aproximação para o cálculo das propriedades de um fluxo de material ao longo de um transportador que a classe C_{11} - Esteira Bipartida (apresentada no Capítulo 7). A classe C_{15} - Esteira 2 - Esteira 3 é então resultado da composição de 2 classes C_{10} e de uma terceira classe C_{14} - Limitador de Vazão. Estas relações são ilustradas no Diagrama de classes da Fig. B.15.

Fig. B.15. Diagrama de classes p/ C_{13} e C_{15} . C_{12} - Preparador

O modelo desta classe foi apresentado como parte do modelo da classe C_{13} no Capítulo 7.

 C_{15} - Esteira 2-Esteira 3 (Fig. B.16)

O limitador de vazão permite que a vazão destinada ao difusor (m_{LV1}), não ultrapasse o valor máximo de K_{m_LV} . Neste caso o excesso de cana (m_{LV2}) na saída da Esteira 2 é enviado de volta pela Esteira 3 ao início da Esteira 2.

Fig. B.16. Modelo da classe C₁₅ - Esteira 2-Esteira 3.**C₁₆ - Válvula de Água (Fig. B.17)**

A Válvula de Água pode estar ‘Aberta’ ou ‘Fechada’. Quando aberta pode assumir 3 posições, fornecendo em cada caso uma vazão de água constante (m_{VA}).

Fig. B.17. Modelo da classe C₁₆ - Válvula de Água.

A classe C₂₂ - Difusor é resultado da composição apresentada na Fig. B.18, cujas classes compartilham variáveis em ciclo fechado. Para o objeto Difusor, as 14 instâncias da classe C₁₈ – Recipiente Bomba nele contidas são chamadas RB1, RB2-3, RB4, RB5, ..., RB14 e MD.

Fig. B.18. Composição da classe C_{22} . C_{17} - Aquecedor (Fig. B.19)

O *Aquecedor* tem dois estados discretos: 'On', cujo equacionamento é definido de acordo com o apresentado anteriormente, e 'Off', onde a temperatura de saída do caldo (T_{AQ}) é igual a temperatura de entrada (T_{AMB}) – correspondente a temperatura ambiente. T_V é a temperatura do vapor fornecido ao aquecedor e também é um dado de entrada. Quando o Aquecedor está 'On', a temperatura de saída do caldo é dada pela equação abaixo (Hugot, 1986), onde m_{AQ} é o fluxo em massa de caldo e K_{T_AQ} é uma constante auxiliar:

$$T_{AQ} = T_V - (T_V - T_{AMB}) \cdot \exp(-K_{T_AQ}/m_{AQ})$$

Fig. B.19. Modelo da classe C_{17} - Aquecedor. C_{18} - Válvula de caldo (Fig. B.20)

Esta classe é puramente contínua e é modelada pelo seguinte sistema de equações, onde a posição da válvula $P_{V.11.C79}$ é determinada por um objeto do sistema supervisório:

Fig. B.20. Modelo da classe C_{18} - Válvula de Caldo. C_{19} - Moenda (Fig. B.21)

Para a moenda, tem-se que o fluxo em massa de caldo produzido (m_{c_MD}) é dado pelas equação abaixo, onde K_{α_MD} é o coeficiente de extração da moenda, K_{fb_MD} é porcentagem de fibra na cana (considerada constante), e m_{b_T14} é o fluxo em massa de bagaço que chega à moenda:

$$m_{c_MD} = K_{\alpha_MD} \cdot m_{b_T14} \cdot (1 - K_{fb_MD})$$

A quantidade de açúcar presente no caldo não é alterada: $A_{c_MD} = A_{cb_T14}$.

Fig. B.21. Modelo da classe C₁₉ - Moenda.**C₂₀ - Recipiente-Bomba (Fig. B.22)**

A vazão de um *Recipiente-Bomba* (m_{TBi}) do difusor é determinada em função da potência da bomba P_{tRBi} , determinada por um PID em função do volume de caldo no correspondente recipiente do difusor (V_{RBi}). A capacidade do tanque é dada por K_{V_RBi} .

Fig. B.22. Modelo da classe C₂₀ - Tanque-Bomba.**C₂₁ - Transportador (Fig. B.23)**

Para modelagem do transportador, este foi dividido em 14 seções, correspondentes aos 14 recipientes que coletam o caldo de cana que atravessa o transportador.

Para uma determinada seção i, os valores da porcentagem de açúcar em peso no caldo que atravessa a camada de cana (A_{c_Ti}) e da porcentagem de açúcar no caldo no interior do bagaço (A_{cb_Ti}) são dados pelas equações abaixo, onde x é a distancia horizontal até o início da seção e y é a distancia vertical até a superfície da camada de cana.

P/ y=0 (superfície da camada de cana):

$$A_{cb_Ti}(x,0) = A_{c_Ti+2} + [A_{cb_Ti}(0,0) - A_{c_Ti+2}] * \exp(C_{1_Ti} * x)$$

P/ y>0:

$$A_{cb_Ti}(x,y) = A_{cb_Ti}(x,0) - C_{2_Ti} * [A_{c_Ti}(x,y) - A_{c_Ti+2}]$$

$$A_{c_Ti}(x,y) = A_{c_Ti+2} + [A_{cb_Ti}(x,0) - A_{c_Ti+2}] / (1 + C_{2_Ti}) * \exp(-C_{1_Ti} * x) * (1 - \exp(C_{3_Ti} * y))$$

As variáveis das equações acima são calculadas por:

$$C_{1_Ti} = C_{0_Ti} * m_{c_Ti} * m_{b_Ti} * K_{C1_T} / (m_{cb_Ti} * K_{L_T}^2 * K_{v_T}^2)$$

$$C_{2_Ti} = C_{1_Ti} * v_T / C_{0_Ti}$$

$$C_{3_Ti} = - C_{0_Ti} * (1 + C_{2_Ti}) / K_{v_T}$$

$$P/i = 1 \quad C_{0_Ti} = (C_{P.I1.C12} + C_{P.I2.C13} + C_{AQ}) * K_{C0_T},$$

$$P/i \neq 1 \quad C_{0_Ti} = (C_{P.I1.C12} + C_{P.I2.C13}) * K_{C0_T},$$

$$n_{cb_Ti} = m_{b_Ti} * (100 - K_{fb_T})$$

$$A_{c_Ti} = 1/K_{L_T} * \int A_{c_Ti}(x, K_{H_T}).dx$$

Nas equações acima, tem-se que:

C_{0_Ti} – coeficiente de preparação total;

$C_{P.I2.C13}$ – coeficiente de preparo do picador;

$C_{P.I1.C12}$ – coeficiente de preparo do esmagador;

C_{AQ} – coeficiente de preparo do aquecedor;

v_T – velocidade do transportador / velocidade da camada de cana;

K_{C0_T} – constante auxiliar de C_0 ;

K_{C1_T} – constante auxiliar de C_1 ;

K_{v_T} – velocidade do caldo que atravessa a camada de cana (constante);

K_{L_T} – largura do recipiente (constante);

K_{H_T} – altura média da camada de cana no recipiente;

m_{c_Ti} – fluxo em massa do caldo que atravessa a camada de cana;

m_{cb_Ti} – fluxo em massa do caldo contido no bagaço;

m_{b_Ti} – fluxo em massa de bagaço (fibra+caldo);

K_{fb_T} – porcentagem de fibra na cana (considerada constante).

Na modelagem do *Transportador*, não existe interesse em calcular a quantidade de açúcar do caldo e da cana em todos os pontos x e y . Para cada seção i , determina-se apenas o valor de A_{c_Ti} e $A_{cb_Ti}(L,0)$, que são utilizados nos cálculos das seções sucessiva e precedente, pois $A_{cb_Ti+1}(0,0) = A_{cb_Ti}(L,0)$. O equacionamento apresentado, no entanto, é válido para regime permanente. É preciso considerar o atraso de tempo entre a entrada da cana no recipiente e a sua saída, e entre a saída do caldo de um recipiente e a entrada no recipiente anterior. Tem-se então as seguintes equações dinâmicas para cada recipiente, onde $A_{c\tau_Ti}$ é o valor corrigido de A_{c_Ti+2} , considerando o atraso de tempo τ_T :

$$\dot{A}_{cb_Ti} = \{[A_{c\tau_Ti} + A_{cb_Ti-1} * \exp(C_{1_Ti} * K_{L_Ti})] - A_{cb_Ti}\} / \tau_{v_T}$$

$$\dot{A}_{c\tau_Ti} = (A_{c_Ti+2} - A_{c\tau_Ti}) / \tau_T$$

$$A_{c_Ti} = A_{c\tau_Ti} * [1 + (1 - \exp(C_{3_Ti} * K_{H_T})) / (K_{L_T} + C_{2_Ti} * K_{L_T}) * (K_{L_T} * C_{1,i} - \exp(C_{1_Ti} * K_{L_T}) - 1) / C_{1_Ti}] + A_{cb_Ti-1} * [(1 - \exp(C_{3_Ti} * K_{H_T})) / (K_{L_T} + C_{2_Ti} * K_{L_T})]$$

$$\dot{m}_{c_Ti} = (m_{c_Ti+2} - m_{c_Ti}) / \tau_T$$

Fig. B.23. Modelo da classe C₂₁ - Transportador.**C₂₃ - Controle Local do Difusor (Fig. B.24)**

Esta classe realiza a sequência de comandos necessários para ligar ou desligar o Difusor. As transições $t_{1_20_Ii}$ e $t_{2_20_Ii}$ indicam os métodos da instância i da classe Recipiente-Bomba que compõe o Difusor.

C₂₄ - Tanque-Bomba (Fig. B.25)

A classe C₂₄ – Tanque-Bomba - Sulfitação é semelhante à classe C₁₈ - Recipiente-Bomba do Difusor, mas aqui a potência da bomba não é determinada por um PID, mas é uma variável externa de um objeto da classe C₂₅ - Variador de Potência.

C₂₅ - Variador de Potência (Fig. B.14)

Esta classe permite a variação da potência (P_{t_VP}) da bomba entre três valores constantes (K_{Pt_VP1} , K_{Pt_VP2} , K_{Pt_VP3}).

C₂₆ - Compressor (Fig. B.27)

Basicamente, quando o compressor está ligado, o ar é fornecido a pressão K_{p_C} .

Fig. B.24. Modelo da classe C₂₃ - Controle Local do Difusor. Fig. B.25. Modelo da classe C₂₄ - Tanque-Bomba. Fig. B.26. Modelo da classe C₂₅ - Variador de Potencia. Fig. B.27. Modelo das classe C₂₆ - Compressor.

C_{27} - Caixa de Cal (Fig. B.28)

Cada bandeja de cal colocada na caixa é suficiente para secar o ar durante um intervalo de $\theta_{\max}$. Depois de atingir este intervalo, a cal é considerada ‘saturada’ (p_{6_18}).

Fig. B.28. Modelo da classe C_{27} - Caixa de cal.

Como no caso da classe C_{22} - Difusor, o objeto da classe C_{32} - Sulfitador resultado da composição de um objeto de cada uma das seguintes classes: C_{28} - Válvula de Ar Comprimido, C_{29} - Forno Rotativo e C_{30} - Coluna de Sulfitação.

C_{28} - Válvula de Ar Comprimido (Fig. B.29)

A admissão de ar comprimido no forno é determinada por uma válvula que é controlada por um PID em função do pH do caldo na saída do processo.

Fig. B.29. Modelo da classe C_{28} - Válvula de Ar Comprimido.

C_{29} - Forno Rotativo (Fig. B.30)

O volume de enxofre no forno é dado por V_{SO2_FR} , que é consumido proporcionalmente ao fluxo de ar ($m_{a_VAC.I1.C28}$). Sempre que uma carga de enxofre é adicionada ao forno, o volume aumenta de um fator constante K_{V_FR} .

Fig. B.30. Modelo da classe C₂₉ - Forno Rotativo.**C₃₀ - Coluna de Sulfitação (Fig. B.31)**

O modelo da coluna de sulfitação é apenas contínuo. A coluna é um elemento passivo, sempre que houver fluxo de caldo e de ar, ocorrerá a mistura. Não existem comandos ou sinais de controle. A vazão de caldo é determinada pela bomba e a vazão de ar pela válvula de ar comprimido. O pH do caldo sulfitado é determinado pela fórmula abaixo:

$$pH_{CS} = -\log \left[\frac{(m_{a_VAC.I1.C28}/\rho_a * K_{SO2} + m_{CS}/\rho_c * 10 * (-K_{pHc}))}{(m_{CS}/\rho_c)} \right]$$

Nesta fórmula, tem-se que:

pH_{CS} , K_{pHc} – pH do caldo sulfitado e pH do caldo antes da sulfitação;

K_{SO2} – constante relacionada ao número de mols de SO₂ no ar insuflado;

$m_{a_VAC.I1.C28}$ – vazão de ar que atravessa o sulfitador;

m_{CS} – vazão em massa de caldo que atravessa o sulfitador;

ρ_a , ρ_c – densidade do ar e do caldo.

Fig. B.31. Modelo da classe C₃₀ - Coluna de Sulfitação.**C₃₂ - Trocador de Calor (Fig. B.32)**

Considera-se que o Trocador de Calor pode assumir dois estados: 'On' e 'Off'.

Fig. B.32. Modelo da classe C₃₂ - Trocador de calor.

C₃₃ - Tambor Rotativo (Fig. B.33)

No tambor rotativo, a vazão de água ($m_{H_2O_TR}$) é função da posição da válvula de admissão de água (P_{TR}), que é determinada em função da vazão de cal (considerada constante – K_{mCaO_TR}) e do Grau Baumé desejado (K_{GBE_TR}). Quando a posição desejada da válvula é superior a 1 significa que a vazão de água disponível não é suficiente para obter o Grau Baumé desejado. Neste caso, de acordo com os valores fornecidos em (Hugot, 1986), a seguinte função fornece o Grau Baumé da mistura:

$$G_{BE_TR} = 79,909 * (m_{H_2O}/K_{mCaO_TR})^{-0,898}$$

A densidade da mistura obtida (ρ) é dada por:

$$\rho_{lc_TR} = 0,0081 * G_{BE_TR} + 0,9968$$

Fig. B.33. Modelo da classe *C₃₃ - Tanque Rotativo*.

A classe *C₃₆ - Calagem* resultado da composição de um objeto da classe *C₃₄ - Tanque de Leite de Cal* e um da classe *C₃₆ - Tanque Misturador*.

C₃₄ - Tanque de Leite de Cal (Fig. B.34)

Nesta classe, a vazão de saída do tanque (m_{TL}) é determinada em função da posição da válvula (P_{TL}), que por sua vez é determinada por um PID em função do pH do caldo no tanque misturador ($pH_{TM.I1.C35}$).

A classe *C₃₆ - Tanque Misturador* é semelhante a classe *C₂₄ - Tanque Bomba*, onde as interfaces foram alteradas (a vazão de entra é $m_{TL.I1.C34} + m_{CS.I2.C30}$), e onde, além do volume (V_{TB}), determina-se também o pH (pH_{TB}) e a densidade (ρ_{TB}) da mistura. Ambas as classes podem ser definidas como especificação de uma terceira classe *C₃₅ - Tanque Bomba*.

Fig. B.34. Modelo da classe C₃₄ - Tanque de Leite de Cal.C₃₅ - Tanque-Bomba (Fig. B.35) Fig. B.35. Modelo da classe C₃₅ - Tanque-Bomba.C₃₆ - Tanque Misturador (Fig. B.36) Fig. B.36. Modelo da classe C₃₆ - Tanque Misturador.C₃₈ - Divisor de fluxo – Aquecimento (Fig. B.37)

O *Divisor de Fluxo* é responsável por guardar a informação do número de séries de aquecedores em uso, de forma a possibilitar a determinação do fluxo de caldo em cada série.

Se o fluxo de saída imposto pela bomba do tanque misturador é não nulo e todas as *Válvulas On/Off* estão fechadas ($n_{DV}=0$) ocorre falha no sistema.

Fig. B.37. Modelo da classe C₃₈ - Divisor de Fluxo - Aquecimento.

C₃₉ - Válvula On/Off (Fig. B.38)

Esta é a válvula que se encontra na entrada de cada série de aquecedores (Fig. 7.13 do Capítulo 7). Quando está ‘Aberta’ os aquecedores da respectiva série estão sendo utilizados.

