UNIVERSIDADE FEDERAL DE SANTA CATARINA
CENTRO DE TECNOLÓGICO
PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA DE AUTOMAÇÃO E SISTEMAS

Rafael Garlet de Oliveira

Controle Supervisório Hierárquico de Processos Industriais Modelados por Abstrações Sucessivas de Sistemas a Eventos Discretos

Florianópolis
2024

Rafael Garlet de Oliveira

Controle Supervisório Hierárquico de Processos Industriais Modelados por Abstrações Sucessivas de Sistemas a Eventos Discretos

Tese submetida ao Programa de Pós-Graduação em Engenharia de Automação e Sistemas da Universidade Federal de Santa Catarina para a obtenção do título de Doutor em Engenharia de Automação e Sistemas.
Orientador: Prof. Max Hering de Queiroz, Dr.
Coorientador: Prof. José Eduardo Ribeiro Cury, Dr.

Florianópolis
2024

Ficha catalográfica gerada por meio de sistema automatizado gerenciado pela BU/UFSC.
Dados inseridos pelo próprio autor.

Garlet de Oliveira, Rafael
Controle Supervisório Hierárquico de Processos Industriais Modelados por Abstrações Sucessivas de Sistemas a Eventos Discretos / Rafael Garlet de Oliveira ; orientador, Max Hering de Queiroz, coorientador, José Eduardo Ribeiro Cury, 2024.
151 p.

Tese (doutorado) - Universidade Federal de Santa Catarina, Centro Tecnológico, Programa de Pós-Graduação em Engenharia de Automação e Sistemas, Florianópolis, 2024.

Inclui referências.

1. Engenharia de Automação e Sistemas. 2. Sistemas a Eventos Discretos. 3. Teoria de Controle Supervisório. 4. Controle Hierárquico. 5. Abstrações Sucessivas. I. Hering de Queiroz, Max. II. Ribeiro Cury, José Eduardo. III. Universidade Federal de Santa Catarina. Programa de Pós Graduação em Engenharia de Automação e Sistemas. IV. Título.

Rafael Garlet de Oliveira

Controle Supervisório Hierárquico de Processos Industriais Modelados por Abstrações Sucessivas de Sistemas a Eventos Discretos

O presente trabalho em nível de doutorado foi avaliado e aprovado por banca examinadora composta pelos seguintes membros:

Prof. José Eduardo Ribeiro Cury, Dr.
Universidade Federal de Santa Catarina – UFSC

Prof. Antonio Eduardo Carrilho da Cunha, Dr.
Instituto Militar de Engenharia – IME

Prof. Marcos Vicente de Brito Moreira, Dr.
Universidade Federal do Rio de Janeiro – UFRJ

Prof. Públio Macedo Monteiro Lima, Dr.
Universidade Federal de Santa Catarina – UFSC

Certificamos que esta é a **versão original e final** do trabalho de conclusão que foi julgado adequado para obtenção do título de Doutor em Engenharia de Automação e Sistemas.

Documento assinado digitalmente
Julio Elias Normey Rico
Data: 16/09/2024 12:19:52-0300
CPF: ***.840.859-**
Verifique as assinaturas em https://v.ufsc.br

Coordenação do Programa de
Pós-Graduação

Documento assinado digitalmente
Max Hering de Queiroz
Data: 16/09/2024 10:25:51-0300
CPF: ***.550.079-**
Verifique as assinaturas em https://v.ufsc.br

Prof. Max Hering de Queiroz, Dr.
Orientador

Florianópolis, 2024.

Dedico esta tese à memória do meu pai
Carlos Renato Victória de Oliveira.

AGRADECIMENTOS

Em primeiro lugar gostaria de agradecer aos meus orientadores Max Hering de Queiroz e José Eduardo Ribeiro Cury, por todo apoio na realização desse trabalho, desenvolvimento dos conceitos e escrita da tese e artigos. Durante todo esse período de doutorado, ao longo de muitas reuniões semanais pude conhecer não só os excelentes profissionais que são, mas também as excelentes pessoas.

Agradeço a todos os meus professores que me transmitiram o conhecimento muito além do básico para minha formação. Agradeço aos meus colegas pelo perído pré-pandemia, em que estive mais presente na universidade, por todo apoio e convívio nos laboratórios e durante as disciplinas.

Agradeço ao Instituto Federal Catarinense por proporcionar meu afastamento integral durante quatro anos, para que fosse possível me dedicar à minha formação. Agradeço ainda à Universidade Federal de Santa Catarina por disponibilizar a estrutura e laboratórios para desenvolvimento da pesquisa.

Por fim, agradeço à minha esposa Aline e a toda minha família pelo apoio incondicional, que foi fundamental para que eu conseguisse concluir esse desafio.

“Embora mil vezes, mil homens
possa alguém em batalhas conquistar,
ainda assim, maior conquistador
é aquele que conquista a si mesmo”
(Dhammapada, 103)

RESUMO

Nesta tese são desenvolvidas contribuições para o controle supervisório hierárquico de sistemas a eventos discretos (SEDs), viabilizando sua aplicação em processos industriais comandados por um circuito de componentes. Tais sistemas tipicamente possuem natureza contínua, combinada com uma dinâmica a eventos discretos complexa, relacionada a intertravamentos de segurança e outros requisitos lógicos sobre os componentes do processo. Inicialmente, são desenvolvidas estratégias de modelagem e de implementação visando a aplicação da teoria de controle supervisório a um processo industrial típico. Essas estratégias abrangem a preempção de eventos não controláveis, a interação entre supervisor e controle PID e a implementação em redes *Foundation Fieldbus*. Em seguida, tendo em vista a modelagem de circuitos de componentes de processos industriais, como diferentes tipos de válvulas industriais, com o objetivo de evitar o problema da explosão de estados, é desenvolvida uma estratégia de modelagem por abstrações sucessivas, empregando o controle supervisório hierárquico de sistemas a eventos discretos. A cada nível de abstração, os componentes são associados sucessivamente em série ou em paralelo, resultando em modelos abstratos equivalentes intermediários com estrutura isomórfica à de um componente individual, obtendo ao fim um único modelo equivalente que representa o comportamento do circuito. Neste contexto, mostra-se que, ao obter o modelo equivalente para um circuito contendo uma válvula de controle, a propriedade de observador do mapa repórter associado não é atingida, e que esse é um requisito apenas suficiente para garantir o não-bloqueio na estrutura hierárquica. Isto posto, com o intuito de flexibilizar a propriedade de observador, são formalizadas novas condições baseadas em eventos confiáveis e mostra-se que a elegibilidade desses eventos confiáveis em especificações controláveis no alto nível hierárquico passa a ser uma das condições para o não-bloqueio. Por fim, como resultado principal da tese, é formalizada a abordagem interníveis que permite o controle supervisório de um sistema formado por um processo industrial comandado por um modelo de válvula equivalente, mesmo com a sincronização de eventos reais e abstratos no alto nível, diferente dos resultados encontrados na literatura. Em conclusão, a abordagem proposta é aplicada a um exemplo prático de um processo industrial comandado por um circuito contendo uma válvula de controle em série com uma válvula de bloqueio, demonstrando a viabilidade dos métodos para modelagem e controle supervisório hierárquico ótimo e não bloqueante.

Palavras-chave: Sistemas a Eventos Discretos; Teoria de Controle Supervisório; Controle Hierárquico; Abstrações Sucessivas; Eventos Confiáveis; Abordagem Interníveis.

ABSTRACT

This thesis presents contributions to the hierarchical supervisory control of discrete event systems (DES), aiming the application on industrial processes controlled by a circuit of components. This type of process typically exhibits a continuous dynamic, combined with a complex discrete event dynamic associated to safety interlocks and other logic requirements for the process components. Initially, modelling and implementation strategies are developed aiming the application of the supervisory control theory to a typical industrial process. These strategies address the preemption of uncontrollable events, the interaction between the supervisor and the PID control, and the implementation on Foundation Fieldbus systems. Later, considering the modelling of component circuits, such as different types of industrial valves, aiming to avoid the state explosion problem, a strategy of modelling by successive abstractions is proposed, employing the hierarchical supervisory control of discrete event systems. In each abstract level, the componets are associated successively in series or in parallel, resulting in intermediary equivalent abstract models, with a structure isomorphic to a single compenent, and finally in a single abstract equivalent model representing the entire circuit behavior. In this context, upon obtaining the equivalent model for a circuit containing a control valve, the observer property in the associated reporter map is not achieved, and this property is proved to be only sufficient for ensuring nonblocking in the hierarchical structure. Then, with the objective of weaken the observer property, new conditions based on reliable events are defined, and the eligibility of the reliable events on the high-level controllable specifications becomes one of the conditions to guarantee nonblocking. Finally, in order to deal with the synchronization of abstract events with real events at the high-level in this type of structure, the inter-level approach is proposed as the main result of the thesis. This approach allows the supervisory control of an industrial process controlled by an abstract equivalent model, even with the synchronization of abstract with real events, different of the results in the literature. In conclusion, a practical example is presented using the proposed approach in an industrial process controlled by a control valve in series with an on-off valve, showing the applicability of the methods for modeling and obtaining the nonblocking optimal hierarchical supervisory control.

Keywords: Discrete Event Systems; Supervisory Control Theory; Hierarchical Control; Successive Abstractions; Reliable Events; Inter-Level Approach.

LISTA DE FIGURAS

Figura 1 – Processo industrial comandado por um circuito de componentes. . . 20
Figura 2 – Exemplo de um autômato. 31
Figura 3 – Arquitetura para controle hierárquico. 35
Figura 4 – Exemplo de abstração de modelo com dois níveis hierárquicos. . . . 37
Figura 5 – Exemplo de planta operacional com vocalizações. 41
Figura 6 – Arquitetura detalhada para controle hieráquico. 42
Figura 7 – Exemplo de arquitetura completa de controle hierárquico. 43
Figura 8 – Planta operacional e mapa repórter sem consistência de controle. . 45
Figura 9 – Planta operacional e mapa repórter com consistência de controle. . 45
Figura 10 – Palavras vocais parceiras. 47
Figura 11 – Eliminação das palavras vocais parceiras. 48
Figura 12 – Planta operacional sem palavras vocais parceiras. 49
Figura 13 – Estrutura de controle hierárquico sem consistência de marcação. . . 50
Figura 14 – Estrutura de controle hierárquico com mapa repórter não observador. 53
Figura 15 – Processo industrial comandado por uma válvula de bloqueio. 54
Figura 16 – Processo industrial comandado por uma válvula de bloqueio: (a) modelo de níveis no tanque $\mathbf{G_N}$ e (b) modelo da válvula de bloqueio $\mathbf{G_V}$. 55
Figura 17 – Processo industrial comandado por uma válvula de bloqueio: (a) modelo da preempção $\mathbf{G_P}$ e (b) modelo da vazão no tanque $\mathbf{G_{VAZ}}$. 55
Figura 18 – $\mathbf{G}$: Autômato da planta global de um processo industrial comandado por uma válvula de bloqueio. 56
Figura 19 – $\mathbf{G^{op}}$: Modelo da planta operacional com as vocalizações em um processo industrial comandado por uma válvula de bloqueio. 56
Figura 20 – $\mathbf{G^{ge}}$: Modelo da planta do gerente em um processo industrial comandado por uma válvula de bloqueio. 58
Figura 21 – Processo industrial comandado por uma válvula de bloqueio: (a) especificação E^{ge} para evitar *overflow*, (b) supervisor gerencial $\mathcal{S}^{ge}$. 58
Figura 22 – Planta piloto situada no Departamento de Automação e Sistemas. . 61
Figura 23 – Diagrama de instrumentação do processo estudado. 61
Figura 24 – (a) Diagrama com intervalos de operação para os níveis no tanque e (b) autômato **$G_{Níveis}$**: que representa as mudanças de níveis no tanque. 65
Figura 25 – **G_{Chave}**: autômato que modela o comportamento da chave seletora. 66
Figura 26 – (a) **G_{Bomba}**: autômato que modela o comportamento da bomba e (b) **$G_{Válvula}$**: autômato que representa a o comportamento da válvula. . 67