Fig. B.38. Modelo da classe C₃₉ - Válvula On/Off.

C₄₀ - Válvula 2 Posições – Aquecedor (Fig. B.39)

Esta classe modela o comportamento de um aquecedor e sua respectiva válvula para cada série. Ela é, portanto, o resultado da composição de um objeto *Aquecedor* com um objeto *Válvula 2 Posições*. Quando a válvula está no estado ‘P2’ há fluxo de caldo através do aquecedor. Quando o aquecedor está no estado ‘On’ o fluxo de caldo é aquecido.

No caso dos primeiros aquecedores de cada série $x_1=1$ e $x_2=0$, portanto o fluxo de entrada no aquecedor é de $m_{V2P_2} = x_1 * m_{VOO.I1.C39}$ que corresponde a saída do *Divisor de Fluxo*. No caso dos demais aquecedores, tem-se que $x_1=0$ e $x_2=1$, portanto $m_{V2P_2} = x_2 * m_{V2P_1.I2.C40}$, que corresponde a saída do aquecedor precedente. O mesmo é válido para temperatura de entrada do caldo, que no caso do primeiro aquecedor equivale a temperatura ambiente (T_{AMB}) e nos demais casos à temperatura na saída do aquecedor precedente ($T_{AQ.I2.C40}$).

A classe C₄₇ – *Clarificação* é definida pela composição ilustrada na Fig. B.40, cujos objetos compartilham variáveis em ciclo fechado, pois o caldo resultante da filtragem do lodo retorna ao tanque de caldo a ser clarificado. Os 3 objetos da classe C₄₄ – *Clarificador* considerados para instância Clarificação são chamados de (Clarificador 1, Clarificador 2 e Clarificador 3). Os 3 objetos de C₄₆ – *Filtro* são chamados de Filtro 1, Filtro 2 e Filtro 3.

Fig. B.39. Modelo da classe C₄₀ - Válvula 2 Posições – Aquecedor. Fig. B.40. Composição da classe C₄₅ – Clarificação.**C₄₁ - Tanque-Bomba Clarificação (Fig. B.41)**

A classe C₄₁ – Tanque-Bomba Clarificação é uma especialização da classe C₃₅ – Tanque-Bomba e faz interface com objetos da classe C₄₀ - Válvula de 2P – Aquecedor e C₄₄ - Filtro.

Fig. B.41. Modelo da classe C₄₁ - Tanque-Bomba Clarificação.

A classe C₄₃ - Divisor de Fluxo Clarificação é semelhante a classe C₃₇ - Divisor de Fluxo, mas ao invés de fazer interface com um objeto da classe C₃₅ – Tanque Misturador, o faz com um objeto da classe C₄₁ - Tanque-Bomba - Clarificação. Ambas podem então ser definidas como especialização de uma terceira classe C₄₂ – Divisor de Fluxo.

C₄₂ – Divisor de Fluxo (Fig. B.41)

Fig. B.42. Modelo da classe *C₄₂ - Divisor de Fluxo*.

C₄₃ - Divisor de Fluxo - Clarificação

Neste caso a função de habilitação e_{2_42} e o vetor de variáveis externas $X_{ext_c_42}$ correspondem a e_{2_43} : $m_{TB.I1.C41} > 0$ AND $n_{DF} = 0$ e $X_{ext_c_43} = \{m_{TB.I1.C41}\}$.

C₄₄ – Clarificador (Fig. B.43)

Quando o clarificador está no estado ‘Enchendo’ o fornecimento de caldo clarificado (m_{c_CL}) e de lodo (m_{l_CL}) é nulo. No estado ‘Normal’ o volume no clarificador permanece constante. O clarificador pode ser desligado tanto cheio quanto vazio.

Fig. B.43. Modelo da classe *C₄₄ - Clarificador*.

C₄₅ - Divisor de Lodo

Esta classe também é uma especialização da classe *C₄₂*. Neste caso a função de habilitação e_{2_42} e os vetores de variáveis externas X_{ext_42} e internas X_{int_42} correspondem a e_{2_45} : $(m_{l_CL.I1.C44} + m_{l_CL.I2.C44} + m_{l_CL.I3.C44}) > 0$ AND $n_{DF} = 0$, $X_{ext_45} = \{m_{l_CL.I1.C44}, m_{l_CL.I2.C44}, m_{l_CL.I3.C44}\}$ e $X_{int_45} = \{l_1, l_2, l_3\}$.

C₄₆ - Filtro de Lodo

Esta classe modela a extração de caldo (m_{c_F}) e produção de torta (m_{t_F}) a partir do lodo proveniente dos clarificadores.

Fig. B.44. Modelo da classe *C₄₆ - Filtro de Lodo*.

A classe *C₅₁ – 1º Efeito* é definida pela composição de 1 objeto (Tanque 1º Efeito) da classe *C₄₇ - Tanque-Bomba 1º. Efeito*, um objeto (Divisor de Fluxo 1º. Efeito) da classe *C₄₈ - Divisor de Fluxo Evaporação*, e 3 objetos (Corpo 1-1, Corpo 2-1 e Corpo 3-1) da classe *C₅₀ - Corpo 1º Efeito* (que é uma especialização da classe *C₄₉ - Corpo A*).

C₄₇ - Tanque-Bomba 1º. Efeito (Fig. B.45)

Esta classe é uma especialização da classe C35, onde o fluxo de entrada é determinado pela soma dos fluxos provenientes dos clarificadores (*C₄₄*) acrescida dos eventuais fluxo de retorno dos corpos do 1º Efeito.

Fig. B.45. Modelo da classe *C₄₇ - Tanque-Bomba 1º Efeito*.

C₄₈ – Divisor de Fluxo Evaporação

Esta classe também é uma especialização da classe *C₄₂*. Neste caso a função de habilitação *e_{2_42}* e o vetor de variáveis externas *X_{ext_42}* são substituídos por *e_{2_48}*: $m_{TB.I1.C35} > 0$ AND $n_{DF} = 0$ e $X_{ext_48} = \{m_{TB.I1.C53}\}$.

C₄₉ – Corpo A (Fig. B.47)

Para cada corpo do evaporador pode-se identificar 3 estados principais: enchendo, volume constante e esvaziando. O equacionamento de cada fase é feito através dos balanços de massa e energia no corpo (Cadet et al, 1999), (Elhaq; Giri; Unbehauen, 1999) e (Jesus; Almeida, 1999).

A Fig. B.46 apresenta a nomenclatura para as entradas e saídas em um corpo.

Fig. B.46. Nomenclatura para um corpo.

A seguir apresenta-se o equacionamento para cada estado. Considera-se que todo o vapor de entrada é condensado ($m_{v_in} = m_{w_out}$).

Enchendo

Quando um corpo é posto em operação, após a manutenção, a saída de caldo permanece bloqueada até atingir o volume desejado:

$$m_{c_out} = 0; m_{c_out} = 0;$$

Considerando que $m_{v_in} = m_{w_out}$, o balanço de massa é representado pela seguinte equação, onde *M* é a quantidade de massa no corpo:

$$\dot{M} = m_{c_in} - m_{v_out} \quad (1)$$

Sendo *B_M* o Brix (% em massa de açúcar e impurezas solúveis) do caldo no corpo e *B_{in}* o Brix do caldo de entrada, o balanço de massa de açúcar é dado por:

$$\frac{d(M \cdot B_M)}{dt} = \dot{M} \cdot B_M + M \cdot \dot{B}_M = m_{c_in} \cdot B_{in} \quad (2)$$

O balanço de energia é dado por:

$$\frac{d(M \cdot h_M)}{dt} = \dot{M} \cdot h_M + M \cdot \dot{h}_M = m_{c_in} \cdot h_{c_in} + m_{v_in} \cdot \lambda_{v_in} - m_{v_out} \cdot h_{v_out} \quad (3)$$

Na equação acima tem-se que:

$$h_M = \text{entalpia do caldo no corpo}$$

h_{c_in} = entalpia do caldo entrando no corpo

λ_{v_in} = calor latente de vaporização, liberado pela condensação do vapor de entrada (m_{v_in})

h_{v_out} = entalpia do vapor saindo do corpo (m_{v_out}), gerado pela evaporação da água no caldo.

O calor latente de vaporização (λ_{v_in}) é dado por em kJ/kg pela equação abaixo, onde T_{v_in} é a temperatura de entrada do vapor no corpo, em °C:

$$\lambda_{v_in} = 2501,119 - (2,37553 \cdot T_{v_in}) + (5,5 \cdot 10^{-4} \cdot T_{v_in}^2) - (1,26 \cdot 10^{-5} \cdot T_{v_in}^3) \quad (4)$$

A entalpia h_M é dada, em kJ/kg pela equação abaixo, onde T_M está em °C:

$$h_M = 4,1253 \cdot T_M - 0,024804 \cdot B_M \cdot T_M + 6,7 \cdot 10^{-5} \cdot B_M \cdot T_M^2 + 1,8691 \cdot 10^{-3} \cdot T_M^2 - 9,271 \cdot 10^{-6} \cdot T_M^3 \quad (5)$$

A entalpia (h_{v_out}) do vapor saturado m_{v_out} que deixa o corpo é dada, em kJ/kg pela equação abaixo, onde T_{v_out} está em °C:

$$h_{v_out} = 2501,179 + 1,822 \cdot T_{v_out} + 1,283 \cdot 10^{-4} \cdot T_{v_out}^2 - 9,088 \cdot 10^{-6} \cdot T_{v_out}^3 \quad (6)$$

A temperatura do vapor saturado (T_{v_out}) é a temperatura de ebulição do caldo, que é a mesma do caldo no corpo (T_M), que está prestes a evaporar. Portanto:

$$T_{v_out} = T_M \quad (7)$$

A temperatura T_M é calculada em função da temperatura de ebulição da água para pressão do corpo (K_{Teb}) e da concentração de açúcar no caldo (B_M). Ela é dada por:

$$T_M = K_{Teb} + 6,064 \cdot 10^{-5} \cdot [(273,15 + K_{Teb})^2 \cdot B_M^2 / (374,3 - K_{Teb})^{0,38}] \cdot [5,84 \cdot 10^{-7} \cdot (B_M - 40)^2 + 0,00072] \quad (8)$$

Observa-se que K_{Teb} é considerada constante e conhecida, pois depende apenas da pressão no corpo.

Finalmente, o volume (V_M) de caldo no corpo é dado por:

$$\dot{V}_M = m_{c_in} \cdot \rho_{c_in} - m_{v_out} \cdot \rho_{H_2O} \quad (9)$$

Nesta equação ambas a densidade do caldo na entrada do corpo (ρ_{c_in}) e a densidade da água (ρ_{H_2O}) são conhecidas.

Tem-se então um sistema de 9 equações e 9 incógnitas (T_{v_out} , T_M , h_{v_out} , h_M , λ_{v_in} , M , B_M , m_{v_out} e V_M), onde as variáveis de entrada são m_{c_in} , h_{c_in} , m_{v_in} , T_{v_in} .

Volume Constante

Após o enchimento do corpo, o volume é mantido constante através da regulação do volume de saída. Este é o modo normal de operação do evaporador. Tem-se então que:

$$m_{c_out} \neq 0; m_{c_out} = 0;$$

$$V_M = \text{cte} \Rightarrow \dot{V}_M = 0$$

Para este caso, a equação de balanço de massa é reescrita como:

$$\dot{M} = m_{c_in} - m_{v_out} - m_{c_out} \quad (1)$$

Considera-se que a concentração do caldo que sai do corpo é igual a concentração do açúcar no corpo (B_M). Assim, o balanço de massa de açúcar é dado por:

$$\dot{M} * B_M + M * \dot{B}_M = m_{c_in} * B_{in} - m_{c_out} * B_M \quad (2)$$

O balanço de energia é dado por:

$$\dot{M} * h_M + M * \dot{h}_M = m_{c_in} * h_{c_in} + m_{v_in} * \square_{v_in} - m_{v_out} * h_{v_out} - m_{c_out} * h_M \quad (3)$$

As equações (4), (5), (6), (7), (8) e (9) não são alteradas:

O volume de caldo constante impõem ainda a seguinte restrição, no lugar da equação (10) do caso Enchendo:

$$m_{c_in} * \rho_{c_in} - m_{v_out} * \rho_{H_2O} - m_{c_out} * \rho_{c_out} = 0 \quad (10)$$

A densidade do caldo na saída (ρ_{c_out}) é considerada igual a densidade do caldo no corpo (ρ_M), e é dada por:

$$\rho_{c_out} = \rho_M \quad (11)$$

$$\rho_M = M/V_M \quad (12)$$

Tem-se agora um sistema de 12 equações e 12 incógnitas (T_{v_out} , T_M , h_{v_out} , h_M , h_{c_in} , λ_v , M , B_M , m_{v_out} , m_{c_out} , ρ_{c_out} e ρ_M).

Esvaziando

Nesta configuração, a entrada de vapor e de caldo é cortada e o volume de caldo presente no tanque é esvaziado como caldo de retorno ao tanque precedente (m_{c_out}) a uma taxa constante K_{c_out} . Tem-se as seguintes equações:

$$m_{c_out} = K_{c_out}; m_{c_out} = 0;$$

$$B_M = \text{cte} \Rightarrow \dot{B}_M = 0$$

$$h_M = \text{cte} \Rightarrow \dot{h}_M = 0$$

Tendo como base o equacionamento apresentado, o modelo da classe C_{49} – *Corpo* é apresentado na Fig. B.47.

Fig. B.47. Modelo da classe C₄₉ – Corpo A.**C₅₀ – Corpo 1º Efeito (Fig. B.48)**

Esta classe é uma especialização da classe C₄₉.

No caso do 1º. Efeito, durante o período de operação normal, o fluxo de entrada e de saída de caldo é mantido constante e a entrada de vapor é regulada por um PID em função do Brix de saída do caldo.

A classe C₅₅ – 2º. Efeito é definida pela composição de 1 objeto (Tanque 2º Efeito) da classe C₅₂ – Tanque-Bomba 2º. Efeito, um objeto (Divisor de Fluxo 2º. Efeito) da classe C₄₈ – Divisor de Fluxo Evaporação, um objeto (Divisor de Vapor 2º. Efeito) da classe C₅₃ – Divisor de Vapor 2º. Efeito, e 4 objetos (Corpo 1-2, Corpo 2-2 e Corpo 3-2) da classe C₅₄ – Corpo 2º Efeito.

Fig. B.48. Modelo da classe C₅₀ – Corpo 1º Efeito.**C₅₂ - Tanque-Bomba 2º. Efeito (Fig. B.49)**

Esta classe também é uma especialização da classe C₃₅. Neste caso o fluxo de entrada do tanque é a soma dos fluxos provenientes do 1º Efeito, acrescida dos fluxos de retorno do 2º Efeito.

Fig. B.49. Modelo da classe C₅₂ - Tanque-Bomba 2º Efeito.**C₅₃ – Divisor de Vapor 2º. Efeito (Fig. B.50)**

Esta classe também é uma especialização da classe C₄₂. Ela deve determinar a temperatura e a vazão média de vapor fornecido a cada corpo do 2º Efeito.

Fig. B.50. Modelo da classe C₅₃ – Divisor de Vapor 2º Efeito.**C₅₄ – Corpo 2º Efeito (Fig. B.51)**

Esta classe é uma especialização da classe C₄₉.

No caso do 2º. Efeito o vapor é aquele produzido pelo 1º Efeito (a menos do vapor consumido por outros processos da usina). A entrada e saída de caldo são mantidas constantes.

Fig. B.51. Modelo da classe C₅₄ – Corpo 2º Efeito.

A classe C₆₂ – 3-4-5º. Efeito é definida pela composição de 1 objeto (Tanque 3º Efeito) da classe C₅₆ - Tanque-Bomba 3º. Efeito, um objeto (Divisor de Vapor 3º. Efeito) da classe C₅₇ - Divisor de Vapor 3º. Efeito, 1 objeto (Corpo 1-3) da classe C₅₈ - Corpo 3º Efeito, 1 objeto (Corpo 1-4) da classe C₆₀ - Corpo 4º Efeito e 1 objeto (Corpo 1-5) da classe C₆₁ - Corpo 5º Efeito.

Ambas as classes C₆₀ e C₆₁ são especializações de uma classe genérica C₅₉ – Corpo B).

C_{56} - Tanque-Bomba 3º. Efeito (Fig. B.52)

Esta classe também é uma especialização da classe C_{35} . Neste caso o fluxo de entrada do tanque é a soma dos fluxos provenientes do 2º Efeito, acrescida do fluxo de retorno do único corpo do 3º Efeito.

Fig. B.52. Modelo da classe C_{56} - Tanque-Bomba 3º Efeito.

C_{57} – Divisor de Vapor 3º. Efeito (Fig. B.53)

Esta classe considera a divisão de fluxo entre o corpo do 3º efeito e os cozedores.

Fig. B.53. Modelo da classe C_{57} - Divisor de Vapor 3º Efeito.

C_{58} – Corpo 3º. Efeito (Fig. B.54)

Esta classe é uma especialização da classe C_{49} , onde a entrada de caldo no corpo provém do Tanque-Bomba 2º Efeito e a entrada de vapor do Divisor de Vapor 3º Efeito.

Fig. B.54. Modelo da classe C₅₈ – Corpo 3º Efeito.**C₅₉ – Corpo B (Fig. B.55)**

Diferentemente dos 1º, 2º e 3º Corpos, os 4º e 5º Corpos recebem toda a entrada de caldo e vapor do corpo anterior. Portanto, ao contrário da classe C₄₉, esta classe não faz interface *Divisor de Fluxo* ou *Divisor de Vapor*.

Fig. B.55. Modelo da classe C₅₉ – Corpo B.**C₆₀ – Corpo 4º. Efeito (Fig. B.56)**

Esta classe é uma especialização da classe C₅₉, onde a entradas de caldo e vapor do 4º Efeito correspondem as saídas do 3º Efeito.

C₆₁ – Corpo 5º. Efeito (Fig. B.57)

Esta classe é uma especialização da classe C₅₉, onde a entradas de caldo e vapor do 4º Efeito correspondem as saídas do 3º Efeito. Além disso o 5º efeito tem a quantidade de vapor regulada em função do Brix do caldo na saída (Nielsen; Petersen; Nielsen, 1996).

Ambas as classes C₆₄ - *Tanque Xarope* e C₆₆ – *Tanque Massa* são definidas como especialização de uma terceira classe C₆₃ – *Tanque Genérico*.

Fig. B.56. Modelo da classe C₆₀ – Corpo 4º Efeito. Fig. B.57. Modelo da classe C₆₁ – Corpo 5º Efeito.**C₆₃ - Tanque Genérico (Fig. B.58)**

Esta classe determina as propriedades do caldo no tanque (volume (V_T), massa (M_T) e densidade (ρ_T)), em função das propriedades do caldo que chega ao tanque (m_E e ρ_E) e da vazão em massa na saída (m_S). O volume do tanque é K_{V_T} . Quando ocorre transbordamento ou quando o tanque está vazio, considera-se que ocorreu uma falha.

Fig. B.58. Modelo da classe C₆₃ – Tanque Genérico.**C₆₄ - Tanque Xarope (Fig. B.59)**

Além das propriedades calculadas pela classe C₆₃, neste caso é necessário também determinar o Brix (B_T) e a entalpia (h_T) do xarope no tanque. O xarope que chega ao tanque é proveniente da evaporação (m_{c_out.I1.C61}) e o que deixa o tanque é destinado aos cozedores que produzem massa do tipo A (m_{CZ_A.I2.C65}, ..., m_{CZ_A.I11.C65}).

Fig. B.59. Modelo da classe C₆₄ – Tanque Xarope.**C₆₅ – Cozedor (Fig. B.60)**

Os cozedores (cristalizadores) são equipamentos semelhantes aos corpos do evaporador mas que funcionam por bateladas (*batch*) de acordo com o seguinte ciclo (Lauret; Boyer; Gatina, 2000) e (Garcia; Acebes; Prada, 2002):

- 1- *Fazer vácuo* – atividade que despense um intervalo de tempo de $K_{0_CZ_p1}$.
- 2- *Carregar ‘pé’ até cobrir calandra* – o pé se refere a uma quantidade inicial de xarope ($K_{V_CZ_p2}$) que é adicionada à calandra. A variação da massa (M_{CZ}), o volume (V_{CZ}) e o Brix (B_{CZ}) no cozedor são dados por:

$$\dot{M}_{CZ} = m_{x_in_CZ} \quad (1)$$

$$\dot{V}_{CZ} = m_{x_in_CZ} \cdot \rho_{x_in_CZ} \quad (2)$$

$$\rho_{CZ} = M_{CZ}/V_{CZ} \quad (3)$$

$$\dot{B}_{CZ} = (-B_{CZ} \cdot \dot{M}_{CZ} + m_{x_in_CZ} \cdot B_{x_in_CZ})/M_{CZ} \quad (4)$$

$$\dot{h}_{CZ} = (-h_{CZ} \cdot \dot{M}_{CZ} + m_{x_in_CZ} \cdot h_{x_in_CZ})/M_{CZ} \quad (5)$$

- 3- *Concentrar o pé* – consiste em abrir a válvula de entrada de vapor vegetal (proveniente da evaporação – vazão constante K_{V_in}) até atingir um determinado

Brix ($K_{B_CZ_p3}$). O sistema de equações possui 10 incógnitas (M_{CZ} , $m_{v_out_CZ}$, B_{CZ} , h_{CZ} , $h_{v_out_CZ}$, $T_{v_out_CZ}$, T_{CZ} , V_{CZ} , ρ_{CZ} , λ_{v_in})

$$\dot{M}_{CZ} = -m_{v_out_CZ} \quad (1)$$

$$\dot{M}_{CZ} * B_{CZ} + M * \dot{B}_{CZ} = 0 \quad (2)$$

$$\dot{M}_{CZ} * h_{CZ} + M * \dot{h}_{CZ} = m_{v_in} * \lambda_{v_in} - m_{v_out_CZ} * h_{v_out_CZ} \quad (3)$$

$$h_{v_out_CZ} = 2501,179 + 1,822 * T_{v_out_CZ} + 1,283 \cdot 10^{-4} * T_{v_out_CZ}^2 - 9,088 \cdot 10^{-6} * T_{v_out_CZ}^3 \quad (4)$$

$$h_{CZ} = 4,1253 * T_{CZ} - 0,024804 * B_{CZ} * T_{CZ} + 6,7 \cdot 10^{-5} * B_{CZ} * T_{CZ}^2 + 1,8691 \cdot 10^{-3} * T_{CZ}^2 - 9,271 \cdot 10^{-6} * T_{CZ}^3 \quad (5)$$

$$T_{v_out_CZ} = T_{CZ} \quad (6)$$

$$\lambda_{v_in} = 2501,119 - (2,37553 * T_{v_in}) + (5,5 \cdot 10^{-4} * T_{v_in}^2) - (1,26 \cdot 10^{-5} * T_{v_in}^3) \quad (7)$$

$$T_{CZ} = T_{eb} + 6,064 \cdot 10^{-5} * [(273,15 + T_{eb})^2 * B_{CZ}^2 / (374,3 - T_{eb})^{0,38}] * [5,84 \cdot 10^{-7} * (B_{CZ} - 40)^2 + 0,00072] \quad (8)$$

$$\dot{V}_{CZ} = -m_{v_out} * \rho_{H2O} \quad (9)$$

$$\rho_{CZ} = M_{CZ} / V_{CZ} \quad (10)$$

- 4- *Diminuir vácuo* – a concentração do pé continua, mas agora a temperatura de ebulição não é mais constante, mas varia em função do tempo. Esta etapa continua até o Brix atingir o valor de $K_{B_CZ_p4}$. Aproximou-se aqui a diminuição da temperatura de ebulição por uma função linear. As demais equações permanecem as mesmas:

$$T_{eb} = K_{Teb_1} + K_{Teb_2} * \theta \quad (11)$$

- 5- *Injetar semente* – é um evento discreto que adiciona K_{M_sm} ao cozedor. A massa do cozedor (M_{CZ}) passa então a ser formada por uma parcela de semente (K_{M_sm}) e o xarope (M_x), que continua com as mesmas propriedades ($B_x = B_{CZ}$, $h_x = h_{CZ}$, etc.). Despreza-se portanto qualquer efeito da mistura.
- 6- *Aguardar tempo de estabelecimento dos grãos* – neste passo abre-se a válvula de água e continua-se a evaporação. O objetivo é da adição da água é manter taxa de evaporação e simultaneamente impedir a supersaturação. A quantidade de água adicionada deve ser equivalente àquela evaporada. A massa e o Brix do xarope portanto não são alterados, apenas a entalpia da mistura. O novo equacionamento é dado por:

$$\dot{M}_x = K_{mH2O_in_CZ} - m_{v_out_CZ} = 0 \quad (1)$$

$$\dot{M}_x * B_x + M_x * \dot{B}_x = 0 \quad (2)$$

$$\dot{M}_X * h_X + M_X * \dot{h}_X = K_{mH2O_in_CZ} * K_{hH2O_in_CZ} + m_{v_in} * \lambda_{v_in} - m_{v_out_CZ} * h_{v_out_CZ} \quad (3)$$

$$h_{v_out_CZ} = 2501,179 + 1,822 * T_{v_out_CZ} + 1,283.10^{-4} * T_{v_out_CZ}^2 - 9,088 * 10^{-6} * T_{v_out_CZ}^3 \quad (4)$$

$$h_X = 4,1253 * T_X - 0,024804 * B_X * T_X + 6,7.10^{-5} * B_X * T_X^2 + 1,8691.10^{-3} * T_X^2 - 9,271.10^{-6} * T_X^3 \quad (5)$$

$$T_{v_out_CZ} = T_X \quad (6)$$

$$\lambda_{v_in} = 2501,119 - (2,37553 * T_{v_in}) + (5,5.10^{-4} * T_{v_in}^2) - (1,26.10^{-5} * T_{v_in}^3) \quad (7)$$

$$T_X = T_{eb} + 6,064.10^{-5} * [(273,15 + T_{eb})^2 * B_X^2 / (374,3 - T_{eb})^{0,38}] * [5,84.10^{-7} * (B_X - 40)^2 + 0,00072] \quad (8)$$

7- *Alimentação dos cristais* – este passo consiste em continuar a concentração da massa no cozedor mas agora com adição de xarope ($m_{x_in_CZ}$). A massa total no cozedor passa a ser considerada como sendo formada por sacarose (M_{sc}), impureza (M_i), cristais (M_c) e água (M_a). O valor inicial destas massas é dado por:

- A massa de cristais é dada pela massa de sementes: $M_c = K_{M_sm}$.
- A parcela do xarope correspondente ao Brix é dividida em sacarose e impurezas, onde a porcentagem de impurezas é uma constante (K_{imp}): $M_{sc} = M_X * B_X * (1 - K_{imp})$ e $M_i = M_X * B_X * K_{imp}$.
- A massa de água é o restante do xarope: $M_a = M_X * (1 - B_X)$.

O equacionamento durante a adição de xarope é dado por:

$$\dot{M}_{sc} = m_{x_in_CZ} * B_{x_in_CZ} * (1 - K_{imp}) - \dot{M}_c \quad (1)$$

$$\dot{M}_i = m_{x_in_CZ} * B_{x_in_CZ} * K_{imp} \quad (2)$$

$$\dot{M}_a = m_{x_in_CZ} * (1 - B_{x_in_CZ}) - m_{v_out_CZ} \quad (3)$$

$$\dot{M}_c = K_{1_p7} * \exp(K_{2_p7} / (K_{3_p7} + T_X)) * \exp(K_{4_p7} + K_{5_p7} * M_i / M_a) \quad (4)$$

$$M_X = M_a + M_{sc} + M_i \quad (5)$$

$$B_X = (M_i + M_{sc}) / (M_a + M_{sc} + M_i) \quad (6)$$

$$(\dot{M}_a + \dot{M}_i + \dot{M}_{sc}) * h_X + M_X * \dot{h}_X = m_{v_in_CZ} * \lambda_{v_in_CZ} + m_{x_in_CZ} * h_{x_in_CZ} - m_{v_out_CZ} * h_{v_out_CZ} - \dot{M}_c * h_X \quad (7)$$

$$\lambda_{v_in_CZ} = 2501,119 - (2,37553 * T_{v_in_CZ}) + (5,5.10^{-4} * T_{v_in_CZ}^2) - (1,26.10^{-5} * T_{v_in_CZ}^3) \quad (8)$$

$$h_{v_out_CZ} = 2501,179 + 1,822 * T_{v_out_CZ} + 1,283.10^{-4} * T_{v_out_CZ}^2 - 9,088 * 10^{-6} * T_{v_out_CZ}^3 \quad (9)$$

$$h_X = 4,1253 * T_X - 0,024804 * B_X * T_X + 6,7.10^{-5} * B_X * T_X^2 +$$

$$1,8691.10^{-3} \cdot T_X^2 - 9,271.10^{-6} \cdot T_X^3 \quad (10)$$

$$T_{v_out_CZ} = T_X \quad (11)$$

$$T_X = T_{eb} + 6,064.10^{-5} \cdot [(273,15 + T_{eb})^2 \cdot B_X^2 / (374,3 - T_{eb})^{0,38}] \cdot [5,84.10^{-7} \cdot (B_X - 40)^2 + 0,00072] \quad (12)$$

$$V_{CZ} = M_a \cdot \rho_{H_2O} + M_c \cdot \rho_c + M_i \cdot \rho_i + M_{sc} \cdot \rho_{sc} \quad (13)$$

$$M_{CZ} = M_X + M_c \quad (14)$$

$$\rho_{CZ} = M_{CZ} / V_{CZ} \quad (15)$$

Este passo continua até que o volume no cozedor se reduza a K_{V_p7} .

- 8- *Evaporar água* – o processo do passo 7 continua mas agora sem adição de xarope. Este passo continua até que o volume no cozedor se reduza a K_{V_p8} . As equações que são alteradas são:

$$\dot{M}_{sc} = - \dot{M}_c \quad (1)$$

$$\dot{M}_i = 0 \quad (2)$$

$$\dot{M}_a = - m_{v_out_CZ} \quad (3)$$

$$(\dot{M}_a + \dot{M}_i + \dot{M}_{sc}) \cdot h_X + M_X \cdot \dot{h}_X = m_{v_in_CZ} \cdot \lambda_{v_in_CZ} - m_{v_out_CZ} \cdot h_{v_out_CZ} - \dot{M}_c \cdot h_X \quad (7)$$

- 9- *Despejar conteúdo* – evento discreto que despeja o conteúdo do cozedor em um tanque de massa anterior à centrífuga.
- 10- *Limpeza do cozedor* – introduz no cozedor um jato de água que é eliminado para limpeza. Esta atividade tem a duração de K_{θ_p10} .

C₆₆ - Tanque Massa (Fig. B.61)

Esta classe também é uma especialização da classe *C₆₃ – Tanque Genérico*. O índice l_{MA} , l_{MB} e l_{MC} indicam qual o tipo de massa armazenada neste tanque (ex.: se for massa do tipo A, então $l_{MA} = 1$ e $l_{MB} = l_{MC} = 0$). Diferentemente do *Tanque de Xarope*, aqui a adição de massa é um evento discreto (disparo de t_{3_66}). Do *Tanque de Massa*, a massa é destinada às centrífugas ($m_{CT_A.I1.C67}$, ..., $m_{CT_C.I10.C67}$).

C₆₇ – Centrífuga (Fig. B.62)

As centrífugas também são equipamentos que funcionam por bateladas, segundo o seguinte ciclo:

Passo 1 - *Carregamento da massa* – carrega um determinado volume de massa – é dividido em 3 etapas, onde a válvula de entrada assume 3 posições diferentes para permitir um melhor controle do volume admitido. Neste passo a centrífuga opera a baixa rotação.

Passo 2 - *Pré Lavagem* – opera com média rotação por um intervalo de tempo de $K_{\theta_CT_p2}$.

Passo 3 - *Lavagem* – opera com alta rotação e consome água para lavagem. Separa a massa inicial em mel e magma (ou açúcar). Considera-se valores médios para as porcentagens de cada componente de acordo com o tipo de massa carregada (A, B ou C).

Passo 4 - *Descarregamento* – evento discreto que envia os componentes aos respectivos tanques.

Fig. B.60. Modelo da classe C₆₅ - Cozedor.