Figura 27 – (a) $\mathbf{G_{PB}}$: preempção pelos eventos da bomba e (b) $\mathbf{G_{PV}}$: preempção pelos eventos da válvula. 67
Figura 28 – $\mathbf{G_{Vazão}}$: modelo que representa a vazão no tanque. 68
Figura 29 – Especificação de ação reativa na bomba E_{AB} (a) e na válvula E_{AV} (b). 69
Figura 30 – E_{IBV}: Especificação de intertravamento entre bomba e válvula. . . 69
Figura 31 – E_M: Especificação de modos de operação. 70
Figura 32 – $\mathcal{S}_{\text{MR}}$: Supervisor de modos de operação reduzido. 71
Figura 33 – $\mathcal{S}_{CoordR}$: Coordenador reduzido de resolução de conflito. 72
Figura 34 – Arquitetura de implementação dos supervisores e controle PID. . . . 73
Figura 35 – Estratégia de controle na rede Foundation Fieldbus. 74
Figura 36 – Gráfico com resultados experimentais. De cima para baixo: evolução da chave seletora no painel IHM e desabilitação da ação de *Start*, evolução da bomba, válvula de controle, nível e SP. 75
Figura 37 – Simbologia em Diagramas ISA: (a) válvula de bloqueio, (b) válvula de controle. 79
Figura 38 – Circuito de válvulas representado em um diagrama. 79
Figura 39 – (a) $\mathbf{G_{Bomba}}$: Modelo de bomba centrífuga com evento $BMantem$ e (b) $\mathbf{G_{Valvula}}$: modelo de válvula de bloqueio com possibilidade de falha. 80
Figura 40 – Modelos de preempção da bomba: $\mathbf{G_{PB}}$ (a) e da válvula: $\mathbf{G_{PV}}$ (b). . 80
Figura 41 – $\mathbf{G_{Vazao}}$: Modelo de vazão no tanque 81
Figura 42 – (a) E_{AB}: Especificação de ação reativa da bomba (b) E_{AV}: Especificação de ação reativa da válvula. 81
Figura 43 – (a) E_M: Especificação de modos de operação. 82
Figura 44 – Diagrama industrial de planta com duas válvulas de bloqueio em paralelo (a) e com três válvulas de bloqueio, sendo uma em paralelo com duas em série (b). 83
Figura 45 – E_M: Especificação de modos de operação para processo com duas válvulas em paralelo. 83
Figura 46 – E_M: Especificação de modos de operação para processo com uma válvula em paralelo com outras duas em série. 84
Figura 47 – Abstrações sucessivas em um circuito de componentes. 86
Figura 48 – Arquitetura multinível para circuito de válvulas, onde $\mathbf{G}_{\mathbf{12}}^{\mathbf{op}}$ e $\mathbf{G}_{\mathbf{34}}^{\mathbf{op}}$ são as plantas do operador associando as válvulas em série, $\mathbf{G}_{\mathbf{1234}}^{\mathbf{op}}$ representa a associação em paralelo, $\mathbf{G}^{\mathbf{Veq}}$ é a abstração do circuito numa válvula equivalente e $\mathbf{G_{proc}}$ modela os demais componentes do processo industrial. 86
Figura 49 – Modelos para válvulas de bloqueio em série com travamento: (a) $\mathbf{G}_{\mathbf{1}}^{\mathbf{V}}$ com estado inicial fechada e (b) $\mathbf{G}_{\mathbf{2}}^{\mathbf{V}}$ com estado inicial aberta. . . . 88

Figura 50 – E_{12}: especificação local para válvulas em série. 88
Figura 51 – $\mathbf{G_{12}^{voc}}$: modelo de vocalizações para válvulas em série, onde V1A, V1F, V1M, V1TA, V1TF correspondem aos eventos da válvula 1 V_{1Abre}, V_{1Fecha}, $V_{1Mantem}$, $V_{1TAberta}$ e $V_{1TFechada}$, análogo também para a válvula 2; e A, F, M, TA, TF correspondem aos eventos a serem vocalizados V_{12Abre}, $V_{12Fecha}$, $V_{12Mantem}$, $V_{12TAberta}$ e $V_{12TFechada}$. 89
Figura 52 – $\mathbf{G_{12}^{voc}}$: modelo de vocalizações para duas válvulas em série representado como autômato de Mealy. 90
Figura 53 – $\mathbf{G_{12}^{op}}$: planta operacional para duas válvulas em série. 91
Figura 54 – $\mathbf{G_{12}^{Veq}}$: abstração de duas válvulas em série. 92
Figura 55 – Modelos para válvulas de bloqueio em paralelo com travamento: (a) $\mathbf{G_1^V}$ com estado inicial fechada e (b) $\mathbf{G_2^V}$ com estado inicial fechada. 93
Figura 56 – E_{12}: especificação para duas válvulas de bloqueio em paralelo. . . . 93
Figura 57 – $\mathbf{G_{12}^{voc}}$: modelo de vocalizações para válvulas de bloqueio em paralelo representado como autômato de Mealy. 94
Figura 58 – $\mathbf{G_{12}^{op}}$: planta operacional para duas válvulas em paralelo. 95
Figura 59 – $\mathbf{G_{12}^{Veq}}$: abstração de duas válvulas em paralelo. 96
Figura 60 – (a) $\mathbf{G}_1^V$: Modelo de uma válvula de controle em uma configuração série. (b) $\mathbf{G}_2^V$: Modelo de uma válvula de bloqueio em uma configuração série. 97
Figura 61 – E_{12}: Especificação local para duas válvulas (controle – bloqueio) em série. 97
Figura 62 – $\mathcal{S}_{12}$: Supervisor local para duas válvulas (controle – bloqueio) em série. 98
Figura 63 – $\mathbf{G_{12}^{voc}}$: modelo de vocalizações para uma válvula de controle em série com uma de bloqueio representado como autômato de Mealy. . . . 98
Figura 64 – $\mathbf{G}^{op}$: Planta do operador para uma válvula de controle em série com uma válvula de bloqueio. 99
Figura 65 – $\mathbf{G_{12}^{Veq}}$: Modelo de abstração de uma válvula equivalente para duas válvulas (controle – bloqueio) em série. 100
Figura 66 – Diagrama de um processo industrial controlado por uma válvula de controle em série com uma válvula de bloqueio. 101
Figura 67 – (a) $\mathbf{G_{PV}}$: Modelo de preempção por meio da válvula equivalente da associação em série controle-bloqueio. (b) $\mathbf{G_{PB}}$: Modelo de preempção da bomba. 102
Figura 68 – $\mathbf{G_{VAZ}}$: Modelo de vazão do tanque. 103
Figura 69 – Estrutura em que o mapa repórter não é observador: (a) planta do operador $\mathbf{G^{op}}$ e (b) planta gerencial $\mathbf{G^{ge}}$. 111

Figura 70 – Duas especificações gerenciais: (a) o evento γ é desabilitado depois das cadeias α e $\alpha\beta$, (b) o evento β é desabilitado depois da ocorrência de α. 112
Figura 71 – Autômato que reconhece especificação gerencial E^{ge} para abstração de uma válvula de controle em série com uma de bloqueio. 113
Figura 72 – $\mathcal{S}^{ge}$: Supervisor gerencial que implementa a especificação E^{ge} para abstração de uma válvula de controle em série com uma de bloqueio. 113
Figura 73 – Estrutura hierárquica com composição no gerente. 118
Figura 74 – Exemplo de aplicação da composição paralela interníveis. $\mathbf{G_1^{op}}$: autômato vocalizador; $\mathbf{G_2}$: autômato no nível do gerente. 121
Figura 75 – Estrutura hierárquica com composição interníveis. 122
Figura 76 – Linguagem gerada de $\mathbf{G^{op}}$ no exemplo 6.3.1. 124
Figura 77 – Estrutura hierárquica com composição no gerente: equivalência entre modelo composto do gerente e abstração da composição interníveis. 127
Figura 78 – Em relação a θ_1, o evento α é confiável, mas β é não confiável. . . . 131
Figura 79 – Em relação a θ a confiabilidade dos eventos é mantida, ou seja, o evento α é confiável, mas β é não confiável. 131
Figura 80 – (a) $\mathbf{G_N}$: Modelo do tanque simplificado com três divisões de nível. (b) $\mathbf{G_P}$: Modelo de preempção da válvula. (c) $\mathbf{G_{VAZ}}$: Modelo de vazão do tanque. 133
Figura 81 – (a) $\mathbf{G_1^{op}}$: Modelo operacional de uma válvula de bloqueio com falha simplificada. (b) $\mathbf{G_1^{ge}}$: Modelo abstrato de uma válvula de bloqueio com falha simplificada. 134
Figura 82 – $\mathbf{G_2 = G_N||G_P||G_{VAZ}}$: Composição paralela entre os modelos do processo. 134
Figura 83 – $\mathbf{G^{op} = G_1^{op}||^I G_2}$: Composição interníveis entre o modelo operacional da válvula simplificada e o processo. 135
Figura 84 – $\mathbf{G^{ge} = G_1^{ge}||G_2}$: composição paralela da abstração da válvula simplificada com o processo. Esse modelo também é obtido como a abstração de $\mathbf{G^{op}}$. 135
Figura 85 – (a) E_A: Modelo que representa especificação de ação da válvula. (b) E_L: Modelo que representa especificação de limite de operação do tanque. 136
Figura 86 – $\mathcal{R}^{ge}$: Supervisor reduzido para o processo industrial simplificado. . . 136
Figura 87 – $\mathcal{S}^{ge}$: Supervisor gerencial para o processo industrial simplificado. As transições com o evento não confiável A são distinguidas pela cor cinza. 137

Figura 88 – (a) E_{AV}: Especificação de ação reativa da válvula. (b) E_{AB}: Especificação de ação reativa da bomba. (c) E_M Especificação de modos de atuação. 140

LISTA DE TABELAS

Tabela 1 – Representação de C^{op} por meio de uma tabela. 41
Tabela 2 – Mapa de desabilitações C^{op} do operador em um processo industrial comandado por uma válvula de bloqueio:. 59
Tabela 3 – Números de estados dos modelos dos supervisores 72
Tabela 4 – Número de estados na síntese monolítica para diferentes circuitos. 85
Tabela 5 – Mapa de desabilitações do operador $C_{12}^{op} : Q_{12}^{op} \times \Sigma_{12,c}^{eq} \rightarrow \Delta_{12}$, onde Q_{12}^{op} são estados de G_{12}^{op}, $\Sigma_{12,c}^{eq}$são os eventos controláveis de G_{12}^{Veq}, Δ_{12} são as desabilitações em G_{12}^{op}. 91
Tabela 6 – Mapa de desabilitações do operador $C_{12}^{op} : Q_{12}^{op} \times \Sigma_{12,c}^{eq} \rightarrow \Delta_{12}$, onde Q_{12}^{op} são estados de G_{12}^{op}, $\Sigma_{12,c}^{eq}$são os eventos controláveis de G_{12}^{Veq}, Δ_{12} são as desabilitações em G_{12}^{op}. 95
Tabela 7 – Mapa de desabilitações do operador $C_{12}^{op} : Q_{12}^{op} \times \Sigma_{12,c}^{eq} \rightarrow \Delta_{12}$, onde Q_{12}^{op} são estados de $\mathbf{G^{op}}$, $\Sigma_{12,c}^{eq}$são os eventos controláveis de $\mathbf{G_{12}^{Veq}}$, Δ_{12} são as desabilitações em $\mathbf{G^{op}}$. 99