Fig. B.61. Modelo da classe C₆₆ – Tanque Massa. Fig. B.62. Modelo da classe C₆₇ - Centrífuga.C₆₈ - Tanque Magma (Fig. B.63)

Esta classe também é uma especialização da classe C₆₃ – Tanque Genérico.

Fig. B.63. Modelo da classe C₆₈ – Tanque Magma.**C₆₉ - Tanque Mel (Fig. B.64)**

Esta classe também é uma especialização da classe C₆₃ – Tanque Genérico.

Fig. B.64. Modelo da classe C₆₉ – Tanque de Mel.**C₇₀ – Caminhão de Mel C (Fig. B.65)**

Conforme apresentado anteriormente, o mel C é um sub-produto comercializável. Esta classe modela então o carregamento de mel C em caminhões e sua saída da usina.

Fig. B.65. Modelo da classe C₇₀ – Caminhão de Mel C.**C₇₁ – Tanque de Açúcar (Fig. B.66)**

Este tanque armazena o açúcar antes da passagem pelo secador. O transporte até o secador é realizado por uma esteira.

Fig. B.66. Modelo da classe C₇₁ – Tanque de Açúcar.**C₇₂ – Secador (Fig. B.67)**

A quantidade de açúcar que deixa o Secador e prossegue para o Empacotador (m_{SC}) é proporcional a quantidade de açúcar na entrada do Secador ($m_{TA.I1.C71}$).

Fig. B.67. Modelo da classe C₇₂ – Secador.**C₇₃ – Empacotador (Fig. B.68)**

O Empacotador recebe o açúcar do Secador e armazena em sacos.

Fig. B.68. Modelo da classe C₇₃ – Empacotador.

As próximas classe apresentadas pertencem ao Sistema Supervisório da Usina Cruz Alta. Observa-se que as classes C₇₄ e C₇₆ foram apresentadas no Capítulo 7.

C_{75} – Supervisor Fosso (Fig. B.69)

Esta classe é responsável por estimar o volume de cana no Fosso (V_F), efetuando a transferência de cana para a Mesa 2 quando solicitado ($t_{1,75}$) e providenciando o descarregamento de caminhões de cana no Fosso quando a Mesa 1 está suficientemente abastecida ($t_{2,75}$).

Fig. B.69. Modelo da classe C_{75} – Supervisor Fosso.

C_{77} – Gerenciador da Produção de Caldo (Fig. B.70)

Esta classe inicia ($t_{1,77}$) e finaliza ($t_{6,77}$) a produção de caldo, atuando sobre os objetos do Sistema Supervisório ou diretamente sobre os equipamentos, como para as esteiras.

Fig. B.70. Modelo da classe C_{77} – Gerenciador da Produção de Caldo.

Quando a usina está em operação, a produção de caldo pode ser temporariamente suspensa através do disparo de t_{24_77} , sendo reabilitada pelo disparo de t_{23_77} .

C₇₈ - Interface Variadores de Velocidade (Fig. B.71)

Esta classe atua sobre os *Variadores de Velocidade* (C_9), da recepção (VV. Mesa 1 e VV. Mesa 2), do preparo (relacionados a VV. Esteira 1 e VV. Esteira 2) e da difusão (VV. Transportador), impondo o volume de produção de caldo desejado. Além disso atua também sobre a Válvula de Água do difusor, aumentando o fluxo de água de acordo com o fluxo de cana no transportador.

Fig. B.71. Modelo da classe *C₇₈ – Interface Variadores de Velocidade*.

C₇₉ – Interface Válvula de Caldo (Fig. B.72)

Esta classe permite a um elemento externo (operador da usina) determinar a abertura de válvula de caldo da difusão.

Fig. B.72. Modelo da classe *C₇₉ – Interface Válvula de Caldo*.

C₈₀ – Supervisor Tanque-Bomba Sulfitação (Fig. B.73)

De acordo com o volume do tanque que armazena o caldo proveniente do difusor, esta classe habilita e desabilita a produção de caldo ou a sulfitação.

Fig. B.73. Modelo da classe *C₈₀ – Supervisor Tanque-Bomba Sulfitação*.

C₈₁ - Interface Bandeja de Cal (Fig. B.74)

Esta classe inicia (t_{1_81}) e suspende (t_{4_81}) o fornecimento de cal ao processo de sulfitação, providenciando a troca da bandeja de cal em intervalos regulares de K_0 .

Fig. B.74. Modelo da classe *C₈₁ – Interface Bandeja de Cal*.

C₈₂ – Interface Forno (Fig. B.75)

Esta classe é semelhante à classe *C₈₁*, mas interage com o forno, supervisionando o fornecimento de enxofre.

Fig. B.75. Modelo da classe C₈₂ – Interface Forno.**C₈₃ – Gerenciador Sulfitação - Calagem (Fig. B.76)**

Esta classe inicia (t_{1_83}) e finaliza (t_{21_83}) a sulfitação e calagem do caldo, atuando sobre os demais objetos do Sistema Supervisório ou diretamente sobre os equipamentos. Quando a usina está em operação, a sulfitação e calagem do caldo pode ser temporariamente suspensão através da desabilitação e habilitação do processo.

Fig. B.76. Modelo da classe C₈₃ – Gerenciador da Sulfitação.

A classe C_{85} – *Supervisor Tanque Leite de Cal* é semelhante a classe C_{80} – *Supervisor Tanque-Bomba Sulfitação*, onde foram alteradas as interfaces. Ambas as classes podem ser definidas como especificação de uma terceira classe C_{84} – *Supervisor Tanque*.

C_{84} – *Supervisor Tanque* (Fig. B.77)

De acordo com o volume do tanque monitorado, esta classe habilita e desabilita os processos anteriores e posteriores.

Fig. B.77. Modelo da classe C_{84} – *Supervisor Tanque*.

C_{85} – *Supervisor Tanque Leite de Cal* (Fig. B.78)

De acordo com o volume do tanque de leite de cal, esta classe habilita e desabilita a produção de leite e a sulfitação.

Fig. B.78. Modelo da classe C_{85} – *Supervisor Tanque Leite de Cal*.

C_{86} – *Supervisor Tanque Misturador* (Fig. B.79)

Esta classe também é uma especialização da classe C_{84} – *Supervisor Tanque*. De acordo com o volume do tanque de leite de cal, ela habilita e desabilita a sulfitação e o aquecimento.

Fig. B.79. Modelo da classe C_{86} – *Supervisor Tanque Misturador*.

C₈₇ – Interface Variador de Potência (Fig. B.80)

Esta classe interage com o variador de potência das bombas de saída dos tanque, modificando o fluxo de caldo destinado à sulfitação (Interface VP Sulfitação) ou ao aquecimento (Interface VP Aquecimento).

Fig. B.80. Modelo da classe *C₈₇ – Interface Variador de Potência*.

C₈₈ – Interface Aquecedor (Fig. B.81)

Esta classe é responsável por atuar sobre o aquecedor e sua respectiva válvula, solicitando sua manutenção preventiva sistematicamente. É reservado um intervalo de tempo de K_0 para manutenção, ao final da qual o aquecedor sucessivo da série de aquecedores é colocado em manutenção.

Fig. B.81. Modelo da classe *C₈₈ – Interface Aquecedor*.

C₈₉ - Serie de Aquecedores (Fig. B.82)

Esta classe centraliza a atuação sobre os 4 aquecedores de uma série e sobre a respectiva *Válvula On/Off*.

C₉₀ – Gerenciador Aquecimento (Fig. B.83)

Esta classe liga e desliga as 3 séries de aquecedores de acordo com a quantidade de caldo a ser processada.

Fig. B.82. Modelo da classe C_{89} - *Série de Aquecedores*.***C₉₁ – Interface Clarificador-Filtro (Fig. B.84)***

Esta classe faz a interface com um clarificador e um filtro. Periodicamente é realizada a manutenção preventiva do clarificador e do filtro. Uma vez solicitado o esvaziamento do clarificador, se o mesmo não ocorre em um intervalo de tempo de K_0 é detectada falha (t_{9_91}) devido ao entupimento da tubulação.

C₉₂ – Supervisor Tanque-Bomba Clarificação (Fig. B.85)

Esta classe também é uma especialização da classe C_{84} – *Supervisor Tanque*. De acordo com o volume do tanque que recebe o caldo do aquecimento, ela habilita e desabilita os processos de clarificação e aquecimento.

Fig. B.83. Modelo da classe C₉₀ – Gerenciador Aquecimento. Fig. B.84. Modelo da classe C₉₁ – Interface Clarificador - Filtro.

Fig. B.85. Modelo da classe C₉₂ – Supervisor Tanque-Bomba Clarificação.**C₉₃ – Gerenciador Clarificação (Fig. B.86)**

Esta classe faz gerencia o processo de clarificação, solicitando o acionamento dos clarificadores de acordo como volume de produção desejado.

Fig. B.86. Modelo da classe C₉₃ – Gerenciador Clarificação.

C₉₄ - Supervisor Tanque-Bomba Evaporação (Fig. B.87)

Esta classe também é uma especialização da classe *C₈₄ – Supervisor Tanque*. De acordo com o volume do tanque que recebe o caldo da clarificação, ela habilita e desabilita os processos de clarificação e evaporação.

Fig. B.87. Modelo da classe *C₉₄ – Supervisor Tanque-Bomba Evaporação*.

C₉₅ – Interface Variadores de Potência – Evaporação (Fig. B.88)

Esta classe atua sobre os variadores de potência que determinam o fluxo de caldo enviado ao 1º e 2º Efeito da evaporação, de acordo com o volume de produção desejado.

Fig. B.88. Modelo da classe *C₉₅ – Interface Variadores de Potência - Evaporação*.

C₉₆ – Gerenciador Evaporação (Fig. B.89)

Esta classe faz gerencia o processo de evaporação, solicitando o acionamento dos equipamentos quando necessário.

Fig. B.89. Modelo da classe C₉₆ – Gerenciador Evaporação.**C₉₇ – Interface Cozedor (Fig. B.90)**

Esta classe seleciona o tipo de cozimento a ser executado no cozedor e realiza a produção de ciclos sucessivamente até que seja solicitado sua interrupção.

Fig. B.90. Modelo da classe C₉₇ – Interface Cozedor.

C₉₈ – Gerenciador Genérico Cozimento

Esta classe gerencia a produção de um tipo de massa, solicitando seu cozimento nos equipamentos de n_1 a n_2 . A produção é interrompida no caso de detecção de falha, informada através dos disparos de t_{15_98} e t_{17_98} . A Fig. B.91 apresenta o modelo de uma de suas especializações para o caso do cozimento de massa tipo C.

C₉₉ – Gerenciador Cozimento A

Esta classe é uma especialização da classe C₉₈, onde a transição t_{7_98} é associada à seguinte chamada de método: ‘ $t_{7_99}/t_{1_97.11}$ – Inicia Cozimento A’.

C₁₀₀ – Gerenciador Cozimento B

Esta classe é uma especialização da classe C₉₈, onde a transição t_{7_98} é associada à seguinte chamada de método: ‘ $t_{7_99}/t_{2_97.11}$ – Inicia Cozimento B’.

C₁₀₁ – Gerenciador Cozimento C (Fig. B.91)

Esta classe é uma especialização da classe C₉₈, onde a transição t_{7_98} é associada à seguinte chamada de método: ‘ $t_{7_99}/t_{3_97.11}$ – Inicia Cozimento C’.

Fig. B.91. Modelo da classe C_{101} – Gerenciador Cozimento C. C_{102} – Gerenciador Cozimento Global (Fig. B.92)

Esta classe inicia e interrompe o cozimento de acordo com o solicitado por um elemento externo (operador da usina), que deve também informar o número de cozedores que produziram cada tipo de massa.

Fig. B.92. Modelo da classe C_{102} – Gerenciador Cozimento.

O gerenciamento das centrífugas realizado de forma semelhante ao dos cozedores. Assim tem-se as seguintes classes:

C₁₀₃ – Interface Centrífuga

Esta classe é semelhante a *C₉₇ – Interface Cozedor*, mas com as seguintes chamadas de métodos:

$t_{5_103} \rightarrow t_{1_67.11}$ – Iniciar ciclo na *Centrífuga*
 $t_{8_103} \rightarrow t_{10_67.11}$ – Passar de Config A p/ Config B na *Centrífuga*
 $t_{9_103} \rightarrow t_{11_67.11}$ – Passar de Config B p/ Config A na *Centrífuga*
 $t_{10_103} \rightarrow t_{15_67.11}$ – Passar de Config C p/ Config A na *Centrífuga*
 $t_{11_103} \rightarrow t_{14_67.11}$ – Passar de Config A p/ Config C na *Centrífuga*
 $t_{13_103} \rightarrow t_{12_67.11}$ – Passar de Config B p/ Config C na *Centrífuga*
 $t_{14_103} \rightarrow t_{13_67.11}$ – Passar de Config C p/ Config B na *Centrífuga*

C₁₀₄ – Gerenciador Genérico Centrifugação

Esta classe é semelhante a *C₉₈ – Gerenciador Genérico Cozimento*, mas com as seguintes funções de junção e chamadas de métodos:

j_{4_104} : $X = n_1$; $l_1 = \text{'Interface Cozedor_' + X}$;
 j_{5_104} : $X = X + 1$; $l_1 = \text{'Interface Cozedor_' + X}$;
 j_{10_104} : $X = X + 1$; $l_1 = \text{'Interface Cozedor_' + X}$;
 j_{11_104}, j_{12_104} : $X = n_1$; $l_1 = \text{'Interface Cozedor_' + X}$;
 $t_{8_104} \rightarrow t_{4_103.11}$ – Finaliza centrifugação

C₁₀₅ – Gerenciador Centrifugação A

Esta classe é uma especialização da classe *C₁₀₄*, onde a transição t_{7_104} é associada à seguinte chamada de método: ' $t_{7_105} \rightarrow t_{1_103.11}$ – Inicia Centrifugação A'.

C₁₀₆ – Gerenciador Centrifugação B

Esta classe é uma especialização da classe *C₁₀₄*, onde a transição t_{7_104} é associada à seguinte chamada de método: ' $t_{7_106} \rightarrow t_{2_103.11}$ – Inicia Centrifugação B'.

C₁₀₇ – Gerenciador Centrifugação C

Esta classe é uma especialização da classe *C₁₀₄*, onde a transição t_{7_104} é associada à seguinte chamada de método: ' $t_{7_107} \rightarrow t_{3_103.11}$ – Inicia Centrifugação C'.

C₁₀₈ – Gerenciador Centrifugação Global

Esta classe é semelhante a *C₁₀₂ – Gerenciador Centrifugação Global*, mas com as seguintes chamadas de métodos:

$t_{2_108} \rightarrow t_{1_105.11}$ – $\{1, n_A\}$ – Inicia centrifugação A
 $t_{3_108} \rightarrow t_{1_106.12}$ – $\{n_A + 1, n_B\}$ – Inicia centrifugação B
 $t_{3_108} \rightarrow t_{1_107.13}$ – $\{n_B + 1, n_C\}$ – Inicia centrifugação C
 $t_{2_108} \rightarrow t_{13_105.11}$ – $\{1, n_A\}$ – Finaliza centrifugação
 $t_{3_108} \rightarrow t_{13_106.12}$ – $\{n_A + 1, n_B\}$ – Finaliza centrifugação
 $t_{3_108} \rightarrow t_{13_107.13}$ – $\{n_B + 1, n_C\}$ – Finaliza centrifugação

C₁₀₉ – Supervisor Tanque-Xarope (Fig. B.93)

Esta classe também é uma especialização da classe *C₈₄ – Supervisor Tanque* (apresentada no Anexo 1). De acordo com o volume do tanque de xarope, ela habilita e desabilita os processos de cozimento A e evaporação.

Fig. B.93. Modelo da classe *C₁₀₉ – Supervisor Tanque Xarope*.

C₁₁₀ – Supervisor Tanque Massa

Idem a *C₁₀₉ – Supervisor Tanque Xarope*, mas com as seguintes chamadas de métodos:

$t_{1_110} \rightarrow t_{15_104.11}$ – Desabilita Centrifugação
 $t_{2_110} \rightarrow t_{14_104.11}$ – Habilita Centrifugação
 $t_{3_110} \rightarrow t_{17_98.12}$ – Desabilita Cozimento
 $t_{4_110} \rightarrow t_{16_98.12}$ – Habilita Cozimento

C₁₁₁ – Supervisor Tanque Magma

Esta classe é semelhante a *C₁₀₉ – Supervisor Tanque Xarope*, mas com as seguintes chamadas de métodos:

$t_{1_111} \rightarrow t_{19_98.12}$ – Desabilita Cozimento
 $t_{2_111} \rightarrow t_{18_98.12}$ – Habilita Cozimento
 $t_{3_111} \rightarrow t_{17_104.11}$ – Desabilita Centrifugação
 $t_{4_111} \rightarrow t_{16_104.11}$ – Habilita Centrifugação

C₁₁₂ – Supervisor Tanque Mel

Esta classe é semelhante a *C₁₀₉ – Supervisor Tanque Xarope*, mas com as seguintes chamadas de métodos:

$t_{1_112} \rightarrow t_{15_98.12}$ – Desabilita Cozimento
 $t_{2_112} \rightarrow t_{14_98.12}$ – Habilita Cozimento
 $t_{3_112} \rightarrow t_{19_104.11}$ – Desabilita Centrifugação
 $t_{4_112} \rightarrow t_{18_104.11}$ – Habilita Centrifugação

C₁₁₃ – Interface Caminhão de Mel C (Fig. B.94)

Esta classe providencia o carregamento de caminhões de mel C quando solicitado por um elemento externo (operador da usina).

Fig. B.94. Modelo da classe C₁₁₃ – Interface Caminhão de Mel C.**C₁₁₄ – Interface Secador – Empacotador (Fig. B.95)**

Esta classe providencia o empacotamento do açúcar armazenado no *Tanque de Açúcar* quando solicitado por um elemento externo (operador da usina).

Fig. B.95. Modelo da classe C₁₁₄ – Interface Secador-Empacotador.**B.1.6. Atividade 7 – Verificação dos Modelos****Modelo em redes PTD-OO e Diagrama de Atividade**

Continuando a aplicação do procedimento proposto para modelagem, a Fig. B.96 apresenta o detalhamento do Diagrama de Atividade da Fig. B.5, considerando agora as atividades referentes às comunicações entre os objetos.

Seguindo o procedimento apresentado no Capítulo 3, o Diagrama de Atividades apresentado é convertido para um modelo em redes de Petri (Fig. B.97), cujos elementos são relacionados com os elementos do modelo em redes PTD-OO dos objetos.

Modelo em redes PTD-OO e Diagramas de Seqüência e/ou Colaboração

A Fig. B.6 apresenta a relação entre as interação dos Diagramas de Seqüência do Caso de Uso ‘Descarregar caminhão c/ caçamba basculante’ e as transições dos modelos em redes PTD das classes.

Fig. B.96. Detalhamento do Diagrama de Atividades da Fig. B.5.

B.2. Análise dos Modelos em redes PTD-OO

A seguir apresenta-se a verificação de uma propriedade de alcançabilidade para a Usina Cruz Alta.

Considera-se que os objetos envolvidos nesta verificação têm os seguintes estados iniciais:

- $O_{1,2}$ = Caminhão c/ Caçamba Basculante 1; $X_{1,2} = \{K_{\alpha_CB} = 0,009, K_{q_CB} = 0,013, \alpha_{CB} = 0, V_C = ind, \theta_{aux} = 0, K_{\theta_C1} = 300, K_{\theta_C2} = 250, l_1 = \text{Interface Mesas}, l_2 = ind, l_3 = \text{Mesa 1}, l_4 = \text{Fosso}, q_{CB} = 0\}$; $m_{2,1} = \{p_{1,2}\}$;
- $O_{1,5}$ = Guindaste Mesa; $X_{1,5} = \{K_{v_G} = 0,1, K_{\theta_G} = 30, n_{fG} = 0, V_{fG} = 0, \theta_{aux} = 0, l_1 = \text{Fosso}, l_2 = \text{Mesa 1}, v_G = 0\}$; $m_{1,5} = \{p_{1,5}\}$;

Fig. B.97. Conversão para redes de Petri do Diagrama de Atividades da Fig. B.96.

Fig. B.98. Diagrama de Sequência do Caso de Uso 'Descarregar caminhão c/ caçamba basculante'.

- $O_{2,5} = \text{Guindaste Fosso}$; $X_{2,5} = \{K_{V_G} = 0,1, K_{\theta_G} = 30, n_{fG} = 0, V_{fG} = 0, \theta_{aux} = 0, l_1 = \text{Fosso}, l_2 = \text{Mesa 1}, v_G = 0\}$; $m_{2,5} = \{p_{1,5}\}$;
- $O_{1,6} = \text{Fosso}$; $X_{1,6} = \{V_F = 50, V_{CF} = 0, K_{V_fCG} = 1, l_1 = ind\}$; $m_{1,6} = \{p_{1,6}\}$;
- $O_{1,7} = \text{Mesa 1}$; $X_{1,7} = \{V_M = ind, V_{CM} = 0, K_{q_M} = 1, K_{V_M} = ind, l_1 = ind, l_2 = \text{Chuveiro 1}, l_3 = \text{VV Mesa 1}, q_M = 0\}$; $m_{1,7} = \{p_{2,7}, p_{4,7}\}$;

- $O_{1.74} = \text{Interface Mesas}$; $X_{1.74} = \{V_{M1} = ind, V_{M2} = ind, K_V = ind, V_C = 0, q = 0, l_1 = \text{Mesa 1}, l_2 = \text{Mesa 2}, l_3 = \text{Supervisor Fosso}\}$; $m_{1.74} = \{p_{1.74}, p_{8.74}, p_{9.74}\}$;
- $O_{1.75} = \text{Supervisor Fosso}$; $X_{1.75} = \{V_F = ind, K_{fx} = ind, K_V = ind, V_C = 0, l_1 = \text{Interface Mesas}, l_2 = ind, l_3 = \text{Fosso}\}$; $m_{1.75} = \{p_{1.75}\}$;

B.2.1. Propriedade 2

B.2.1.1. Etapa 1 - Definição do enunciado da propriedade

O enunciado da **Propriedade 2** é definido de acordo com o tipo de enunciado PA1 (apresentado no Capítulo 4, Seção 4.3.3.1):

- **Propriedade 2** - Quando um caminhão c/ caçamba basculante (por exemplo $O_{1.2}$ – Caminhão c/ Caçamba Basculante 1) chega a usina (evento e_0), ele deixa a usina (evento e_f) após no máximo 30 min: e_0 = disparo de $t_{1.2.O1}$; e_f = alcance de $m_{1.2} = \{p_{1.2}\}$; $\Delta\theta = 30 \text{ min} = 1800s$.

B.2.1.2. Etapa 2 - Definição do conjunto de restrições da propriedade

São consideradas as seguintes restrições, correspondentes aos tipos de restrições descritos na Seção 4.3.3.2 do Capítulo 4:

- Restrição 2A (correspondente a R5) – Neste intervalo de tempo, os demais caminhões (objetos $O_{2.2}$, ..., $O_{10.2}$ e $O_{1.3}$, ..., $O_{10.3}$) estão fora da usina: $m_{2.2} = \dots = m_{10.2} = \{p_{1.2}\}$ e $m_{1.3} = \dots = m_{10.3} = \{p_{1.3}\}$ em $\theta_{1.2.O1} \leq \theta \leq \theta(e_f)$.
- Restrição 2B (correspondente a R5) – Os guindastes ($O_{1.5}$ e $O_{2.5}$) estão livres quando o caminhão chega a usina: $p_{1.5.O1} = p_{1.5.O2} = 1$ em $\theta = \theta_{1.2.O1}$.
- Restrição 2C (correspondente a R2) – Não ocorreu nem ocorre travamento da Esteira 1 ou na Mesa 1 por excesso de cana: $t_{1.13.O1}$ e $t_{1.7.O1}$ não dispararam em $0 \leq \theta \leq \theta_{1.2.O1}$.
- Restrição 2D (correspondente a R8) – O volume de cana do caminhão que chega à usina está entre 3 e 5 m³: $V_{C.O1.C2}(\theta_{1.2.O1}) \in [3, 5]$.

B.2.1.3. Etapa 3 – Construção dos Diagramas de Colaboração Estáticos

A Fig. B.99 apresenta o Diagrama de Colaboração Estático ilustrando as interações entre objetos relevantes para a verificação da **Propriedade 2**.

Resumidamente, através da análise do objeto Caminhão c/ Caçamba 1 são determinados dois cenários possíveis para o destino do caminhão: o **Cenário 1**, correspondente ao descarregamento na Mesa 1 e o **Cenário 2**, correspondente ao descarregamento no Fosso. A determinação de qual cenário será executado é feita pelo

objeto Interface Mesas em base ao volume de cana na Mesa 1. Analisando os guindastes, os **Cenários 1 e 2** são decompostos em **Cenários 1-1 e 1-2**, e **2-1-1 e 2-1-2**, correspondentes aos casos em que é necessário ou não trocar o gancho dos guindastes. Todos os demais cenários gerados durante a análise da parte discreta dos objetos resultam impossíveis.

Fig. B.99. Diagrama de Colaboração das interações relevantes para a **Propriedade 2**.

B.2.1.4. *Etapa 4.1 – Parte Discreta – Busca de Cenários ($O_{1.2}$ - Caminhão c/ Caçamba Basculante 1)*

As transições $t_{11_2.O1}$, $t_{13_2.O1}$ e $t_{15_2.O1}$ deste objeto são duplicadas na versão desdobrada da rede, pois existem dois objetos da classe C_5 cujos métodos podem ser chamados por este objeto. Tem-se então que as transições $t_{11_2.O1a}$, $t_{13_2.O1a}$ e $t_{15_2.O1a}$ chamam os métodos associados a $t_{1_5.O1}$, $t_{14_5.O1}$ e $t_{24_5.O1}$, enquanto $t_{11_2.O1b}$, $t_{13_2.O1b}$ e $t_{15_2.O1b}$ chamam os métodos associados a $t_{1_5.O2}$, $t_{14_5.O2}$ e $t_{24_5.O2}$.

- *Busca 1* (a partir do disparo de $t_{1_2.O1}$): $\Gamma_0, p_{2_2.O1}, !t_{1_2.O1}, \dots, !t_{16_2.O1} \mid\!\!\! \mid p_{1_2.O1} \otimes \Gamma_f$, onde $p_{2_2.O1}$ = pós-condição de $t_{1_2.O1}$.
- *Definição de Cenários* – A análise do seqüente da *Busca 1* resulta apenas em cenários que, de fato, conduzem a $p_{2_2.O1}$, e onde $\Gamma_0 = \Gamma_f = \emptyset$:
 - **Cenário 1:** $t_{2_2.O1}; t_{3_2.O1}; t_{5_2.O1}; t_{11_2.O1a}; t_{12_2.O1}; t_{13_2.O1a}; t_{14_2.O1}; t_{15_2.O1a}; t_{16_2.O1}; t_{7_2.O1}; t_{9_2.O1}$.
 - **Cenário 2:** $t_{2_2.O1}; t_{4_2.O1}; t_{6_2.O1}; t_{11_2.O1b}; t_{12_2.O1}; t_{13_2.O1b}; t_{14_2.O1}; t_{15_2.O1b}; t_{16_2.O1}; t_{8_2.O1}; t_{10_2.O1}$.
 - **Cenários 3 a 9:** semelhante ao **Cenário 1**, trocando $t_{11_2.O1a}$, $t_{13_2.O1a}$ e/ou $t_{15_2.O1a}$ por $t_{11_2.O1b}$, $t_{13_2.O1b}$ e/ou $t_{15_2.O1b}$.
 - **Cenários 10 a 16:** semelhante ao **Cenário 2**, trocando $t_{11_2.O1b}$, $t_{13_2.O1b}$ e/ou $t_{15_2.O1b}$ por $t_{11_2.O1a}$, $t_{13_2.O1a}$ e/ou $t_{15_2.O1a}$.

A Fig. B.100 ilustra a ordem parcial de disparo para os **Cenários 1 e 2**.

Fig. B.100. Ordem parcial de disparos – Cenários 1 e 2 – Propriedade 2.

B.2.1.5. Etapa 4.2 – Elaboração de Hipóteses ($O_{1.2}$ - Caminhão c/ Caçamba Basculante 1)

São feitas as seguintes hipóteses:

- Hipótese 2A (correspondente a H1) – O objeto Interface Mesas sempre recebe imediatamente a informação sobre a chegada de um caminhão: $t_{2_2.O1}$ dispara em $\Delta\theta = 0$ após sua habilitação em $O_{1.2}$.
- Hipótese 2B (correspondente a H1) – A Mesa 1 e o Fosso estão disponíveis para descarregamento do caminhão: $t_{5_2.O1/3_7.O1}$ e $t_{6_2.O1/2_6.O1}$ disparam em $\Delta\theta = 0$ após sua habilitação em $O_{1.2}$.
- Hipótese 2C (correspondente a H9) – A velocidade do cabo do guindaste é constante durante o descarregamento: $v_{G.12.C5} = \text{cte p/ } \theta_{13_2.O1a/14_5.O1} \leq \theta \leq \theta_{14_2.O1}$ (**Cenário 1**) ou $\theta_{13_2.O1b/14_5.O1} \leq \theta \leq \theta_{14_2.O1}$ (**Cenário 2**).

B.2.1.6. Etapa 4.3 – Parte Contínua – Evolução de variáveis contínuas e datas de disparos ($O_{1.2}$ - Caminhão c/ Caçamba Basculante 1)

• **Cenários 1, 3 a 9:**

A análise da parte contínua leva as seguintes conclusões:

- Como resultado da Hipótese 2A, $\theta_{2_2.O1/17.74.O1} = \theta_{1_2.O1}$.
- $\theta_{18_74.O1/3_2.O1} \geq \theta_{2_2.O1/17.74.O1}$, $\theta_{\text{aux}} = 0$, $I_2 = \text{Guindaste Mesa } (O_{1.5})$ - o que implica na habilitação das transições $t_{11_2.O1a}$, $t_{13_2.O1a}$ e $t_{15_2.O1a}$ no lugar das transições $t_{11_2.O1b}$, $t_{13_2.O1b}$ e $t_{15_2.O1b}$, tornando os **Cenários 3 a 9** impossíveis (O **Cenário 1** deve então ser possível).
- Como resultado da Hipótese 2B, $\theta_{5_2.O1/3_7.O1} = \theta_{18_74.O1/3_2.O1} + K_{\theta_C1}$.
- $\theta_{11_2.O1a/1_5.O1} \geq \theta_{5_2.O1/3_7.O1}$; $\theta_{12_2.O1} = \theta_{11_2.O1a/1_5.O1}$; $\theta_{13_2.O1a/14_5.O1} \geq \theta_{12_2.O1}$.
- $\theta_{14_2.O1} = \theta_{13_2.O1a/14_5.O1} + \theta_d$, onde θ_d é o tempo de descarregamento.