LISTA DE ABREVIATURAS E SIGLAS

ADEF	Autômato Determinístico de Estados Finitos
CLP	Controlador Lógico Programável
FF	Foundation Fieldbus
IHM	Interface Humano-Máquina
PID	Proporcional Integral Derivativo
SED	Sistema a Eventos Discretos
TCS	Teoria de Controle Supervisório

LISTA DE SÍMBOLOS

Σ	Conjunto de eventos (Alfabeto)
ϵ	Cadeia vazia
Σ^*	Conjunto de cadeias
L	Linguagem
$\overline{L}$	Prefixo-fechamento de uma linguagem
$P_i(L)$	Projeção natural de uma linguagem
$P_i^{-1}(L)$	Projeção natural inversa de uma linguagem
$\|\|$	Produto síncrono de linguagens ou composição paralela de autômatos
$\mathbf{G}$	Autômato
T_0	Alfabeto de saída de um autômato vocalizador
τ_0	Evento silencioso
ω	Função de saída de um autômato vocalizador
Δ	Estrutura de controle (desabilitações)
$\mathcal{S}$	Supervisor
$\mathcal{C}$	Conjunto de linguagens controláveis
$Sup\mathcal{C}$	Máxima linguagem controlável
$\mathbf{G^{op}}$	Planta do operador em uma estrutura hierárquica
$\mathbf{G^{ge}}$	Planta do gerente em uma estrutura hierárquica
$\mathcal{S}^{ge}$	Supervisor do gerente
C^{op}	Mapa de desabilitações do operador
θ	Mapa repórter
$\mathcal{X}_\tau$	Conjunto de trechos silenciosos de um evento abstrato τ
$\mathcal{S}^{ge\rightarrow op}$	Supervisor induzido do gerente para o operador
$\dot{\cup}$	União disjunta de conjuntos
θ^{-1}	Mapa repórter inverso
$\|\|^I$	Composição paralela inter-níveis

SUMÁRIO

1	**INTRODUÇÃO**	**19**
1.1	OBJETIVOS	21
1.2	TRABALHOS RELACIONADOS	23
1.3	ORGANIZAÇÃO DO DOCUMENTO	26
2	**CONTROLE SUPERVISÓRIO HIERÁRQUICO DE SEDS**	**27**
2.1	LINGUAGENS FORMAIS E AUTÔMATOS	27
2.1.1	**Alfabetos e Linguagens**	**27**
2.1.2	**Autômatos Determinísticos de Estados Finitos**	**29**
2.1.3	**Composição de Autômatos**	**31**
2.1.4	**Autômatos Vocalizadores**	**32**
2.2	TEORIA DE CONTROLE SUPERVISÓRIO	33
2.3	CONTROLE HIERÁRQUICO DE SEDS	35
2.3.1	**Consistência Hierárquica de Baixo Nível**	**44**
2.3.2	**Consistência Hierárquica**	**46**
2.3.3	**Controle Hierárquico Não Bloqueante**	**49**
2.4	EXEMPLO DE MODELAGEM E SÍNTESE DE SUPERVISORES EM ARQUITETURA DE CONTROLE HIERÁRQUICO	53
2.5	DISCUSSÃO	59
3	**SÍNTESE DE SUPERVISORES PARA UM PROCESSO INDUSTRIAL COM CONTROLE PID E IMPLEMENTAÇÃO EM REDE FOUNDATION FIELDBUS**	**60**
3.1	COMPLEXIDADE DOS SISTEMAS HÍBRIDOS	62
3.2	MODELAGEM E SÍNTESE DOS SUPERVISORES	64
3.3	IMPLEMENTAÇÃO	72
3.4	RESULTADOS OBTIDOS	74
3.5	CONCLUSÃO	76
4	**MODELAGEM HIERÁRQUICA POR ABSTRAÇÕES SUCESSIVAS**	**77**
4.1	MODELAGEM DE CIRCUITOS DE COMPONENTES SEM A UTILIZAÇÃO DE NÍVEIS HIERÁRQUICOS	78
4.2	ARQUITETURA MULTINÍVEL PARA CIRCUITOS DE COMPONENTES COM ABSTRAÇÕES SUCESSIVAS	85
4.3	MODELAGEM PARA DUAS VÁLVULAS DE BLOQUEIO	87
4.3.1	**Modelagem Para Válvulas em Série**	**87**
4.3.2	**Modelagem Para Válvulas em Paralelo**	**93**
4.4	MODELAGEM PARA UMA VÁLVULA DE CONTROLE EM SÉRIE COM UMA VÁLVULA DE BLOQUEIO	96
4.5	APLICAÇÃO DA ESTRATÉGIA DE MODELAGEM	100

4.6 DISCUSSÃO 104
5 ARQUITETURA HIERÁRQUICA NÃO BLOQUEANTE BASEADA EM EVENTOS CONFIÁVEIS 105
5.1 EVENTO CONFIÁVEL 105
5.2 ALFABETO SUFICIENTE PARA PREFIXO FECHAMENTO DE UMA LINGUAGEM 107
5.3 CONTROLE HIERÁRQUICO NÃO BLOQUEANTE COM EVENTOS CONFIÁVEIS 109
5.4 DISCUSSÃO 114
6 ABORDAGEM INTERNÍVEIS PARA ESTRUTURA HIERÁRQUICA COM COMPOSIÇÃO NO GERENTE 115
6.1 CONSISTÊNCIA DE CONTROLE PERSISTENTE 116
6.2 ESTRUTURA HIERÁRQUICA COM COMPOSIÇÃO NO GERENTE . 117
6.3 ABORDAGEM FORMAL INTERNÍVEIS 119
6.4 EXEMPLO DE APLICAÇÃO EM UM PROCESSO INDUSTRIAL SIMPLIFICADO 132
6.5 EXEMPLO DE APLICAÇÃO: PROCESSO INDUSTRIAL COMANDADO POR UM CIRCUITO DE VÁLVULAS 138
6.6 CONCLUSÃO DO CAPÍTULO 141
7 CONCLUSÕES E PERSPECTIVAS 142
REFERÊNCIAS 145

1 INTRODUÇÃO

Os processos industriais comumente possuem características inerentes tanto a dinâmicas contínuas quanto a eventos discretos. Tipicamente os sistemas dinâmicos contínuos, seja em tempo contínuo ou discreto, são comandados por controladores PID, enquanto um controlador lógico programável (CLP) implementa intertravamentos e a lógica de operação dos atuadores discretos. Alguns exemplos comuns de malhas de controle em processos industriais são voltadas ao controle de nível, temperatura, vazão, pressão, cujos sensores e atuadores podem operar em sinais contínuos ou discretos. De uma maneira geral os processos industriais apresentam diversos riscos de acidentes, tanto aos seus operadores quanto aos equipamentos instalados. Bridges e Clark (2011) identificam que a maior parte dos acidentes em processos industriais ocorrem em operações não rotineiras, como nos procedimentos de inicialização e finalização dos processos, que podem ser classificadas como uma dinâmica a eventos discretos. Com o aumento da complexidade e exigências pela segurança dos processos, padrões internacionais estabelecem a necessidade da utilização de métodos formais para validação de sistemas de controle, como os implementados em CLP (IEC 61508-1, 2010). Essas exigências visam reduzir os riscos de acidentes e aumentar a segurança envolvida em processos industriais.

Como método formal para projeto e implementação da lógica de operação de processos, nesta tese é utilizada a Teoria de Controle Supervisório (TCS) e suas extensões, introduzida por Ramadge e Wonham (1989). A TCS se utiliza de autômatos e linguagens formais para projetar supervisores que garantem especificações lógicas ao processo através de um controle realimentado permissivo de sistemas a eventos discretos (SEDs). A escolha da TCS se justifica pelo fato de que ela provê métodos para síntese de supervisores que garantem que as especificações sejam atendidas de forma não bloqueante e minimamente restritiva ao processo. Em geral, o processo de síntese de supervisores possui complexidade computacional de ordem polinomial no número de estados dos autômatos que modelam a planta e as especificações.

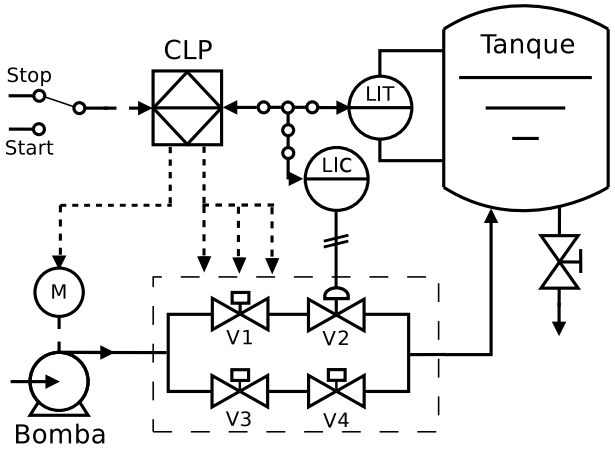
Um dos desafios da TCS consiste no crescimento exponencial do número de estados dos autômatos ao se executar a composição de subsistemas, o que é conhecido como explosão de estados. Alternativamente, algumas extensões da TCS exploram a arquitetura da complexidade dos processos. Segundo essa ideia, os sistemas complexos são formados por partes que interagem entre si e que podem ser decompostos em sub-sistemas e, de maneira sucessiva, chegar a elementos primitivos (SIMON, 1962). Os níveis hierárquicos são uma forma de organizar os sistemas em unidades mais simples, que se relacionam entre si de maneira ordenada, o que pode ser usado para projetar sistemas complexos. O controle modular (WONHAM; RAMADGE, 1988) e o controle modular local (QUEIROZ; CURY, 2000) exploram características da planta e

das especificações em relação a uma modularidade horizontal. Já o controle supervisório hierárquico de sistemas a eventos discretos (ZHONG; WONHAM, 1990) consiste em uma abordagem que explora a modularidade vertical dos subsistemas.

No entanto, a maioria das publicações sobre a TCS é aplicada em modelos em que a dinâmica a eventos discretos é bem caracterizada pelo próprio problema. Já a aplicação das técnicas da TCS em processos industriais em que predominam dinâmicas contínuas é menos frequente na literatura (WONHAM *et al.*, 2018). Grande parte desses trabalhos empregam supervisores baseados em redes de Petri aplicados a processos em bateladas (TITTUS; ÅKESSON, 1998; GU; BAHRI, 2002). Em Balemi *et al.* (1993) é implementado um supervisor para especificações de segurança em um processo a eventos discretos controlado, entretanto a metodologia proposta altera a abordagem da TCS, ao passo que a implementação é feita em dispositivos não utilizados na indústria. Por outro lado, ao abordar processos industriais comandados por um circuito de componentes como válvulas e bombas industriais, os trabalhos existentes são ainda mais limitados, conforme será melhor detalhado na Seção 1.2.

Tomando como base essas limitações da literatura, a ideia geral desta tese é desenvolver um método para controle supervisório hierárquico de sistemas a eventos discretos que possa ser aplicado a processos industriais comandados por um circuito de componentes. Em processos industriais típicos, são utilizadas estruturas como as da Figura 1, com o objetivo de controle do nível de líquido em um tanque, por exemplo.

Figura 1 – Processo industrial comandado por um circuito de componentes.



Fonte: Elaborado pelo autor.

Esse tipo de processo é comandado por um circuito que pode ser formado por válvulas industriais de controle, de bloqueio, de duas ou três vias, e bombas que promovem a vazão de um líquido. Esse circuito, tipicamente, tem a função de transportar um líquido até um tanque e manter esse líquido em determinado nível, respeitando ainda questões de segurança, como transbordamento e segurança dos equipamentos. Demais componentes que podem compor esse tipo de processo se enquadram como sensores, chaves seletoras, válvulas manuais, controladores lógicos.

A combinação da dinâmica contínua da variável de processo, como o nível em um tanque por exemplo, com a dinâmica discreta dos sensores e atuadores caracteriza esse tipo de estrutura como um sistema híbrido (ALUR *et al.*, 1995). Porém, sob o viés dos sistemas híbridos a problemática que surge está relacionada à complexidade dos modelos resultantes e processos utilizados, o que se torna um limitador para aplicações em processos industriais. No geral a dinâmica discreta que deriva do procedimento de obtenção de abstrações discretas de uma dinâmica contínua não possui um modelo com número finito de estados (KOUTSOUKOS *et al.*, 2000; ALUR *et al.*, 2000).

O segundo problema que surge nesse tipo de estrutura está relacionado com a modelagem e síntese de supervisores para o circuito de componentes. No geral, a composição de válvulas em circuitos causa o crescimento exponencial dos modelos resultantes, o que pode inviabilizar aplicações práticas (YAMALIDOU; KANTOR, 1991; YEH; CHANG, 2012). Como discutido no Capítulo 4, o acoplamento intrínseco de estruturas de válvulas não possibilita que os métodos para controle modular tragam vantagens em relação à obtenção dos modelos.

1.1 OBJETIVOS

O objetivo geral desta tese é desenvolver estratégias de modelagem e implementação, bem como novos resultados formais que contribuam para a aplicação do controle supervisório hierárquico de sistemas a eventos discretos em processos industriais comandados por um circuito de componentes.

Os processos industriais juntamente com os seus controladores, a exemplo do controle PID, são caracterizados como sistemas de tempo contínuo. Em processos industriais complexos é comum haver camadas de segurança que garantam certas propriedades ao sistema. Nesses casos, o controle supervisório pode servir também como uma camada adicional de segurança que garanta propriedades à dinâmica do processo, bem como à sua segurança. O primeiro problema que surge está relacionado com a natureza dos eventos que correspondem às mudanças da variável contínua, como nível ou temperatura em um processo por exemplo. Tipicamente esses eventos são considerados como não controláveis, pois são obtidos pela leitura de sensores. Para garantir as propriedades das especificações, bem como a controlabilidade do sistema a eventos discretos resultante, um dos objetivos específicos desta tese é desenvolver estratégias de modelagem e de implementação que representem a possibilidade de preempção de eventos discretos não controláveis por meio da intervenção do controle supervisório sobre os atuadores e sobre o controle contínuo do processo.

Neste trabalho, assume-se que os componentes como válvulas de controle, válvulas de bloqueio ou bombas de vazão são organizados de tal maneira que podem ser formados circuitos equivalentes por meio de abstrações sucessivas em níveis hierárquicos. Com essa estratégia de modelagem, esta tese visa demonstrar que é

possível reduzir as complexidades de modelagem e síntese do controle supervisório de processos industriais complexos comandados por um circuito de componentes, tornando viável a sua aplicação.

Por outro lado, ao se construir uma estrutura hierárquica, devem ser garantidas algumas condições a respeito da consistência entre os modelos operacionais e gerenciais (de baixo e alto nível) para que seja possível aplicar os métodos existentes. Mais especificamente, com os métodos existentes na literatura, para esse tipo de estrutura, uma das propriedades suficientes (mas não necessária) para a garantia de não bloqueio é a propriedade de observador (WONG; WONHAM, 1996). Entretanto, ao se considerar a possibilidade de falhas no acionamento de válvulas industriais, nem sempre a propriedade de observador é atingida. Dessa forma, um dos objetivos desta tese é propor uma novas condições, que flexibilizam a propriedade de observador, para garantir que o sistema resultante seja não bloqueante, mesmo para os casos em que não se atinge essa propriedade.

Por fim, como contribuição principal da tese, são abordadas estruturas hierárquicas em que há a composição de modelos no nível mais alto da hierarquia chamado de nível do gerente. Nesses casos, a maior problemática que existe é relacionada à sincronização de eventos entre um modelo abstrato e um modelo que não passa por abstração. Essa questão envolve não só a ocorrência de eventos no nível do gerente, mas também a ocorrência de eventos nos níveis mais baixos, pois esses são responsáveis por gerar os eventos abstratos. Dessa forma, um objetivo desta tese é desenvolver uma abordagem formal que considere a sincronização de eventos no nível mais alto da hierarquia e que possibilite relacionar os diferentes níveis hierárquicos.

Objetivo Geral

Desenvolver estratégias de modelagem e implementação, bem como uma nova abordagem formal para a aplicação do controle supervisório hierárquico em processos industriais comandados por um circuito de componentes.

Objetivos Específicos

1. Desenvolver uma estratégia de modelagem e de implementação para controle supervisório de sistemas a eventos discretos aplicável a processos industriais contínuos;
2. Propor uma estratégia de modelagem hierárquica multinível por abstrações sucessivas de circuitos equivalentes;
3. Demonstrar novos resultados que permitam flexibilizar a condição de observador para controle supervisório hierárquico não bloqueante;
4. Desenvolver uma abordagem formal para o problema do controle hierárquico com composição no gerente em que há sincronização de eventos.

1.2 TRABALHOS RELACIONADOS

O controle supervisório de processos industriais é um tema ainda pouco explorado. A estratégia de modelagem e implementação em processos industriais, como proposta no Capítulo 3, contempla a possibilidade de preempção da dinâmica contínua por meio dos atuadores, o que garante a controlabilidade das especificações, mesmo na existência de plantas com eventos unicamente não controláveis, e possibilita a aplicação direta dos métodos clássicos da teoria de controle supervisório. Essa abordagem difere de outros métodos que modificam a teoria de controle supervisório para que se possa lidar com eventos forçados, como é o caso de Sanchez (1996). Existem trabalhos que se utilizam de redes de Petri para desenvolver o controle, sendo que o controlador para os circuitos de válvulas é obtido indissociavelmente do controlador do processo. Yamalidou e Kantor (1991) realizam a modelagem e controle de processos da indústria química usando redes de Petri. Para operações contínuas, a rede de Petri é modelada de forma a simplificar sua dinâmica ao não considerar valores intermediários das variáveis contínuas, somente valores limites, como por exemplo o fato de existir vazão, ou não existir, em uma tubulação. No trabalho não é considerada a possibilidade de preempção da dinâmica contínua. Fica claro que a abordagem de modelagem pode ser generalizada para sistemas maiores, com um número maior de válvulas, o que é feito com o auxílio de tabelas, cujas células são definidas segundo a posição das válvulas. Entretanto, a metodologia é baseada em obter um modelo global contendo todas as válvulas do circuito, não solucionando o problema da complexidade, o que nesta tese será tratado no Capítulo 4 por meio da estratégia de modelagem por abstrações sucessivas.

Ainda se tratando sobre estratégias de modelagem e implementação em processos industriais, no trabalho de Yeh e Chang (2012) é apresentado um procedimento utilizando a teoria de controle supervisório para gerar supervisores de resposta à emergência em processos em batelada na indústria química. É criado um procedimento padrão para gerar os supervisores para qualquer tipo de sistema que possui algumas características similares, sendo explorados nesse trabalho sistemas híbridos com circuito de válvulas em batelada. É considerado um modelo de autômato para as válvulas contendo quatro estados: aberta, fechada, travada aberta e travada fechada, sendo esses últimos os estados que indicam falhas na válvula. As especificações destinadas a tratar o travamento das válvulas envolvem todas as válvulas do circuito em que estão relacionadas, empregando o controle modular, o que não resolve a problemática da complexidade. De modo que haja a garantia na ocorrência dos eventos dos atuadores sem que ocorram múltiplos eventos não controláveis da planta é empregado o conceito de preempção. O modelo para as válvulas de bloqueio com travamento proposto por esses autores assemelha-se ao modelo de válvulas trabalhado por Cassandras e Lafortune (2008).

No trabalho de Pu (2000), é proposto um método para modelagem de sistemas a eventos discretos, que generaliza o conceito de estruturas de controle. Utilizando abstrações hierárquicas, o método baseia-se em uma ideia de estrutura multinível, permitindo ainda a composição de sistemas no nível mais alto da hierarquia. De modo a garantir a consistência dos modelos ao longo dos níveis hierárquicos, o autor se baseia no conceito de abstrações consistentes, entretanto permanecendo com o requisito da propriedade de observador. Um trabalho importante, que também flexibiliza alguns requisitos na estrutura hierárquica é de Cunha e Cury (2007). Além de também generalizar o conceito de estruturas de controle, de modo similar ao autor acima, flexibilizam ainda a condição de consistência de marcação, ao considerar marcações flexíveis de cadeias em modelos de alto nível. Entretanto, ambos autores colocam como requisito para a garantia de não bloqueio nas estruturas a propriedade de observador do mapa repórter associado, a qual será demonstrada nesta tese como uma propriedade demasiadamente conservadora em alguns casos. Nesta tese, tal propriedade é flexibilizada por novas condições formalizadas no Capítulo 5. Um trabalho que propõe uma estrutura organizacional em níveis hierárquicos é o de Seow (2014). São divididos níveis hierárquicos em uma estrutura de modo a simplificar a análise e projeto de supervisores. No entanto, nos trabalhos citados acima, existe a restrição de não permitir a sincronização de eventos no nível gerencial, no caso de estruturas com composição no gerente, o que é solucionado nesta tese como uma inovação por meio da abordagem interníveis, desenvolvida no Capítulo 6.

Alguns trabalhos importantes que abordam a questão da observação de eventos através dos níveis hierárquicos são relacionados a seguir. Em (LEDUC *et al*., 2005a, 2005b), é introduzido o controle supervisório hierárquico baseado em interfaces, em que um sistema é dividido em diferentes níveis conectados por interfaces, o que limita as informações trocadas entre eles. Essa abordagem diminui a complexidade de analizar o supervisor para sistemas de grande escala. Seguindo essa mesma linha, Hill *et al.* (2010) desenvolve uma arquitetura multi-nível empregando controle supervisório hierárquico baseado em interfaces. Em (SCHMIDT; BREINDL, 2011) e (SCHMIDT; BREINDL, 2008), são estabelecidas novas propriedades que flexibilizam algumas condições para garantir o controle hierárquico não bloqueante e minimamente restritivo. Considerando a condição de observabilidade entre os níveis, duas condições são propostas e Boutin *et al.* (2011), baseadas em uma consistência de observação. Essas propriedades trabalham com autômatos de Mealy sob observação parcial, ou seja, em que eventos são classificados em observáveis e não observáveis. Existem ainda outros trabalhos que lidam com observação parcial de eventos, mas a propriedade de observador é sempre uma condição necessária para garantir o não bloqueio (ZAMANI FEKRI; HASHTRUDI-ZAD, 2009; KOMENDA *et al*., 2015).

A ideia para o objeto de estudo desta tese se originou a partir da dissertação

de mestrado de Muler (2018), em que é proposta uma ideia de metodologia, utilizando controle hierárquico de SEDs, para obtenção do modelo de uma válvula equivalente em circuitos de válvulas. No trabalho citado é projetado um controle supervisório visando assegurar quesitos de segurança em um processo industrial de controle de nível. O sistema estudado pode ser considerado um sistema híbrido, pois possui uma dinâmica contínua, bem como atuadores discretos, contendo uma válvula reguladora em uma malha de válvulas e uma bomba. No trabalho, a dinâmica contínua é simplificada para que sejam sinalizados somente limites relevantes no que diz respeito a questões de segurança do processo. O controlador contínuo é responsável pela operação normal do processo, que é o controle de nível em um tanque, enquanto o supervisor age somente em questões em que seja necessário intervir para garantir condições de segurança ao processo industrial. Como por exemplo, no caso de uma sintonia ineficiente do controlador contínuo, se o processo se encontra próximo a uma situação de transbordamento, o supervisor age sobre os atuadores garantindo condições para o processo retornar a uma região segura de funcionamento. A modelagem das válvulas é feita com dois estados, aberta ou fechada. Em cada estado é considerado um evento que mantém a válvula no mesmo estado (auto-laço), para que seja permitida, dessa forma, a aplicação da preempção da dinâmica contínua. No trabalho é sintetizado um supervisor monolítico reduzido e implementado em rede Foundation Fieldbus, para demonstrar a aplicabilidade do método. Entretanto, o trabalho se limitou a aplicação da estratégia de modelagem em um processo industrial e em propor uma ideia inicial de modelagem multinível com válvulas de bloqueio.