- Considerando a Hipótese 2C, a expressão de θ_d é dada pelo seguinte equacionamento (válido p/ $\theta_{13_2.O1a/14_5.O1} \leq \theta \leq \theta_{14_2.O1}$):
 - $\dot{\alpha}_{CB} = K_{\alpha_CB} * v_{G.I2.C5} \Rightarrow \alpha_{CB}(\theta) = K_{\alpha_CB} * v_{G.O1.C5} * (\theta - \theta_{13_2.O1a/14_5.O1})$
 - $q_{CB} = K_{q_CB} * \alpha_{CB} \Rightarrow q_{CB}(\theta) = K_{q_CB} * K_{\alpha_CB} * v_{G.O1.C5} * (\theta - \theta_{13_2.O1a/14_5.O1})$
 - $\dot{V}_{CB} = q_{CB} \Rightarrow V_{CB}(\theta) = V_{CB}(\theta_{13_2.O1a/14_5.O1}) + K_{q_CB} * K_{\alpha_CB} * v_{G.O1.C5} * (\theta - \theta_{13_2.O1a/14_5.O1})^2 / 2$
 - $V_{CB}(\theta_{13_2.O1a/14_5.O1} + \theta_d) = 0 \Rightarrow \theta_d = (-2 * V_{CB}(\theta_{13_2.O1a/14_5.O1}) / (K_{q_CB} * K_{\alpha_CB} * v_{G.O1.C5}))^{1/2}$
- $\theta_{15_2.O1a/24_5.O1} \geq \theta_{13_2.O1a/14_5.O1} + \theta_d$; $\theta_{16_2.O1} = \theta_{15_2.O1a/24_5.O1}$; $\theta_{7_2.O1/4_7.O1} \geq \theta_{16_2.O1}$; $\theta_{9_2.O1} = \theta_{7_2.O1/4_7.O1} + K_{\theta_C1}$.
- No caso do **Cenário 1**, a condição para que a **Propriedade 2** seja verdadeira é: $\theta_{7_2.O1/4_7.O1} \leq 1800 - K_{\theta_C1}$.
- **Cenários 2, 10 a 16**

É feita uma análise semelhante à realizada para os **Cenários 1, 3 a 9**, resultando em:

 - Como resultado da Hipótese 2A, $\theta_{2_2.O1/17.74.O1} = \theta_{1_2.O1}$.
 - $\theta_{18_74.O1/3_2.O1} \geq \theta_{2_2.O1/17.74.O1}$, $\theta_{aux} = 0$, $I_2 = \text{Guindaste Fosso (O}_{2.5})$, tornando os **Cenários 10 a 16** impossíveis.
 - Como resultado da Hipótese 2B, $\theta_{6_2.O1/2_6.O1} = \theta_{5_75.O1/4_2.O1} + K_{\theta_C1}$.
 - $\theta_{11_2.O1b/1_5.O2} \geq \theta_{6_2.O1/2_6.O1}$; $\theta_{12_2.O1} = \theta_{11_2.O1b/1_5.O2}$; $\theta_{13_2.O1b/14_5.O2} \geq \theta_{12_2.O1}$.
 - $\theta_{14_2.O1} = \theta_{13_2.O1b/14_5.O2} + \theta_d$ (θ_d dado pela mesma expressão do **Cenário 1**).
 - $\theta_{15_2.O1b/24_5.O2} \geq \theta_{13_2.O1b/14_5.O2} + \theta_d$; $\theta_{16_2.O1} = \theta_{15_2.O1b/24_5.O2}$; $\theta_{8_2.O1/4_6.O1} \geq \theta_{16_2.O1}$; $\theta_{9_2.O1} = \theta_{8_2.O1/4_6.O1} + K_{\theta_C2}$.
 - No caso do **Cenário 2**, a condição para que a **Propriedade 2** seja verdadeira é: $\theta_{8_2.O1/4_6.O1} \leq 1800 - K_{\theta_C2}$.

Para determinar os tempos de disparo das transições, os objetos Interface Mesas, Supervisor Fosso, Mesa 1, Fosso, Guindaste Mesa e Guindaste Fosso devem ser analisados.

B.2.1.7. ***Etapla 5.1 – Parte Discreta – Busca de Cenários (O_{1.74} - Interface Mesas)***

Desdobrando a rede deste objeto, surgem tantas transições correspondentes aos métodos oferecidos quanto objetos das classes C_2 (*Caminhão c/ Caçamba Basculante*) e C_3 (*Caminhão c/ Correntes*). No entanto, de acordo com Restrição 2A, com exceção das transições correspondentes à interface com $O_{1.2}$, as demais transições nunca serão disparadas. Estas transições não são, portanto, consideradas nesta busca.

- **Cenário 1:**

- *Busca 1* (até o disparo de $t_{2_2.O1/17.74.O1}$): como a data de disparo de $t_{2_2.O1/17.74.O1}$ é imposta pela Hipótese 2A, esta busca é omitida.
- *Busca 2* (do disparo de $t_{2_2.O1/17.74.O1}$ até o disparo de $t_{18_74.O1/3_2.O1}$): corresponde à busca do seqüente $\Gamma_0, p_{10_74.O1}, !t_{1_74.O1}, \dots, !t_{16_74.O1}, t_{18_74.O1} \vdash \Gamma_f$, que resulta em apenas um cenário, apresentado a seguir, onde $\Gamma_0 = \emptyset, \Gamma_f = p_{9_74.O1}$.
- *Busca 3* (a partir do disparo de $t_{18_74.O1/3_2.O1}$): esta busca não foi considerada relevante para a verificação da propriedade analisada.
- *Definição de cenários:*
 - **Cenário 1:** $t_{2_2.O1/17.74.O1}; t_{18_74.O1/3_2.O1}$.

- **Cenário 2:**

- *Busca 1* (até o disparo de $t_{2_2.O1/17.74.O1}$): como a data de disparo de $t_{2_2.O1/17.74.O1}$ é imposta pela Hipótese 2A, esta busca é omitida.
- *Busca 2* (do disparo de $t_{2_2.O1/17.74.O1}$ até o disparo de $t_{19_74.O1/2_75.O1}$): corresponde à busca do seqüente $\Gamma_0, p_{10_74.O1}, !t_{1_74.O1}, \dots, !t_{16_74.O1}, t_{19_74.O1} \vdash \Gamma_f$ que resulta em apenas um cenário, apresentado a seguir, onde $\Gamma_0 = \emptyset, \Gamma_f = p_{9_74.O1}$.
- *Busca 3* (a partir do disparo de $t_{19_74.O1/2_75.O1}$): esta busca não foi considerada relevante para a verificação da propriedade analisada.
- *Definição de cenários:*
 - **Cenário 2:** $t_{2_2.O1/17.74.O1}; t_{19_74.O1/2_75.O1}$.

B.2.1.8. *Etapa 5.2 – Elaboração de Hipóteses ($O_{1.74}$ - Interface Mesas)*

É feita a seguinte hipótese:

- Hipótese 2D (correspondente a H1) – O objeto Supervisor Fosso recebe imediatamente as solicitações da Interface Mesas: $t_{19_74.O1/2_75.O1}$ dispara em $\Delta\theta = 0$ após sua habilitação em $O_{1.74}$.

B.2.1.9. *Etapa 5.3 – Parte Contínua – Evolução de variáveis contínuas e datas de disparos ($O_{1.74}$ - Interface Mesas)*

- **Cenários 1 e 2**

As condições para o disparo de $t_{18_74.O1/3_2.O1}$ e $t_{19_74.O1/2_75.O1}$ são complementares (uma das duas sempre é verdadeira). Assim, no caso do **Cenário 1** $\theta_{18_74.O1/3_2.O1} = \theta_{2_2.O1/17.74.O1}$. e, no caso do **Cenário 2**, de acordo com a Hipótese 2D, $\theta_{19_74.O1/2_75.O1} = \theta_{2_2.O1/17.74.O1}$.

B.2.1.10. Etapa 5.1 – Parte Discreta – Busca de Cenários ($O_{1.75}$ - Supervisor Fosso)

Semelhantemente ao realizado para o Interfaces Mesas, não são consideradas as transições de interface com os objetos das classes C_2 (*Caminhão c/ Caçamba Basculante*) e C_3 (*Caminhão c/ Correntes*), com exceção de $O_{1.2}$.

- **Cenário 1:** Não contém transições deste objeto.
- **Cenário 2:** A princípio a ordem de disparo de $t_{19_74.O1/2_75.O1}$ em relação a $t_{5_75.O1/4_2.O1}$ não é conhecida. Dois casos são então considerados:
 - **Cenário 2-1** (disparo de $t_{19_74.O1/2_75.O1}$ antes do disparo de $t_{5_75.O1/4_2.O1}$):
 - *Busca 1* (até o disparo de $t_{19_74.O1/2_75.O1}$): como a data de disparo de $t_{19_74.O1/2_75.O1}$ é imposta pela Hipótese 2D, esta busca é omitida.
 - *Busca 2* (do disparo de $t_{19_74.O1/2_75.O1}$ até o disparo de $t_{5_75.O1/4_2.O1}$): corresponde a busca do seqüente $\Gamma_0, p_{3_75.O1}, !t_{1_75.O1}, \dots, !t_{6_75.O1}, t_{5_75.O1} \vdash \Gamma_f$, que resulta em apenas um cenário, apresentado a seguir, onde $\Gamma_0 = \emptyset$, $\Gamma_f = p_{1_75.O1}$.
 - *Busca 3* – (do disparo de $t_{5_75.O1/4_2.O1}$): esta busca não foi considerada relevante para a verificação da propriedade analisada.
 - *Definição de cenários:*
 - **Cenário 2-1:** $t_{19_74.O1/2_75.O1}; t_{5_75.O1/4_2.O1}$.
 - **Cenário 2-2** (disparo de $t_{5_75.O1/4_2.O1}$ antes do disparo de $t_{19_74.O1/2_75.O1}$):
 - *Busca 1* (até o disparo de $t_{5_75.O1/4_2.O1}$) para que este cenário seja verdadeiro, o único estado possível para o objeto é $p_{3_75} =$ pré-condição de $t_{5_75.O1/4_2.O1}$.
 - *Busca 2* (do disparo de $t_{5_75.O1/4_2.O1}$ ao disparo de $t_{19_74.O1/2_75.O1}$): corresponde a busca do seqüente $\Gamma_0, p_{1_75.O1}, !t_{1_75.O1}, \dots, !t_{6_75.O1}, t_{2_75.O1} \vdash \Gamma_f$, que resulta em apenas um cenário, apresentado a seguir, onde $\Gamma_0 = \emptyset$, $\Gamma_f = p_{3_75.O1}$.
 - *Busca 3* (a partir do disparo de $t_{19_74.O1/2_75.O1}$): esta busca não foi considerada relevante para a verificação da propriedade analisada.
 - *Definição de cenários:*
 - **Cenário 2-2:** $t_{5_75.O1/4_2.O1}; t_{19_74.O1/2_75.O1}$.

B.2.1.11. Etapa 5.2 – Elaboração de Hipóteses ($O_{1.75}$ - Supervisor Fosso)

É feita a seguinte hipótese:

- Hipótese 2E (correspondente a H1) – Considerando as restrições definidas para esta propriedade o objeto Supervisor Fosso não está habilitado a emitir uma ordem de descarregamento no Fosso da chegada do Caminhão c/ Caçamba Basculante ($O_{1.2}$) à

usina até que um pedido seja emitido pelo Supervisor Mesas: $p_{3_75.O1} = 0$ entre os disparos de $t_{1_2.O1}$ e $t_{19_74.O1/2_75.O1}$.

De acordo com está hipótese, o **Cenário 2-2** é impossível.

B.2.1.12. Etapa 5.3 – Parte Contínua – Evolução de variáveis contínuas e datas de disparos ($O_{1.75}$ - Supervisor Fosso)

- **Cenário 2-1**

- Não existem condições adicionais para o disparo, portanto $\theta_{5_75.O1/4_2.O1} = \theta_{19_74.O1/2_75.O1}$.

B.2.1.13. Etapa 5.1 – Parte Discreta – Busca de Cenários ($O_{1.7}$ - Mesa 1)

Semelhantemente ao realizado para o Interfaces Mesas, não são consideradas as transições de interface com os objetos das classes C_2 (*Caminhão c/ Caçamba Basculante*) e C_3 (*Caminhão c/ Correntes*), com exceção de $O_{1.2}$.

- **Cenário 1**

- *Busca 1* (até o disparo de $t_{5_2.O1/3_7.O1}$): como a data de disparo de $t_{5_2.O1/3_7.O1}$ é imposta pela Hipótese 2B, esta busca é omitida.
- *Busca 2* (do disparo de $t_{5_2.O1/3_7.O1}$ até o disparo de $t_{7_2.O1/4_7.O1}$): corresponde a busca do seqüente $\Gamma_0, p_{3_7.O1}, !t_{1_7.O1}, \dots, !t_{6_7.O1}, t_{4_7.O1} \vdash \Gamma_f$, que resulta em apenas um cenário, apresentado a seguir, onde $\Gamma_0 = \emptyset$, $\Gamma_f = p_{2_7.O1}$.
- *Busca 3* (a partir do disparo de $t_{7_2.O1/4_7.O1}$): esta busca não foi considerada relevante para a verificação da propriedade analisada.
- *Definição de cenários:*
 - **Cenário 1:** $t_{5_2.O1/3_7.O1}; t_{7_2.O1/4_7.O1}$.

- **Cenário 2-1:** Não contém transições deste objeto.

B.2.1.14. Etapa 5.2 – Elaboração de Hipóteses ($O_{1.7}$ - Mesa 1)

Nenhuma hipótese é elaborada.

B.2.1.15. Etapa 5.3 – Parte Contínua – Evolução de variáveis contínuas e datas de disparos ($O_{1.7}$ - Mesa 1)

- **Cenário 1**

- Não existem condições adicionais para o disparo, portanto $\theta_{7_2.O1/4_7.O1} = \theta_{16_2.O1}$.

B.2.1.16. Etapa 5.1 – Parte Discreta – Busca de Cenários ($O_{1.6}$ - Fosso)

Semelhantemente ao realizado para o Interfaces Mesas, não são consideradas as transições de interface com os objetos das classes C_2 (*Caminhão c/ Caçamba Basculante*) e C_3 (*Caminhão c/ Correntes*), com exceção de $O_{1.2}$.

- **Cenário 1:** Não contém transições deste objeto.
- **Cenário 2-1:**
 - *Busca 1* (até o disparo de $t_{6_2.O1/2_6.O1}$): como a data de disparo de $t_{6_2.O1/2_6.O1}$ é imposta pela Hipótese 2B, esta busca é omitida.
 - *Busca 2* (do disparo de $t_{6_2.O1/2_6.O1}$ até o disparo de $t_{8_2.O1/4_6.O1}$): corresponde a busca do seqüente $\Gamma_0, p_{2_6.O1}, !t_{1_7.O1}, \dots, !t_{6_7.O1}, t_{4_7.O1} \vdash \Gamma_f$, que resulta em apenas um cenário, apresentado a seguir, onde $\Gamma_0 = \emptyset$, $\Gamma_f = p_{1_6.O1}$.
 - *Busca 3* – Evolução a partir do disparo de $t_{8_2.O1/4_6.O1}$: esta busca não foi considerada relevante para a verificação da propriedade analisada.
 - *Definição de cenários:*
 - **Cenário 1:** $t_{6_2.O1/2_6.O1}; t_{8_2.O1/4_6.O1}$.

B.2.1.17. Etapa 5.2 – Elaboração de Hipóteses ($O_{1.6}$ - Fosso)

Nenhuma hipótese é elaborada.

B.2.1.18. Etapa 5.3 – Parte Contínua – Evolução de variáveis contínuas e datas de disparos ($O_{1.6}$ - Fosso)

- **Cenário 2-1**
 - Não existem condições adicionais para o disparo, portanto $\theta_{8_2.O1/4_6.O1} = \theta_{16_2.O1}$.

B.2.1.19. Etapa 5.1 – Parte Discreta – Busca de Cenários ($O_{1.5}$ - Guindaste Mesa)

- **Cenário 1**

Semelhantemente ao realizado para o Interfaces Mesas, não são consideradas as transições de interface com os objetos das classes C_2 (*Caminhão c/ Caçamba Basculante*) e C_3 (*Caminhão c/ Correntes*), com exceção de $O_{1.2}$.

 - *Busca 1* (até o disparo de $t_{11_2a.O1/1.5.O1}$): de acordo com a Restrição 2B, nenhuma pode ser disparada transição até o disparo de $t_{11_2a.O1/1.5.O1}$.
 - *Busca 2* (do disparo de $t_{11_2a.O1/1.5.O1}$ até o disparo de $t_{13_2a.O1/14_5.O1}$): corresponde a busca do seqüente $\Gamma_0, p_{4_5.O1}, !t_{3_5.O1}, \dots, !t_{26_5.O1}, t_{14_5.O1} \vdash \Gamma_f$, que resulta em dois cenários. Para o **Cenário 1-1** $\Gamma_0 = p_{2_5.O1}$; $\Gamma_f = p_{16_5.O1}$, para o **Cenário 1-2** $\Gamma_0 = p_{3_5.O1}$; $\Gamma_f = p_{16_5.O1}$.