Visando empregar níveis de abstração para realizar a modelagem de estruturas complexas, é necessário fazer uso de uma representação que possibilite descrever a troca de informações entre esses níveis. Nesse sentido, neste trabalho são definidos os autômatos vocalizadores, que são uma particularização de autômatos de Moore (MOORE, 1956). Esse tipo de estrutura permite a construção de modelos com saídas representadas em seus estados. Essa escolha se dá direcionada pela aplicação dos circuitos de componentes em uma estrutura multinível, como será melhor abordado no capítulo 4. Os autômatos vocalizadores diferem das máquinas de Mealy, que representam as saídas em seus eventos, com sua sinalização ao nível superior dada por meio de uma projeção natural, como utilizado em Schmidt e Breindl (2011). Esse modelo difere também dos sistemas baseados em agregação de estados utilizados em Torrico e Cury (2002), em que os estados de uma planta de alto nível são uma partição de estados da planta de baixo nível, formada levando em conta eventos relevantes a serem sinalizados ao nível superior.

1.3 ORGANIZAÇÃO DO DOCUMENTO

Este documento está organizado da seguinte forma: No Capítulo 2 é feito um estudo sobre a Teoria de Controle Supervisório de SEDs com destaque no Controle Supervisório Hierárquico de SEDs, onde se propõe uma padronização da notação e alguns novos conceitos sobre esse tema. Nesse capítulo é detalhado um exemplo completo de aplicação de modelagem e síntese de supervisores utilizando o controle hierárquico. No capítulo 3, é desenvolvida uma estratégia de modelagem para a síntese de supervisores, utilizando a teoria de controle supervisório, para processos industriais sob controle PID, incluindo sua implementação em rede Foundation Fieldbus. O Capítulo 4 propõe uma estratégia de modelagem de circuitos de componentes utilizando o controle supervisório hierárquico de SEDs. No Capítulo 5, são formalizados novos conceitos para a modelagem e síntese de controle hierárquico não bloqueante baseada em eventos confiáveis. No Capítulo 6, desenvolve-se formalmente a abordagem interníveis e sua aplicação para síntese de supervisores no controle hierárquico. O Capítulo 7 traz as conclusões da tese e perspectivas para continuação da pesquisa.

2 CONTROLE SUPERVISÓRIO HIERÁRQUICO DE SEDS

Os sistemas a eventos discretos (SEDs) caracterizam-se por possuir dinâmica dirigida por eventos em um conjunto discreto de estados. Sistemas de manufatura, sistemas de tráfego e protocolos de comunicação, podem ser citados como exemplos que se enquadram como SEDs. Esse tipo de dinâmica difere dos sistemas de dinâmica contínua, cujas variáveis têm seus valores alterados continuamente em função do tempo (CASSANDRAS; LAFORTUNE, 2008). Os processos industriais complexos normalmente possuem dinâmica contínua, associada a variáveis como nível e temperatura por exemplo, combinada com dinâmica a eventos discretos dirigida por sinais provenientes da leitura de sensores discretos e acionamento de atuadores, como pistões, bombas e válulas por exemplo.

A teoria de controle supervisório (TCS) enunciada por Ramadge e Wonham (1989) é um dos mais importantes métodos formais para o controle de SEDs. Nesta teoria, considera-se a planta como o comportamento em malha aberta, com todas as sequências de eventos possíveis, enquanto que o supervisor tem a ação de habilitar ou, de maneira dual, desabilitar um subconjunto de eventos da planta para atingir determinados requisitos. Desta forma, diz-se que o supervisor possui natureza permissiva. A teoria de controle supervisório possui algumas extensões que promovem a diminuição da complexidade dos resultados em determinados contextos. O controle modular promove a modularidade horizontal, ao passo que o controle hierárquico promove a modularidade vertical ao explorar a modelagem em diferentes níveis hierárquicos.

Este capítulo trata dos conceitos iniciais sobre linguagens e autômatos que servem como base para a teoria de controle supervisório, a qual é descrita na sequência juntamente com sua extensão sobre o controle modular. A seguir, a teoria de controle supervisório hierárquico de SEDs é discutida juntamente com uma proposta de padronização de sua notação. Os conceitos apresentados neste capítulo se baseiam em Cassandras e Lafortune (2008) e Wonham e Cai (2019). Para ilustrar os conceitos é trabalhado um exemplo de aplicação do controle hierárquico em um caso prático.

2.1 LINGUAGENS FORMAIS E AUTÔMATOS

2.1.1 Alfabetos e Linguagens

Um alfabeto é definido como um conjunto finito e não vazio de símbolos, que representa a ocorrência de eventos em um SED. As cadeias, ou palavras, sobre um alfabeto Σ são formadas por sequências finitas de símbolos desse alfabeto. O símbolo ϵ é utilizado para descrever uma cadeia vazia que representa, em um SED, a situação em que não ocorre nenhum evento. O conjunto de todas as cadeias finitas formadas por elementos de Σ, incluindo a cadeia vazia ϵ, é chamado de Σ^*.

A concatenação de duas cadeias sobre um alfabeto Σ é definida como a simples justaposição destas. A cadeia vazia ϵ é o elemento identidade da concatenação. Um prefixo de uma cadeia $s \in \Sigma^*$ é uma cadeia $t \in \Sigma^*$, tal que, existe uma cadeia $u \in \Sigma^*$, onde $s = tu$. A notação $t \leq s$ indica que a cadeia t é um prefixo da cadeia s.

Uma linguagem L sobre um alfabeto Σ ($L \subseteq \Sigma^*$) é definida como um conjunto de cadeias formadas com símbolos desse alfabeto. As linguagens são dispositivos que permitem a representação de SEDs, pois podem representar sequências de eventos como cadeias. Apesar de não possibilitar a representação de estados no contexto de SEDs, as linguagens permitem representar todas as sequências de eventos possíveis de ocorrerem em um sistema. Dado que linguagens são definidas como conjuntos, as demais operações sobre conjuntos se também se aplicam, como interseção e união.

A concatenação de duas linguagens L_1 e L_2 é o conjunto formado pela concatenação de cadeias de L_1 com cadeias de L_2.

Definição 2.1.1. ***Concatenação de Linguagens (CASSANDRAS; LAFORTUNE, 2008):***
A concatenação de duas linguagens $L_1 \subseteq \Sigma^*$ e $L_2 \subseteq \Sigma^*$ é definida por:

$$L_1 L_2 := \{s \in \Sigma^* : (s = s_1 s_2)\, e\, (s_1 \in L_1)\, e\, (s_2 \in L_2)\}$$

O prefixo-fechamento de uma linguagem L (denotado como $\overline{L}$) é o conjunto formado por todos os prefixos de todas as cadeias de L.

Definição 2.1.2. ***Prefixo-Fechamento (CASSANDRAS; LAFORTUNE, 2008):***
O prefixo fechamento de $L \subseteq \Sigma^*$ é definido como:

$$\overline{L} := \{s \in \Sigma^* : \exists t \in \Sigma^*\, (st \in L)\}$$

Em outras palavras, o prefixo fechamento de $L \subseteq \Sigma^*$ é o conjunto de todas as cadeias formadas com elementos de Σ que levam a cadeias de L.

Definição 2.1.3. ***Projeção Natural (CASSANDRAS; LAFORTUNE, 2008):***
Sejam Σ e Σ_i conjuntos de eventos com $\Sigma_i \subseteq \Sigma$, a projeção natural $P_i : \Sigma^* \to \Sigma_i^*$ é definida recursivamente por:

$$P_i(\epsilon) = \epsilon$$
$$P_i(\sigma) = \begin{cases} \epsilon & se \quad \sigma \notin \Sigma_i \\ \sigma & se \quad \sigma \in \Sigma_i \end{cases}$$
$$P_i(u\sigma) = P_i(u)P_i(\sigma), onde\ u \in \Sigma^*,\ \sigma \in \Sigma$$

O conceito de projeção natural pode ser estendido para linguagens de modo que:

$$P_i(L) = \{u_i \in \Sigma_i^* : u_i = P_i(u)\ para\ algum\ u \in L\}.$$

A operação de projeção natural de uma linguagem, $P_i(L)$, apaga os eventos, nas cadeias u, que estão em Σ e não estão em Σ_i, ou seja, essa operação apaga os eventos de $\Sigma \setminus \Sigma_i$.

A projeção inversa $P_i^{-1} : 2^{\Sigma_i^*} \rightarrow 2^{\Sigma^*}$ é definida como:

$$P_i^{-1}(L) = \{u \in \Sigma^* : P_i(u) \in L\}.$$

Esta operação, quando aplicada a uma linguagem $L \subseteq \Sigma_i^* \subseteq \Sigma$, produz um conjunto formado por todas as cadeias que podem ser construídas com eventos de Σ cuja projeção P_i esteja em L.

Exemplo 2.1.1. ***Projeção Natural:*** *Como exemplo podem-se considerar os alfabetos* $\Sigma_i = \{a, b\} \subset \Sigma = \{a, b, c\}$*. Para uma linguagem* $L = \{acb\} \subset \Sigma^*$*:*

$P_i(L) = \{ab\}$ ***e***
$P_i^{-1}(\{ab\}) = \{ab, cab, acb, abc, ccab, accb, abcc, ...\}$

O produto síncrono, ou composição síncrona, de linguagens é a operação que permite desenvolver modelos de SEDs com determinada modularidade horizontal.

Definição 2.1.4. ***Produto Síncrono de Linguagens (CASSANDRAS; LAFORTUNE, 2008):***

Para duas linguagens, $L_1 \subseteq \Sigma_1^*$ *e* $L_2 \subseteq \Sigma_2^*$*, o produto síncrono de* L_1 *com* L_2 *é definido por:*

$$L_1 \parallel L_2 = P_1^{-1}(L_1) \cap P_2^{-1}(L_2),$$

Esta operação permite compor linguagens de alfabetos distintos, e o alfabeto da linguagem resultante consiste na união dos alfabetos envolvidos ($\Sigma_1 \cup \Sigma_2$).

2.1.2 Autômatos Determinísticos de Estados Finitos

Dadas as limitações de representar sistemas a eventos discretos por linguagens, normalmente se utiliza o conceito de autômatos para esse tipo de representação. Os autômatos são uma estrutura matemática formal que permite o reconhecimento de linguagens, além de possibilitar a representação de estados em um sistema. Possibilitam ainda a representação de SEDs de uma forma gráfica, o que facilita a construção de modelos. Neste trabalho, serão empregados autômatos determinísticos de estados finitos (ADEFs), em que o número de estados é limitado, a função de transição de estados pode ser parcial e cada evento definido em um estado causa uma transição a somente um estado. No decorrer desta tese, os ADEFs são chamados simplesmente de autômatos.

Definição 2.1.5. ***Autômatos determinísticos de estados finitos (CASSANDRAS; LAFORTUNE, 2008):***

Os autômatos são definidos como uma quíntupla

$$\mathbf{G} = (Q, \Sigma, f, q_0, Q_m), \textit{ onde:}$$

- Q *é um conjunto finito de estados;*
- Σ *é um alfabeto finito e não vazio;*
- $f : Q \times \Sigma \rightarrow Q$ *é uma função de transição parcial. A notação* $f(q, \sigma) = q'$ *representa que do estado* q *chega-se ao estado* q' *por meio da ocorrência do evento* σ*.*
- $q_0 \in Q$ *é o estado inicial;*
- $Q_m \subseteq Q$ *é um conjunto de estados marcados, que, no contexto de representação dos SEDs, são compreendidos como tarefas completas.*

Em muitos casos é conveniente a utilização de uma função de transição estendida para cadeias $\hat{f} : Q \times \Sigma^* \rightarrow Q$ definida como: $\hat{f}(q, \epsilon) = q$ e

$$\hat{f}(q, s\sigma) = f(\hat{f}(q, s), \sigma)$$

A notação $f(q, \sigma)!$ indica que $f(q, \sigma)$ está definida.

Na representação de SEDs se torna importante diferenciar cadeias que se referem a tarefas em andamento e cadeias que se referem a tarefas completas. Nesse sentido, as tarefas completas são sequências de eventos que levam a estados marcados. Um autômato é capaz de reconhecer as linguagens gerada $L(\mathbf{G}) \subseteq \Sigma^*$ e marcada $L_m(\mathbf{G}) \subseteq L(\mathbf{G})$:

$$L(\mathbf{G}) := \{s \in \Sigma^* : \hat{f}(q_0, s) \text{ é definida}\}$$

$$L_m(\mathbf{G}) = \{s \in L(\mathbf{G}) : \hat{f}(q_0, s) \in Q_m\}$$

Um sistema a eventos discretos é dito ser não-bloqueante se

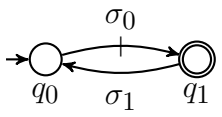
$$\overline{L_m(\mathbf{G})} = L(\mathbf{G}) \tag{2.1}$$

Em outras palavras, essa equação estabelece como critério para não-bloqueio que todas as cadeias geradas por um autômato $\mathbf{G}$ devem ser prefixos de cadeias marcadas. Ou seja, um SED representado pelo autômato $\mathbf{G}$ é não bloqueante quando toda cadeia gerada tiver uma continuação para atingir algum estado marcado.

Os autômatos podem ser representados graficamente na forma de um grafo dirigido, onde os círculos são os estados, as setas são os eventos que ocorrem nas transições de um estado a outro, o estado inicial é representado por uma seta e

os estados marcados, por círculos duplos. Na TCS os eventos são classificados em controláveis e não controláveis. O que difere esses dois tipos de eventos é que os controláveis podem ser desabilitados por um supervisor, enquanto que os não controláveis ocorrem sem a possibilidade de serem desabilitados. Na Figura 2 consta a representação gráfica de um autômato, em que σ_0 é um evento controlável, σ_1, não controlável, q_0 é o estado inicial e q_1 é um estado marcado.

Figura 2 – Exemplo de um autômato.



Fonte: Elaborado pelo autor.

Um autômato representando um SED é dito ser acessível se, a partir do seu estado inicial, é possível atingir, por meio de sequências de eventos, todos os estados do autômato. Um autômato é dito ser co-acessível se, a partir de qualquer um de seus estados, é possível atingir um estado marcado. Se, a partir de um dado estado, é impossível atingir um estado marcado, diz-se que o autômato é bloqueante. Um autômato que é acessível e co-acessível é denominado de autômato *trim*.

2.1.3 Composição de Autômatos

Ao representar SEDs por modelos de autômatos, é comum utilizar agregações de modelos, o que promove modularidade horizontal na etapa de modelagem. A operação mais comum desse tipo é a composição paralela de autômatos, também conhecida como produto síncrono. A composição paralela de n autômatos $\mathbf{G_i}$, $i = \{1, 2, ...n\}$, pode ser obtida realizando-se a evolução em paralelo de todos os n autômatos. Um evento compartilhado por mais de um autômato só é executado quando estiver habilitado, simultaneamente, em todos os autômatos onde esse evento está definido, um evento definido somente em um dos n autômatos evolui livremente no autômato em que está definido. A linguagem gerada do autômato obtido pela composição paralela é igual ao produto síncrono das linguagens geradas de cada autômato envolvido na operação. A linguagem marcada pelo autômato obtido de uma composição paralela é o produto síncrono de todas as linguagens marcadas dos n autômatos da composição.

Definição 2.1.6. ***Composição paralela de autômatos (CASSANDRAS; LAFORTUNE, 2008):***

A composição paralela de dois autômatos $\mathbf{G_1} = (Q_1, \Sigma_1, f_1, q_{0,1}, Q_{1,m})$ *e* $\mathbf{G_2} = (Q_2, \Sigma_2, f_2, q_{0,2}, Q_{2,m})$ *é definida formalmente como o autômato:*

$$\mathbf{G_1}||\mathbf{G_2} := Ac(Q_1 \times Q_2, \Sigma_1 \cup \Sigma_2, f, (q_{0,1}, q_{0,2}), Q_{1,m} \times Q_{2,m}),$$

em que $Ac()$ *indica componente acessível.*

A função de transição $f : (Q_1 \times Q_2) \times (\Sigma_1 \cup \Sigma_2) \rightarrow (Q_1 \times Q_2)$ *é definida por:*

$$f((q_1, q_2), \sigma) = \begin{cases} (f_1(q_1, \sigma), f_2(q_2, \sigma)) \; se \; \sigma \in \Sigma_1 \cap \Sigma_2 \; e \; f(q_1, \sigma)! \; e \; f(q_2, \sigma)! \\ (f_1(q_1, \sigma), q_2) \; se \; \sigma \in \Sigma_1 \; e \; \sigma \notin \Sigma_2 \; e \; f(q_1, \sigma)! \\ (q_1, f_2(q_2, \sigma)) \; se \; \sigma \notin \Sigma_1 \; e \; \sigma \in \Sigma_2 \; e \; f(q_2, \sigma)! \\ indefinida, \; senão \end{cases}$$

2.1.4 Autômatos Vocalizadores

Ao trabalhar com diferentes níveis de abstração para realizar a modelagem de estruturas complexas, é necessário fazer uso de uma representação que possibilite descrever a troca de informações entre esses níveis. Nesse sentido, neste trabalho são utilizados os autômatos vocalizadores, que são uma particularidade de autômatos de Moore (MOORE, 1956), por possibilitarem a construção de modelos com as saídas representadas em seus estados.

Os autômatos de Moore são uma extensão da definição de autômatos, à qual acrescenta-se um alfabeto de saída e uma função de saída, que relaciona a cada estado um único evento de saída (HOPCROFT; ULLMAN, 1979). Essas saídas são definidas de uma maneira geral como símbolos que sinalizam uma determinada informação conforme o estado atingido. Um exemplo são os autômatos com marcação colorida, que distinguem diferentes classes de tarefas associando a cada classe uma cor, com o objetivo de generalizar a marcação de autômatos para se expressar propriedades de vivacidade em termos dessas cores (QUEIROZ *et al.*, 2005). A definição de autômatos vocalizadores apresentada a seguir leva em conta a interpretação de que os sinais de saída são eventos abstratos de um nível hierárquico acima, que portanto geram as linguagens de um modelo abstrato. Destaca-se que, nesta representação, associado a cada estado de um autômato vocalizador pode estar definido somente um evento de saída.

Definição 2.1.7. ***Autômatos vocalizadores:***

Os autômatos vocalizadores são definidos como uma tupla

$$\mathbf{G} = (Q, \Sigma, f, q_0, Q_m, T_0, \omega), \textit{ onde:}$$

- Q *é o conjunto de estados;*
- Σ *representa o alfabeto;*
- $f : Q \times \Sigma \rightarrow Q$ *é uma função parcial de transição de estados;*
- q_0 *é o estado inicial;*
- Q_m *é o conjunto de estados marcados;*

- $T_0 = T \cup \{\tau_0\}$ *é o alfabeto de saída, que contém o alfabeto* T *do autômato vocalizado ao nível hierárquico acima e evento silencioso* τ_0*, para quando o mapa repórter não informa nenhum evento relevante;*
- $\omega : Q \to T_0$ *é a função de saída de* $\mathbf{G}$ *que relaciona a cada estado um único evento de saída, que ocorre assim que uma transição atinge um estado.*

Os estados $q \in Q$, são chamados de estados silenciosos quando $\omega(q) = \tau_0$ e estados vocalizadores (ou estados vocais) quando $\omega(q) \neq \tau_0$. Por definição, para o estado inicial $\omega(q_0) = \tau_0$. Em adição à função de saída ω, é conveniente definir uma extensão para cadeias $\hat{\omega} : L(\mathbf{G}) \to T \cup \{\tau_0\}$, conhecida como mapa vocal[1]:

$$\hat{\omega}(s) = \omega(\hat{f}(q_0, s))$$

2.2 TEORIA DE CONTROLE SUPERVISÓRIO

Na teoria de controle supervisório (RAMADGE; WONHAM, 1989), a planta $\mathbf{G}$ é um autômato sobre o alfabeto $\Sigma = \Sigma_c \dot{\cup} \Sigma_u$, onde Σ_c é um conjunto de eventos controláveis, passíveis de desabilitação, e Σ_u, não controláveis, que ocorrem sem interferência do supervisor. Adiciona-se à planta $\mathbf{G}$ a estrutura de controle $\Delta = 2^{\Sigma_c}$, em que cada $\delta \in \Delta$ corresponde ao conjunto de eventos a desabilitar em cada momento[2].

Define-se um supervisor para uma planta $\mathbf{G}$ como um mapa

$$\mathcal{S} : L(\mathbf{G}) \to \Delta,$$

que associa cadeias da planta a conjuntos de eventos a desabilitar.

Ao supervisor $\mathcal{S}$ pode ser associada uma linguagem $M \subseteq L_m(\mathbf{G})$, sendo que o par $(\mathcal{S}, M)$ é definido como supervisor marcador. A linguagem M tem a função de determinar quais cadeias da planta $\mathbf{G}$ permanecerão marcadas com a ação do supervisor. Utiliza-se $\mathcal{S}/\mathbf{G}$ para denotar $\mathbf{G}$ sob supervisão de $\mathcal{S}$.

A linguagem gerada em malha fechada $L(\mathcal{S}/\mathbf{G}) \subseteq L(\mathbf{G})$ é definida por:

$$\begin{aligned} &\epsilon \in L(\mathcal{S}/\mathbf{G}) \\ &[(s \in L(\mathcal{S}/\mathbf{G})) \,\&\, (s\sigma \in L(\mathbf{G})) \,\&\, (\sigma \notin \mathcal{S}(s))] \iff [s\sigma \in L(\mathcal{S}/\mathbf{G})] \end{aligned} \tag{2.2}$$

A linguagem marcada por $\mathcal{S}/\mathbf{G}$ é: $L_m(\mathcal{S}/\mathbf{G}) = L(\mathcal{S}/\mathbf{G}) \cap M$.

Um supervisor $\mathcal{S}$ é dito ser não bloqueante para uma planta $\mathbf{G}$ se o sistema em malha fechada não possuir bloqueios, ou seja $\overline{L_m(\mathcal{S}/\mathbf{G})} = L(\mathcal{S}/\mathbf{G})$.

[1] É comum a utilização do operador ω para designar tanto a função de saída, quanto sua extensão para cadeias. A diferenciação correta da função utilizada pode ser feita pelo contexto.

[2] Em Ramadge e Wonham (1989) a estrutura de controle é definida como os eventos a serem habilitados, cuja notação normalmente é Γ. Nesta tese utiliza-se a notação acima por ser mais natural trabalhar com os eventos a desabilitar quando se aborda o controle hierárquico.

Para fins de implementação, o supervisor $\mathcal{S}$ pode ser representado por um autômato $\boldsymbol{S} = (X, \Sigma, f, x_0, X_m)$ e um mapa de desabilitações $\Phi : X \to 2^{\Sigma_c}$ que relaciona a cada estado de $\boldsymbol{S}$ um conjunto de eventos a ser desabilitados em $\mathbf{G}$. De maneira geral, qualquer autômato $\boldsymbol{S'}$ pode ser capaz de executar a ação de supervisão sobre $\mathbf{G}$, desde que $L_m(\boldsymbol{S'}||\mathbf{G}) = L_m(\boldsymbol{S})$ e $L(\boldsymbol{S'}||\mathbf{G}) = L(\boldsymbol{S})$. Nesses termos, é possível reduzir o número de estados de um supervisor, mantendo a mesma ação de supervisão, o que pode ser realizado por meio do método de redução de supervisores de Su e Wonham (2004).