- *Busca 3* (do disparo de $t_{13_2a.O1/14_5.O1}$ até o disparo de $t_{15_2.O1a/24_5.O1}$): corresponde a busca do seqüente $\Gamma_0, p_{4_5.O1}, !t_{3_5.O1}, \dots, !t_{26_5.O1}, t_{14_5.O1} \vdash \Gamma_f$, que resulta em apenas um cenário, onde $\Gamma_0 = p_{16_5.O1}; \Gamma_f = p_{25_5.O1}$.
- *Busca 4* (a partir do disparo de $t_{15_2.O1a/24_5.O1}$): esta busca não foi considerada relevante para a verificação da propriedade analisada.
- *Definição de cenários* – A construção da árvore resulta em dois cenários: onde $\Gamma_0 = \emptyset, \Gamma_f = p_{1_6.O1}$:
 - **Cenário 1-1:** $t_{11_2a.O1/1.5.O1}; t_{3_5.O1}; t_{7_5.O1}; t_{11_5.O1}; t_{13_2a.O1/14_5.O1}; t_{18_5.O1}; t_{21_5.O1}; t_{24_5.O1}$.
 - **Cenário 1-2:** $t_{11_2a.O1/1.5.O1}; t_{5_5.O1}; t_{9_5.O1}; t_{3_5.O1}; t_{7_5.O1}; t_{11_5.O1}; t_{13_2a.O1/14_5.O1}; t_{18_5.O1}; t_{21_5.O1}; t_{24_5.O1}$.
- **Cenário 2-1:** Não contém transições deste objeto.

B.2.1.20. Etapa 5.2 – Elaboração de Hipóteses ($O_{1.5}$ - Guindaste Mesa)

Nenhuma hipótese é elaborada.

B.2.1.21. Etapa 5.3 – Parte Contínua – Evolução de variáveis contínuas e datas de disparos ($O_{1.5}$ - Guindaste Mesa)

- **Cenário 1-1**
 - De acordo com a Restrição 2B, $\theta_{11_2.O1a/1_5.O1} = \theta_{5_2.O1/3_7.O1}$.
 - $\theta_{3_5.O1} = \theta_{11_2.O1a/1_5.O1}$.
 - $\theta_{7_5.O1} = \theta_{3_5.O1} + K_{\theta_G}; \theta_{11_5.O1} = \theta_{7_5.O1} + K_{\theta_G}; \theta_{13_2.O1a/14_5.O1} \geq \theta_{11_5.O1} + K_{\theta_G}$.
 - $\theta_{18_5.O1} = \theta_{14_5.O1} + 35 * K_{\theta_G}; \theta_{21_5.O1} = \theta_{18_5.O1} + 35 * K_{\theta_G}; \theta_{24_5.O1} \geq \theta_{21_5.O1} + 35 * K_{\theta_G}$.
- **Cenário 1-2**
 - De acordo com a Restrição 2B, $\theta_{11_2.O1a/1_5.O1} = \theta_{5_2.O1/3_7.O1}$.
 - $\theta_{5_5.O1} = \theta_{11_2.O1a/1_5.O1}; \theta_{9_5.O1} = \theta_{5_5.O1}; \theta_{3_5.O1} = \theta_{9_5.O1}$.
 - $\theta_{7_5.O1} = \theta_{3_5.O1} + K_{\theta_G}; \theta_{11_5.O1} = \theta_{7_5.O1} + K_{\theta_G}; \theta_{13_2.O1a/14_5.O1} \geq \theta_{11_5.O1} + K_{\theta_G}$.
 - $\theta_{18_5.O1} = \theta_{14_5.O1} + 35 * K_{\theta_G}; \theta_{21_5.O1} = \theta_{18_5.O1} + 35 * K_{\theta_G}; \theta_{24_5.O1} \geq \theta_{21_5.O1} + 35 * K_{\theta_G}$.

Como resultado desta análise e da análise dos demais objetos, tem-se que:

- $\theta_{18_74.O1/3_2.O1} = \theta_{1_2.O1}$.
- $\theta_{5_2.O1/3_7.O1} = \theta_{1_2.O1} + K_{\theta_C1}$.

- $\theta_{12_2.O1} = \theta_{1_2.O1} + K_{\theta_C1}$; $\theta_{13_2.O1a/14_5.O1} = \theta_{1_2.O1} + K_{\theta_C1} + 3 * K_{\theta_G}$.
- $\theta_{14_2.O1} = \theta_{1_2.O1} + K_{\theta_C1} + 3 * K_{\theta_G} + \theta_d$.
- $\theta_{15_2.O1a/24_5.O1} = \max (\theta_{1_2.O1} + K_{\theta_C1} + 3 * K_{\theta_G} + \theta_d, \theta_{1_2.O1} + K_{\theta_C1} + 39 * K_{\theta_G})$.
- $\theta_{7_2.O1/4_7.O1} = \max (\theta_{1_2.O1} + K_{\theta_C1} + 3 * K_{\theta_G} + \theta_d, \theta_{1_2.O1} + K_{\theta_C1} + 39 * K_{\theta_G})$.
- Condição para a **Propriedade 2** ser verdadeira é: $\max (K_{\theta_C1} + 3 * K_{\theta_G} + \theta_d; K_{\theta_C1} + 39 * K_{\theta_G}) \leq 1800 - K_{\theta_C1}$.
- Substituindo os valores de acordo com o definido na Seção 7.3.6: $\theta_d \in [716,1; 924,5] \Rightarrow \max (1314,5; 1470) \leq 1500 \Rightarrow$ no caso dos **Cenários 1-1 e 1-2** a **Propriedade 2** é verdadeira.

B.2.1.22. *Etapas 5 – Análise do Objeto O_{1,5}- Guindaste Mesa*

A análise deste objeto é semelhante à do objeto O_{1,5}.

Como resultado desta análise e da análise dos demais objetos, tem-se que:

- $\theta_{5_75.O1/4_2.O1} = \theta_{1_2.O1}$.
- $\theta_{6_2.O1/2_6.O1} = \theta_{1_2.O1} + K_{\theta_C2}$.
- $\theta_{12_2.O1} = \theta_{1_2.O1} + K_{\theta_C2}$; $\theta_{13_2.O1b/14_5.O2} = \theta_{1_2.O1} + K_{\theta_C2} + 3 * K_{\theta_G}$.
- $\theta_{14_2.O1} = \theta_{1_2.O1} + K_{\theta_C2} + 3 * K_{\theta_G} + \theta_d$.
- $\theta_{15_2.O1b/24_5.O2} = \max (\theta_{1_2.O1} + K_{\theta_C2} + 3 * K_{\theta_G} + \theta_d, \theta_{1_2.O1} + K_{\theta_C2} + 39 * K_{\theta_G})$.
- $\theta_{8_2.O1/4_6.O1} = \max (\theta_{1_2.O1} + K_{\theta_C2} + 3 * K_{\theta_G} + \theta_d, \theta_{1_2.O1} + K_{\theta_C2} + 39 * K_{\theta_G})$.
- Condição para a **Propriedade 2** ser verdadeira é: $\max (K_{\theta_C2} + 3 * K_{\theta_G} + \theta_d, K_{\theta_C2} + 39 * K_{\theta_G}) \leq 1800 - K_{\theta_C2}$.
- Substituindo os valores de acordo com o definido na Seção 7.3.6: $\theta_d \in [716,1; 924,5] \Rightarrow \max (1264,5; 1420) \leq 1550 \Rightarrow$ no caso dos **Cenários 2-1-1 e 2-1-2** a **Propriedade 2** também é verdadeira.

B.2.1.23. *Etapas 6 – Construção dos Seqüentes Globais*

São definidos os seqüentes globais, que verificam a alcançabilidade dos **Cenários 1-1, 1-2, 2-1-1 e 2-1-2** do ponto de vista discreto:

- **Cenário 1-1:** $p_{1_2.O1}, p_{9_74.O1}, p_{2_7.O1}, p_{1_5.O1}, p_{2_5.O1}, t_{1_2.O1}, t_{2_2.O1/17_74.O1}, t_{18_74.O1/3_2.O1}, t_{5_2.O1/3_7.O1}, t_{11_2.O1a/1_5.O1}, t_{12_2.O1}, t_{13_2.O1a/14_5.O1}, t_{14_2.O1}, t_{15_2.O1a/24_5.O1}, t_{16_2.O1}, t_{7_2.O1/4_7.O1}, t_{9_2.O1}, t_{3_5.O1}, t_{7_5.O1}, t_{11_5.O1}, t_{14_5.O1} \mid p_{1_2.O1} \otimes p_{9_74.O1} \otimes p_{2_7.O1} \otimes p_{25_5.O1}$.
- **Cenário 1-2:** $p_{1_2.O1}, p_{9_74.O1}, p_{2_7.O1}, p_{1_5.O1}, p_{3_5.O1}, t_{1_2.O1}, t_{2_2.O1/17_74.O1}, t_{18_74.O1/3_2.O1}, t_{5_2.O1/3_7.O1}, t_{11_2.O1a/1_5.O1}, t_{12_2.O1}, t_{13_2.O1a/14_5.O1}, t_{14_2.O1}, t_{15_2.O1a/24_5.O1}, t_{16_2.O1}, t_{7_2.O1/4_7.O1}, t_{9_2.O1}, t_{5_5.O1}, t_{9_5.O1}, t_{3_5.O1}, t_{7_5.O1}, t_{11_5.O1}, t_{14_5.O1} \mid p_{1_2.O1} \otimes p_{9_74.O1} \otimes p_{2_7.O1} \otimes p_{25_5.O1}$.

- **Cenário 2-1-1:** $p_{1_2.O1}, p_{9_74.O1}, p_{1_75.O1}, p_{1_6.O1}, p_{1_5.O1}, p_{2_5.O1}, t_{1_2.O1}, t_{2_2.O1/17_74.O1}, t_{19_74.O1/2_75.O1}, t_{5_75.O1/4_2.O1}, t_{6_2.O1/2_6.O1}, t_{11_2.O1b/1_5.O2}, t_{12_2.O1}, t_{13_2.O1b/14_5.O2}, t_{14_2.O1}, t_{15_2.O1b/24_5.O2}, t_{16_2.O1}, t_{8_2.O1/4_6.O1}, t_{9_2.O1}, t_{3_5.O1}, t_{7_5.O1}, t_{11_5.O1}, t_{14_5.O1} \vdash p_{1_2.O1} \otimes p_{9_74.O1} \otimes p_{1_75.O1} \otimes p_{2_7.O1} \otimes p_{1_6.O1} \otimes p_{25_5.O1}$.
- **Cenário 2-1-2:** $p_{1_2.O1}, p_{9_74.O1}, p_{1_75.O1}, p_{1_6.O1}, p_{1_5.O1}, p_{3_5.O1}, t_{1_2.O1}, t_{2_2.O1/17_74.O1}, t_{19_74.O1/2_75.O1}, t_{5_75.O1/4_2.O1}, t_{6_2.O1/2_6.O1}, t_{11_2.O1b/1_5.O2}, t_{12_2.O1}, t_{13_2.O1b/14_5.O2}, t_{14_2.O1}, t_{15_2.O1b/24_5.O2}, t_{16_2.O1}, t_{8_2.O1/4_6.O1}, t_{9_2.O1}, t_{5_5.O1}, t_{9_5.O1}, t_{3_5.O1}, t_{7_5.O1}, t_{11_5.O1}, t_{14_5.O1} \vdash p_{1_2.O1} \otimes p_{9_74.O1} \otimes p_{1_75.O1} \otimes p_{2_7.O1} \otimes p_{1_6.O1} \otimes p_{25_5.O1}$.

A Fig. B.101 apresenta a ordem parcial de disparos no caso do **Cenário 1-1**.

Fig. B.101. Ordem parcial de disparos – **Cenário 1-1** – **Propriedade 2**.

B.2.1.24. Etapa 7 – Verificação das Hipóteses

Verificação da Hipótese 2A

Fazendo a fusão dos objetos $O_{1,2}$ e $O_{1,74}$, tem-se os seguintes invariantes de lugar: $p_{2_2.O1} + p_{9_74.O1} = 1$ e $p_{1_2.O1} + p_{2_2.O1} + \dots + p_{9_2.O1} = 1$, portanto, se $p_{1_2.O1} = 1$ ($t_{2_2.O1/11_74.O1}$ está habilitada $O_{1,2}$), $p_{2_2.O1} = 0$ e $p_{9_74.O1} = 1$, o que significa que $t_{2_2.O1/11_74.O1}$ também está habilitada em $O_{1,74}$.

Verificação da Hipótese 2B

Fazendo a fusão dos objetos $O_{1,2}$ e $O_{1,7}$ (e desconsiderando $t_{1_7.O1}$ por causa de R_1) tem-se o seguinte invariante de lugar: $p_{1_2.O1} + p_{2_2.O1} + p_{3_2.O1} + p_{4_2.O1} + p_{5_2.O1} + p_{7_2.O1} + p_{8_2.O1} + p_{9_2.O1} = p_{2_7.O1}$, portanto, $p_{4_2.O1} \leq p_{2_7.O1}$ (sempre que $t_{5_2.O1/3_7.O1}$ está habilitada $O_{1,12}$ também está $O_{1,7}$). Semelhantemente, fazendo a fusão de $O_{1,2}$ e $O_{1,6}$ prova-se que sempre que $t_{6_2.O1/2_6.O1}$ está habilitada $O_{1,2}$ também está $O_{1,6}$.

Verificação da Hipótese 2C

O disparo $t_{13_2.O1a/14_5.O1}$ impõe $v_G = K_{v_G}$. Além disso nenhuma equação modifica v_G , que permanece constante até o disparo de $t_{18_5.O1}$. Como $\theta_{18_5.O1} > \theta_{14_2.O1}$, a Hipótese 2C é verdadeira.

Verificação da Hipótese 2D

De forma semelhante às hipóteses anteriores, esta hipótese pode ser verificada através da fusão dos objetos $O_{1,2}$ e $O_{1,6}$.

B.3. Observações

Este anexo é uma complementação do Capítulo 7 e ilustra a aplicação do procedimento de modelagem proposto no Capítulo 3 para o estudo de caso da Usina Cruz Alta.

Além disso é apresentada também a verificação de uma propriedade de alcançabilidade. Observa-se que esta propriedade envolve os objetos Interface Mesas e Interface Fosso. Em ambos objetos algumas variáveis de interface referentes a identidade do caminhão que está descarregando cana são dinâmicas, isto é, os valores destas variáveis podem ser alterados no decorrer da execução da rede. Isto dificulta a análise destes objetos, uma vez que um aspecto da dinâmica discreta do sistema passa a ser representado por uma variável. Para evitar um excessivo número de cenários, no caso da **Propriedade 2**, foi imposta a Restrição 2A, que elimina do problema de análise todos os caminhões exceto $O_{1,2}$.

Para verificar uma **Propriedade 3** que seja equivalente a **Propriedade 2** mas sem a imposição da Restrição 2A, pode se decompor o problema em uma série de verificações de propriedades, onde o tempo de permanência do caminhão na usina é a soma do tempo de espera mais o tempo de descarregamento. Este último é dado pela **Propriedade 2**, enquanto o anterior está relacionado ao número máximo de caminhões que podem estar aguardando na fila para descarregar, e ao tempo máximo de descarregamento de cada um (que é dado por uma propriedade semelhante a **Propriedade 2**).

REFERÊNCIAS BIBLIOGRÁFICAS

- ALLA, H.; DAVID, R. Continuous and hybrid Petri nets. **Journal of Circuits, Systems and Computers**, v.8, n.1, p.159-188, 1998.
- ALUR, R. et al. The algorithmic analysis of hybrid systems. **Theoretical Computer Science**, v.138, p.3-34, 1995.
- ALUR, R.; DILL, D.A Theory of timed automata. **Theoretical Computer Science**, v.126, p.183-235, 1994.
- ANDREU, D. **Commande et supervision des procédés discontinus: une approche hybride**. 1996. 168p. Tese (Doutorado) – Université Paul Sabatier. Toulouse, 1996.
- ANTSAKLIS, P.; KOUTSOUKOS, X. On hybrid control of complex systems: a survey. Em: THE 3RD INTERNATIONAL CONFERENCE ON AUTOMATION OF MIXED PROCESSES: HYBRID DYNAMIC SYSTEMS (ADPM), Reims, 1998. **Proceedings**. [S.I.: s.n.], 1998. p.1-8.
- ANTSAKLIS, P.J.; NERODE, A. Hybrid control systems: an introductory discussion to the special issue. **IEEE Transactions on Automatic Control**, v.43, n.4, p.457-459, 1998.
- AZZOPARDI, D.; HOLDING, D.J. Petri nets and OMT for modeling and analysis of DEDS. **Control Engineering Practice**, v.5, n.10, p.1407-1415, 1997.
- BARESI, L.; PEZZÈ, M. On formalizing UML with high-level Petri nets. **Lecture notes in Computer Science** (Concurrent Object-Oriented Programming and Petri Nets, Advances in Petri Nets), v.2001, p.276-304, 2001.
- BASTIDE, R. Approaches in unifying Petri nets and the object-oriented approach. Em: THE 1ST. WORKSHOP ON OBJECT-ORIENTED PROGRAMMING AND MODELS OF CONCURRENCY, Torino, 1995. **Proceedings**. [S.I.: s.n.], 1995.
- BEEK, D.A.; ROODA, J.E.; TRIENEKENS, B.J. Hybrid modelling and simulation of time-delay elements. Em: THE 11TH EUROPEAN SIMULATION SYMPOSIUM, Erlangen, 1999. **Proceedings**. [S.I.:s.n.], 1999. p.88-92.
- BENNE, M. et al. Artificial neural networks for modelling and predictive control of an industrial evaporation process. **Journal of Food Engineering**, v.46, n.4, p.227-234, 2000.
- BONNIOL, F.; CARCENAC, F. et al. Une étude de cas pour la vérification formelle de propriétés temporelles. Em: JOURNÉES FORMALISATION DES ACTIVITÉS CONCURRENTES (FAC), Toulouse, 2002. **Actes**. Disponível em <<http://www.laas.fr/~francois/SVF/FAC02/>>. Acesso em 22 jan 2004.
- BOOCH, G. **Object-oriented analysis and design with applications**. 2.ed. Redwood City (California): Benjamin/Cummings Pub. Co., 1994. 589p.
- BOOCH, G.; RUMBAUGH, J.; JACOBSON, I. **The Unified Modeling Language user guide**. Reading (Massachusetts): Addison-Wesley, 1999. 482p.
- BOOCH, G.; RUMBAUGH, J.; JACOBSON, I. **UML: guia do usuário**. Rio de Janeiro: Campus, 2000. 472p.
- CADET, C. et al. Knowledge modeling and nonlinear predictive control of evaporators in cane sugar production plants. **Journal of Food Engineering**, v.40, n.1-2, p.59-70, 1999.

- CAMARINHA-MATOR, L.M.; RABELO, R. Chapter 14 – Balanced automation. Em: TZAFESTAS, S. **Computer Assisted Management and Control of Manufacturing Systems**. London: Springer-Verlag, 1997. p376-414.
- CANTÚ, M. **Dominando o Delphi**: a bíblia. Rio de Janeiro: Makron Books do Brasil, 1996. 1192p.
- CARDOSO, J.; VALETTE, R. **Redes de Petri**. Florianópolis: Editora da UFSC, 1997. 212p.
- CHAMPAGNAT, D. **Supervision des systèmes discontinus**: definition d'un modèle hybride et pilotage en temps-réel. 1998. 151p. Tese (Doutorado) – Université Paul Sabatier. Toulouse, 1998.
- CLARKE, E. Verification tools for finite-state concurrent systems. **Lecture notes in Computer Science** (A decade of concurrency - reflections and perspectives). v.8030, p.124-175, 1993.
- CLARKE, E.M.; WING, J.M. Formal methods: state of the art and future directions. **ACM Computing Surveys**, v.28, n.4, p.623-643, 1996.
- DASSAULT. **Genie theme 1 annexe au rapport final**: programmation et verification du logiciel d'application de la fonction trains-trappes. 1996. (Rapport N. DGT-66647).
- DASSAULT. **Genie theme 1**: specification de la fonction trains-trappes d'un système atterrisseur version préliminaire. 1995. (Rapport N. 63491).
- DAVID, R.; ALLA, H. Petri nets for modeling of dynamic systems: a survey. **Automatica**, v.30, n.2, p.175-201, 1994.
- DELATOUR, J. **Contribution a la specification des systèmes temps réel**: l'approche UML/PNO. 2003. 180p. Tese (Doutorado) – Université Paul Sabatier. Toulouse, 2003.
- DI BENEDETTO, M.D.; LYGEROS, J. Centre of excellence DEWS: a new experiment in research, innovation and use of hybrid systems. Em: IFAC CONFERENCE ON ANALYSIS AND DESIGN OF HYBRID SYSTEMS (ADHS), Saint-Malo, 2003. **Proceedings**. [S.I.: s.n.], 2003. p.21-27.
- DRATH, R. Hybrid object nets: an object oriented concept for modelling complex hybrid systems. Em: THE 3RD INTERNATIONAL CONFERENCE ON AUTOMATION OF MIXED PROCESSES: HYBRID DYNAMIC SYSTEMS (ADPM), Reims, 1998. **Proceedings**. [S.I.: s.n.], 1998. p.436-442.
- ELHAQ, S.L.; GIRI, F.; UNBEHAUEN, H. Modelling, identification and control of sugar evaporation - theoretical design and experimental evaluation. **Control Engineering Practice**, v.7, n.8, p.931-942, 1999.
- ELKOUTBI, M.; KELLER, R.K. User Interface Prototyping Based on UML Scenarios and High-Level Petri Nets. **Lecture notes in Computer Science**, v.1825, p.166-186, 2000. / Apresentado a 21st International Conference on Application and theory of Petri Nets, Aarhus, 2000.
- GARCIA, A.; ACEBES, L.F.; PRADA, C. Modelling and simulation of batch processes: a case study. Em: THE 15TH IFAC WORLD CONGRESS, Barcelona, 2002. **Proceedings**. San Diego: Elsevier Inc., 2003.
- GARCIA, H.E. A hierarchical platform for implementing hybrid systems in process control. **Control Engineering Practice**, v.5, n.6, p.779-789, 1997.
- GENRICH, H. Predicate/transition nets. **Lecture notes in Computer Science** (Petri Nets: Central Models and Their Properties, Advances in Petri Nets 1986, Part I), v.254, p.207-247, 1987.

- GIESE, H.; GRAF, J.; WIRTZ, G. Closing the gap between object-oriented modeling of structure and behavior. **Lecture notes in Computer Science**, v.1723, p.534-549, 1999. / Apresentado a 2nd International Conference on The Unified Modeling Language (UML), Fort Collins (Colorado), 1999.
- GIRARD, J-Y. Linear logic. **Theoretical Computer Science**, v.50, p.1-102, 1987.
- GIRAULT, F.; PRADIN-CHEZALVIEL, B.; VALETTE, R. A logic for Petri nets. **Journal Européen des Systèmes Automatisés**, v.31, n.3, p.525-542, 1997.
- GUÉGUEN, H.; LEFEBVRE, M. A comparison of mixed specification formalisms. Em: THE 4TH INTERNATIONAL CONFERENCE ON AUTOMATION OF MIXED PROCESSES: HYBRID DYNAMIC SYSTEMS (ADPM), Dortmund, 2000. **Proceedings**. Aachen: Shaker Verlag, 2000. p.133-138.
- GUÉGUEN, H.; ZAYTOON, J. Principes de la vérification des systèmes hybrides. Em: COLLOQUE FRANCOPHONE SUR LA MODÉLISATION DES SYSTÈMES RÉACTIFS (MSR), Toulouse, 2001. **Actes**. Cachan: Hermes Science Publishing, 2001. p.427-444.
- GUNTER, C.; GEHLOT, V. Nets as tensor theories. Em: THE 10TH CONFERENCE ON APPLICATION AND THEORY OF PETRI NETS, Bonn, 1989. **Proceedings**. [S.I.: s.n.], 1989. p.174-191.
- HALBWACHS, N. et al. Programming and verifying real-time systems by means of the synchronous data-flow programming language Lustre. **IEEE Transactions on Software Engineering**, v.18, n.9, p.785-793, 1992.
- HENZINGER, T.A. et al. HyTech: a model checker for hybrid systems. **Software Tools for Technology Transfer**, v.1, p.110-122, 1997.
- HO, Y.C. Basic research, manufacturing automation, and putting the cart before the horse. **IEEE Transactions on Automatic Control**, v.AC-32, n.12, p.1042-1043, 1987.
- HUGOT, E. **Handbook of cane sugar engineering**. 3.ed. New York: Elsevier Science Pub. Co., 1986. 1166p.
- INCROPERA, F.P.; DE WITT, D.P. **Fundamentals of heat and mass transfer**. 3.ed. New York: Wiley, 1990. 919p.
- JACOBSON, I.; BOOCH, G.; RUMBAUGH, J. **The unified software development process**. Reading (Massachusetts): Addison-Wesley, 1999. 463p.
- JENSEN, K. **Coloured Petri nets: basic concepts, analysis methods and practical use**. 2.ed. Berlin: Springer-Verlag, 1997. v.1.
- JESUS, C.D.F.; ALMEIDA, P.I.F.; Simulação do controle do processo de evaporação de múltiplo efeito utilizado na fabricação de açúcar. Em: II CONGRESSO DE ENGENHARIA DE PROCESSOS DO MERCOSUL (ENPROMER), Florianópolis, 1999. **Proceedings**. [S.I.: s.n.], 1999.
- KHALFAOUI, S. et al. Extraction des scénarios critiques à partir d'un modèle RdP à l'aide de la logique. Em: COLLOQUE FRANCOPHONE SUR LA MODÉLISATION DES SYSTÈMES RÉACTIFS (MSR), Toulouse, 2001. **Actes**. Cachan: Hermes Science Publishing, 2001. p.409-424.
- KHALFAOUI, S. **Méthode de recherche des scénarios redoutés pour l'évaluation de la sûreté de fonctionnement des systèmes mécatroniques du monde automobile**. 2003. 137p. Tese (Doutorado) – Université Paul Sabatier. Toulouse, 2003.

- LAKOS, C. From coloured Petri nets to object Petri nets. **Lecture notes in Computer Science**, v.935, p. 223-228, 1995. / Apresentado a 16th International Conference on Application and theory of Petri Nets, Torino, 1995.
- LAKOS, C. The consistent use of names and polymorphism in the definition of Object Petri Nets. **Lecture notes in Computer Science**, v.1091, p.380-389, 1996. / Apresentado a 17th International Conference on Application and theory of Petri Nets, Osaka, 1996.
- LAURET, P.; BOYER, H.; GATINA, J.C. Hybrid modelling of a sugar boiling process. **Control Engineering Practice**, v.8, n.3, p.299-310, 2000.
- LEMMON, M.; HE, K.X.; MARKOVSKY, I. Supervisory hybrid systems. **IEEE Control Systems**, v.19, n.4, p.42-55, 1999.
- LENNARTSON, B. et al. Hybrid systems in process control. **IEEE Control Systems**, v.16, n.5, p.45-46, 1996.
- LESAR. Grenoble. **Lustre/Lesar**. Disponível em <<http://www-verimag.imag.fr/SYNCHRONE/lustre.html>>. Acesso em 15 jun 2003.
- LJUNG, M. **Formal modelling and automatic verification of Lustre programs using np-tools**. 1999. Dissertação (Mestrado) – Department of Tele-informatics, Royal Institute of Technology. Stockholm, 1999.
- MIYAGI, P.E. **Control system design, programming and implementation for discrete event production systems by using mark flow graph**. 1988. Tese (Doutorado) – Tokyo Institute of Technology. Tokyo, 1988.
- MIYAGI, P.E. **Controle programável: fundamentos do controle de sistemas a eventos discretos**. São Paulo: Edgard Blücher, 1996. 194p.
- MURATA, T. Petri Nets: properties, analysis and applications. **Proceedings of the IEEE**, v.77, n.4, p.541-580, 1989.
- NIELSEN, K.M.; PEDERSEN, T.S.; NIELSEN, J.F.D. Simulation and control of a multiple effect evaporator. Em: UKAC CONTROL CONFERENCE, Exeter, 1996. **Proceedings**. [S.I.: s.n.], 1996.
- NIMMO, I. Future of supervisory systems in process industries: lessons for discrete manufacturing. **Annual Reviews in Control**, v.23, p.45-52, 1999.
- PALUDETTO, M. **Sur la commande des procédés industriels: une méthodologie basée objets et réseaux de Petri**. 1991. 264p. Tese (Doutorado) – Université Paul Sabatier. Toulouse, 1991.
- PERKUSICH, A.; PERKUSICH, M.L.B.; CHANG, S.K. Object oriented design, modular analysis, and fault-tolerance of real-time control software systems. **International Journal of Software Engineering and Knowledge Engineering**, v.6, n.3, p.447-476, 1996.
- PETRI, C. **Kommunikation mit automaten**. 1962. Tese (Doutorado) – Institut für Instrumentelle Mathematik. Bonn, 1962.
- PETTERSON, P.; LARSEN, K.G. Uppaal2k. **Bulletin of the European Association for Theoretical Computer Science**, v.70, p.40-44, 2000.
- SALSBURY, T.I. **Fault detection and diagnosis in HVAC systems using analytical models**. 1996. Tese (Doutorado) – Dep. of Civil and Building Engineering, Loughborough University. Loughborough, 1996.

- SCHÖF, S.; SONNENSCHNEIN, M.; WIETING, R. High-level modeling with THORNS. Em: THE 14TH INTERNATIONAL CONGRESS ON CYBERNETICS, Namur, 1995. **Proceedings**. [S.I.: s.n.], 1995. p.453-458.
- SIBERTIN-BLANC, C. A client-server protocol for the composition of Petri nets. **Lecture notes in Computer Science**, v.691, p. 337-396, 1993. / Apresentado a 14th International Conference on Application and theory of Petri Nets, Chicago, 1993.
- SILVA, B. I. et al. An assessment of the current status of algorithmic approaches to the verification of hybrid systems. Em: THE 40TH IEEE CONFERENCE ON DECISION AND CONTROL, Orlando, 2001. **Proceedings**. Piscataway: IEEE Press, 2001. p.2867-2874.
- SILVA, B.I. et al. Modeling and verifying hybrid dynamic systems using Checkmate. Em: THE 4TH INTERNATIONAL CONFERENCE ON AUTOMATION OF MIXED PROCESSES: HYBRID DYNAMIC SYSTEMS (ADPM), Dortmund, 2000. **Proceedings**. Aachen: Shaker Verlag, 2000. p.323-328.
- SILVA, M. et al. Petri nets and production systems. **Lecture notes in Computer Science** (Lectures on Petri nets II: applications), v.1492, p.85-124, 1998.
- SMV. Pittsburgh. **The SMV System**. Disponível em <<http://www-2.cs.cmu.edu/~modelcheck/smv.html>>. Acesso em 15 jun 2003.
- STURSBURG, O. et al. Block-diagram based modelling and analysis of hybrid processes under discrete control. **Journal Européen des Systèmes Automatisés**, v.32, n.9/10, p.1097-1118, 1998.
- UPPAAL. Uppsala. **UPPAAL**. Disponível em <<http://www.docs.uu.se/docs/rtnv/uppaal/>>. Acesso em 15 jun 2003.
- VALENTIN-ROUBINET, C. Hybrid systems modelling: mixed Petri nets. Em: THE 3RD IMACS, IEEE, WORLD SES, MULTICONFERENCE ON CIRCUITS, SYSTEMS, COMMUNICATIONS AND COMPUTERS (CSCC), Athens, 1999. **Proceedings**. Piscataway: IEEE Press, 1999. p.223-228.
- VALK, R. Petri nets as token objects: an introduction to elementary object nets. **Lecture notes in Computer Science**, v.1420, p.1-25, 1998. / Apresentado a 19th International Conference on Application and theory of Petri Nets, Lisbon, 1998.
- VILLANI, E. **Abordagem híbrida para modelagem de sistemas de ar condicionado em edifícios inteligentes**. 2000. 154p. Dissertação (Mestrado) – Escola Politécnica da Universidade de São Paulo. São Paulo, 2000.
- WANG, L.; PERKUSICH, M.L.B.; CHANG, S.K. Object-oriented Petri nets for modelling and analysis of automated manufacturing systems. **Computer Integrated Manufacturing Systems**, v.26, n.2, p.111-125, 1996.
- WIETING, R. Hybrid high-level nets. Em: THE 28TH WINTER SIMULATION CONFERENCE, Coronado, 1996. **Proceedings**. Piscataway: IEEE Press, 1996. p.848-855.