Usualmente, para o sistema em malha fechada, deseja-se que sejam atendidos alguns requisitos de funcionamento. Esses requisitos podem ser representados por meio de uma linguagem-alvo $K \subseteq L_m(\mathbf{G})$, também chamada de especificação, que determina o comportamento desejado para a planta sob supervisão. Afirma-se que uma linguagem $K \subseteq \Sigma^*$ é controlável em relação a $L(\mathbf{G})$ se

$$\overline{K}\Sigma_u \cap L(\mathbf{G}) \subseteq \overline{K} \tag{2.3}$$

Desta forma, existe um supervisor marcador não-bloqueante que implementa K, tal que $L_m(\mathcal{S}/\mathbf{G}) = K$, se e somente se K for controlável em relação a $L(\mathbf{G})$. A classe de linguagens controláveis contidas em uma linguagem E, em relação à uma planta $\mathbf{G}$ é denotada por $\mathcal{C}(E, \mathbf{G}) = \{K : K \subseteq E$ e K é controlável e.r.a $L(\mathbf{G})\}$. Esse conjunto é não vazio e fechado para união, o que implica que possui um único elemento supremo, denominado de $Sup\mathcal{C}(E, \mathbf{G})$, que é a máxima linguagem controlável contida em E. O supervisor $\mathcal{S}$ pode ser obtido pelo cálculo de $Sup\mathcal{C}(E, \mathbf{G})$, onde E é o comportamento desejado em malha fechada para a planta $\mathbf{G}$. Se para uma dada planta $\mathbf{G}$ e uma especificação E, a máxima linguagem controlável é não-vazia, o supervisor obtido é tal que $L_m(\mathcal{S}/\mathbf{G}) = Sup\mathcal{C}(E, \mathbf{G})$, cuja ação de supervisão é não bloqueante e ótima. Do contrário, diz-se que, para os respectivos modelos, o problema de controle supervisório não tem solução.

Conforme o grau de complexidade da planta e arquitetura do sistema envolvido, pode-se optar por utilizar diferentes estratégias para síntese de supervisor. A abordagem monolítica se baseia em calcular um único supervisor, mesmo nos casos em que a planta é composta por submodelos e a especificação é a composição de diferentes especificações. Nesta abordagem, a planta $\mathbf{G}$ é calculada como a composição paralela dos submodelos $\mathbf{G_i}$ e a especificação K é calculada como o produto síncrono das linguagens K_i que impõem restrições ao comportamento da planta. O supervisor monolítico $\mathcal{S}$, não bloqueante e ótimo, é sintetizado por meio da máxima linguagem controlável $Sup\mathcal{C}(K, \mathbf{G})$.

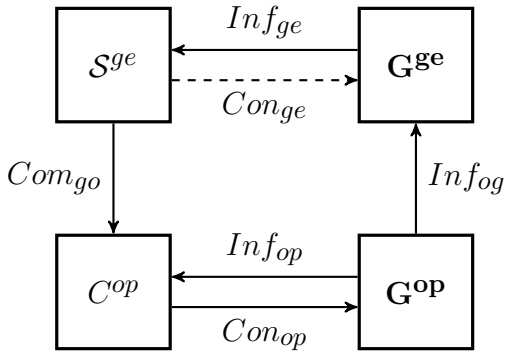
Uma alternativa para reduzir a complexidade da solução é a utilização da abordagem modular para síntese de supervisores (WONHAM; RAMADGE, 1988). Nesta abordagem calcula-se um supervisor $\mathcal{S}_i$ para cada especificação K_i, por meio

da máxima linguagem controlável. Deseja-se que os supervisores modulares sejam não-conflitantes para garantir ausência de bloqueio, condição que se expressa por $\bigcap_{i=1}^{n} \overline{L_m(\mathcal{S}_i/\mathbf{G})} = \overline{\bigcap_{i=1}^{n} L_m(\mathcal{S}_i/\mathbf{G})}$. Quando respeitada a propriedade de não-conflito, atinge-se um comportamento em malha fechada não bloqueante e ótimo, tal que $\bigcap_{i=0,n} L_m(\mathcal{S}_i/\mathbf{G}) = L_m(\mathcal{S}/\mathbf{G})$, onde $\mathcal{S}$ é o supervisor monolítico calculado a partir da especificação $K = \|_{i=1}^{n} K_i$. Nos casos em que não é possível obter supervisores modulares não-conflitantes, pode-se calcular um coordenador para resolução de conflitos, que desabilita eventos, do sistema em malha fechada, que levam a situações de bloqueio (WONG; WONHAM, 1998; QUEIROZ; CURY, 2005). Tomando $\mathbf{G_{conflito}} = \|_{i=1}^{m} (S_i/\mathbf{G})$ como o sistema em malha fechada que satisfaz a especificação K, mesmo apresentando bloqueio, o coordenador pode ser obtido por meio de $Sup\mathcal{C}(\Sigma^*, \mathbf{G_{conflito}})$.

2.3 CONTROLE HIERÁRQUICO DE SEDS

A divisão em níveis hierárquicos ajuda a reduzir a complexidade de sistemas por meio da modularidade vertical (SIMON, 1962). Pela proposta de Zhong e Wonham (1990), estende-se a TCS para considerar uma arquitetura em níveis hierárquicos. De acordo com esta abordagem, inicialmente é feita uma divisão em dois níveis de abstração, tomando-se como analogia um sistema fabril com a divisão entre gerência e operação. A Figura 3 apresenta a arquitetura básica do controle hierárquico, onde o nível de baixo é considerado como operador e o de cima, como gerente.

Figura 3 – Arquitetura para controle hierárquico.



Fonte: Zhong e Wonham (1990).

Nesta arquitetura, a planta a ser controlada situa-se no nível do operador e é representada pelo autômato vocalizador $\mathbf{G^{op}}$, cuja função de saída sinaliza eventos no nível do gerente. A planta no nível do gerente é representada pelo autômato $\mathbf{G^{ge}}$ e é entendida como uma abstração de $\mathbf{G^{op}}$. No nível gerencial são tradadas informações relevantes para tomadas de decisão de alto nível, enquanto que o nível operacional realmente executa as ações de controle.

Pelo canal de informações Inf_{og} são transmitidos os eventos abstratos que formam o alfabeto T da planta abstrata do gerente $\mathbf{G^{ge}}$. Esta planta envia informações para o supervisor $\mathcal{S}^{ge}$ por meio do canal Inf_{ge} (canal de informações do gerente). Como $\mathbf{G^{ge}}$ é uma planta abstrata, sua supervisão somente pode ser executada de maneira virtual. A supervisão de $\mathbf{G^{ge}}$ é feita, então, virtualmente por $\mathcal{S}^{ge}$ e, por esta razão, o canal de controle do gerente Con_{ge} é ilustrado como tracejado. A ação de $\mathcal{S}^{ge}$ é executada efetivamente pelo mapa de desabilitações do operador C^{op}, que recebe as diretivas de controle de $\mathcal{S}^{ge}$ por meio do canal de comando Com_{go} e envia sinais de desabilitação por meio do canal de controle Con_{op}. Para traduzir a desabilitação de eventos abstratos em desabilitações de eventos operacionais, C^{op} recebe por meio do canal de informações do operador, Inf_{op}, os eventos ocorridos em $\mathbf{G^{op}}$, conforme será apresentado à frente.

Em baixo nível, a planta operacional é definida como um autômato vocalizador:

$$\mathbf{G^{op}} = (Q, \Sigma, f, q_0, Q_m, T_0, \omega),$$

com $\Sigma = \Sigma_c \dot{\cup} \Sigma_u$, onde Σ_c representa os eventos controláveis e Σ_u, os não controláveis, o alfabeto de saída é $T_0 = T \cup \{\tau_0\}$ e o evento silencioso é τ_0. A linguagem gerada por $\mathbf{G^{op}}$ é representada por $L(\mathbf{G^{op}})$ e a linguagem marcada por $\mathbf{G^{op}}$ é representada por $L_m(\mathbf{G^{op}})$. Em um primeiro momento considera-se que $Q_m = Q$ (todas linguagens são prefixo-fechadas), pois não é analisada a questão de bloqueio. A função de saída $w : Q \to T_0$, é definida ao se realizar a modelagem da planta do operador, atribuindo a cada estado um elemento de T_0. No decorrer desta tese, os estados a que são atribuídos elementos de T são chamados de *estados vocalizadores*, e os estados a que são atribuídos τ_0 são os *estados silenciosos*. No nível do gerente, $\mathbf{G^{ge}}$ é definido sobre o alfabeto T. A linguagem gerada por $\mathbf{G^{ge}}$ é representada por $L(\mathbf{G^{ge}})$ e a linguagem marcada reconhecida por esse autômato é representada por $L_m(\mathbf{G^{ge}})$.

Definição 2.3.1. ***Mapa Repórter***[3]***:*** *O canal Inf_{og}, denominado de mapa repórter, é definido de maneira recursiva como a função $\theta : L(\mathbf{G^{op}}) \to T^*$, onde $\theta(\epsilon) = \epsilon$ e*

$$\theta(s\sigma) = \begin{cases} \theta(s) & se\ w(f(q_0, s\sigma)) = \tau_0 \quad ou \\ \theta(s)w(f(q_0, s\sigma)) & se\ w(f(q_0, s\sigma)) \neq \tau_0 \end{cases}$$

O mapa repórter θ é uma função causal, ou seja, uma função que preserva prefixos. Para toda cadeia s e $s' \in L(\mathbf{G^{op}})$, se s é prefixo de s' ($s \leq s'$), então $\theta(s)$ é

[3] Em Zhong e Wonham (1990), ω é definido como uma função do mapa repórter θ. Entretanto, no presente trabalho, optou-se por apresentar ω como um elemento definido diretamente no modelo da planta, o que é mais óbvio do ponto de vista de modelagem, enquanto que θ pode ser definido como uma função de ω.

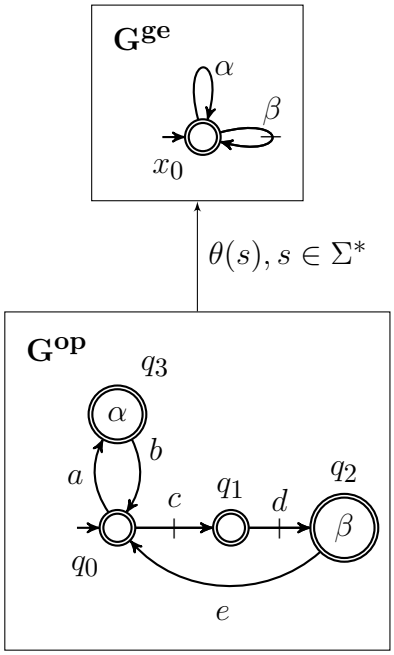
prefixo de $\theta(s')$ ($\theta(s) \leq \theta(s')$). A linguagem reportada ao nível gerencial $L(\mathbf{G^{ge}})$ pelo operador é chamada de θ-imagem da linguagem $L(\mathbf{G^{op}})$, onde:

$$L(\mathbf{G^{ge}}) = \theta(L(\mathbf{G^{op}})) = \{t \in T^* : (\exists s \in L(\mathbf{G^{op}}))\ \ t = \theta(s)\}$$

Para toda cadeia $s \in L(\mathbf{G^{op}})$, o mapa repórter gera cadeias $\theta(s) \in T^*$, gerando assim a linguagem $L(\mathbf{G^{ge}}) \subseteq T^*$ que corresponde à linguagem do modelo abstrado do gerente. A cada novo evento gerado pelo operador, o mapa repórter pode informar um novo evento ao gerente (vocalizar um evento) ou não emitir nova informação (silenciar).

Exemplo 2.3.1. *Na Figura 4 observa-se uma arquitetura de dois níveis, com uma planta operacional* $\mathbf{G^{op}}$*,* $\Sigma = \{a, b, c, d, e\}$*, e sua abstração* $\mathbf{G^{ge}}$*, com* $T = \{\alpha, \beta\}$*. O modelo de* $\mathbf{G^{ge}}$ *é obtido por meio do mapa repórter* θ*, em que algumas vocalizações são* $\theta(a) = \alpha$*,* $\theta(cd) = \beta$*.*

Figura 4 – Exemplo de abstração de modelo com dois níveis hierárquicos.



Fonte: Elaborado pelo autor.

A fim de facilitar e enriquecer a análise da estrutura dos autômatos vocalizadores e sua abstração em níveis hierárquicos, define-se o conceito de *palavras vocais* conforme proposto por Wong e Wonham (1998). São definidas como palavras vocais a cadeia vazia ϵ, bem como todas as sequências de eventos que ligam o estado inicial a um estado vocal. Formalmente pode-se dizer que $s \in L(\mathbf{G^{op}})$ é uma palavra vocal, ou ainda uma cadeia vocal, se $s = \epsilon$, ou se $\omega(s) \neq \tau_0$. Essa definição expressa as cadeias do nível operacional que representam modificações relevantes no nível do gerente. Nesta interpretação, a cadeia vazia ϵ pode ser entendida como relevante no sistema do gerente pois se refere à sua inicialização. As cadeias de $\mathbf{G^{op}}$ que não são vocais são chamadas de palavras silenciosas, ou cadeias silenciosas, de $\mathbf{G^{op}}$.

Definição 2.3.2. ***Linguagem vocal (WONG; WONHAM, 1998):*** *Define-se linguagem vocal $L_{voc}(\mathbf{G^{op}}) \subseteq L(\mathbf{G^{op}})$ como o conjunto de todas as palavras vocais no modelo de $\mathbf{G^{op}}$:*

$$L_{voc}(\mathbf{G^{op}}) = \{s \in L(\mathbf{G^{op}}) : \omega(s) \neq \tau_0\} \cup \{\epsilon\}$$

Adicionalmente, define-se o conceito de *trechos silenciosos* para os eventos $\tau \in T$. São entendidos como sequências de eventos que ligam dois estados vocais, ou o estado inicial a um estado vocal, sem que haja algum outro estado vocal entre eles. Para um evento $\tau \in T$, um trecho silencioso correspondente a τ é uma sequência não vazia de eventos $v \in \Sigma^+$, que é antecedida por uma palavra vocal $s \in L(\mathbf{G^{op}})$, com as seguintes condições: a cadeia sv pertence à linguagem gerada por $\mathbf{G^{op}}$ ($sv \in L(\mathbf{G^{op}})$), o estado atingido por sv vocaliza o evento τ ($\omega(sv) = \tau$) e para todo prefixo $v' < v$, em que $v' \in \Sigma^+$, a palavra sv' é silenciosa ($\omega(sv') = \tau_0$) (WONG; WONHAM, 1998).

Definição 2.3.3. ***Conjunto de trechos silenciosos (WONG; WONHAM, 1998):*** *Formalmente, o conjunto de trechos silenciosos correspondentes a um evento $\tau \in T$ é definido por:*

$$\mathcal{X}_\tau = \{v \in \Sigma^+ : (\exists s \in L_{voc}(\mathbf{G^{op}}))\ \ sv \in L_{voc}(\mathbf{G^{op}})\ \ e\ \ \theta(sv) = \theta(s)\tau\}$$

Os eventos do gerente podem ser classificados em controláveis (T_c) e não controláveis (T_u), de acordo com seus trechos silenciosos. Um evento do gerente é controlável se é possível evitar sua ocorrência pela desabilitação de algum evento controlável em cada um dos seus trechos silenciosos. Para os eventos abstratos não controláveis, todos os seus trechos silenciosos são formados unicamente por eventos não controláveis, não sendo possível evitar sua ocorrência.

Definição 2.3.4. ***Controlabilidade dos eventos gerenciais (WONG; WONHAM, 1998):*** *Os eventos da planta do gerente são definidos como controláveis (T_c) e não controláveis (T_u) conforme:*

$$T_c := \{\tau \in T : \mathcal{X}_\tau \subseteq \Sigma^+ - \Sigma_u^+\}$$
$$T_u := \{\tau \in T : \mathcal{X}_\tau \subseteq \Sigma_u^+\}$$

No caso de algum evento do gerente não se classificar nem como T_c nem como T_u, é dito que existe uma ambiguidade na definição da controlabilidade do evento. No Exemplo 2.3.1, o evento β é definido como controlável na planta do gerente $\mathbf{G^{ge}}$ porque existem eventos controláveis em $\mathbf{G^{op}}$ pertencentes às cadeias que ligam o estado inicial, ou qualquer estado vocal, ao estado que vocaliza β. Já o evento α, em $\mathbf{G^{ge}}$, é não controlável, pois, em $\mathbf{G^{op}}$, todas as cadeias de eventos que ligam o estado inicial, ou qualquer estado vocal, ao estado que vocaliza α são formadas unicamente por eventos não controláveis.

O supervisor marcador no nível gerencial é definido como um mapa $\mathcal{S}^{ge} : L(\mathbf{G^{ge}}) \rightarrow \Delta^{ge}$, associado a uma linguagem marcada $M^{ge} \subseteq L_m(\mathbf{G^{ge}})$, onde $\Delta^{ge} = 2^{T_c}$ é a estrutura de controle de $\mathbf{G^{ge}}$, ou seja, os eventos a serem desabilitados na planta do gerente para atingir uma dada especificação. Esse supervisor associa um conjunto de eventos desabilitados no gerente a cada sequência de eventos observada na linguagem da planta do gerente. Contudo, pela razão de que a supervisão por $\mathcal{S}^{ge}$ é feita de forma virtual, os sinais de desabilitação de eventos são enviados, por meio do canal Com_{go}, ao mapa de desabilitações do operador, C^{op}, que realiza efetivamente a desabilitação de eventos de $\mathbf{G^{op}}$. Deseja-se que o supervisor no nível gerencial, $\mathcal{S}^{ge}$, seja construído de modo que o sistema em malha fechada, $\mathcal{S}^{ge}/\mathbf{G^{ge}}$, respeite restrições impostas por uma linguagem E^{ge}.

Em termos de implementação, o supervisor $\mathcal{S}^{ge}$ pode ser mais convenientemente representado por um autômato $\mathbf{S^{ge}} = (Y, T, \xi, y_0, Y_m)$ e um mapa de desabilitações $\Phi : Y \rightarrow 2^{T_c}$ que relaciona a cada estado de $\mathbf{S^{ge}}$ um conjunto de eventos a ser desabilitado em $\mathbf{G^{ge}}$.

No nível operacional, por sua vez, o supervisor pode ser definido como um mapa de desabilitações do operador $C^{op} : L(\mathbf{G^{op}}) \times \Delta^{ge} \rightarrow \Delta^{op}$, onde $\Delta^{op} = 2^{\Sigma_c}$ é a estrutura de controle de $\mathbf{G^{op}}$. O mapa C^{op} associa cadeias do operador e desabilitações do gerente a desabilitações do operador. Na prática, a ação de C^{op} se resume em desabilitar determinados eventos em $\mathbf{G^{op}}$ para que, desta forma, sejam desabilitados determinados eventos em $\mathbf{G^{ge}}$.

Definição 2.3.5. ***Mapa de desabilitações do operador (ZHONG; WONHAM, 1990):***

$$\begin{aligned} C^{op}(s, \delta^{ge}) := \{\sigma \in \Sigma_c : (\exists u \in \Sigma_u^*) s\sigma u \in L(\mathbf{G^{op}}) \\ \& \ ((\forall u')\ u' < u) \ \rightarrow \ \omega(s\sigma u') = \tau_0 \\ \& \ \omega(s\sigma u) \in \delta^{ge}\} \end{aligned}$$

onde $s \in L(\mathbf{G^{op}})$ são sequências de eventos da planta do operador, e $\delta^{ge} \in 2^{T_c}$ são sinais, provenientes do supervisor do gerente, indicando os eventos que devem ser desabilitados.

Nesta definição, para um evento ser considerado a desabilitar, devem ser respeitadas três condições. Na primeira, analisa-se se existem cadeias de eventos não controláveis, que seguem $s\sigma$ e fazem parte da linguagem da planta do operador. Na segunda, analisa-se se, dentre estas cadeias não controláveis, todos os seus prefixos, que seguem $s\sigma$, levam a estados silenciosos. Por fim, analisa-se se existe uma requisição no gerente para que o evento em questão seja desabilitado, ou seja, se o estado vocalizador atingido pela cadeia em análise vocaliza um evento que deve ser desabilitado no gerente.

Analisando a Definição 2.3.5 do mapa de desabilitações do operador C^{op}, observa-se que, em uma cadeia que antecede um evento gerencial controlável a ser

desabilitado, a ação de controle é retardada ao máximo. Ou seja, se em tal cadeia do operador houver mais de um evento controlável, o evento a ser desabilitado em $\mathbf{G^{op}}$ deve ser sempre o último antes de atingir o estado vocal.

Conforme discutido na seção anterior, um supervisor é projetado com base em uma especificação com o objetivo de impor um comportamento ao sistema em malha fechada. Os supervisores associam cadeias pertencentes à linguagem de uma planta a eventos que devem ser desabilitados na planta. Por outro lado, ao analisar a definição 2.3.5, observa-se que C^{op} é formalizado somente como um mapa que traduz os comandos do supervisor gerencial em sinais de controle para a planta operacional. Assim, é possível representar o supervisor operacional na forma do mapa $C^{op'} : Q \times \Delta^{ge} \rightarrow \Delta^{op}$, onde Q são os estados da planta operacional, Δ^{ge} são os sinais de desabilitação provenientes do supervisor gerencial e Δ^{op} são os sinais de desabilitações enviados à planta operacional. Esta definição exprime o fato de que o mapa $C^{op'}$ observa os sinais de desabilitação do gerente e, em cada estado da planta operacional, decide quais são os eventos a desabilitar para evitar a ocorrência dos eventos vocais que devem ser desabilitados. A definição do mapa de desabilitações do operador em função dos estados do operador e das desabilitações do gerente é dada conforme equação abaixo:

$$C^{op'}(q, \delta^{ge}) := C^{op}(s, \delta^{ge}),\ para\ s\ tal\ que\ f(q_0, s) = q. \tag{2.4}$$

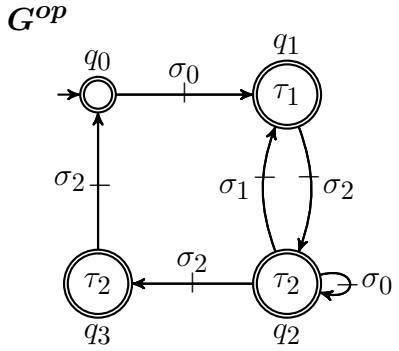
onde $q_0 \in Q$.

A escolha pela utilização de estados na definição do mapa de desabilitações do operador, ao invés de cadeias que levam a estados, se dá por razões de simplicidade na implementação. Conforme ilustrado no exemplo 2.3.2, esse mapa pode ser construído na forma de uma tabela, de maneira genérica independentemente da especificação, com todos os cruzamentos possíveis entre Q e δ^{ge}. A escolha de qual desabilitação efetivamente ocorre na planta do operador é feita em função do supervisor gerencial. No decorrer do texto, estas duas representações apresentadas para o mapa de desabilitações do operador usarão a mesma notação C^{op} e sua diferenciação é dada pelo contexto utilizado.

Exemplo 2.3.2. ***Construção e Representação do Mapa de Desabilitações do Operador:***

O autômato vocalizador da Figura 5 representa o comportamento de uma planta operacional $\mathbf{G^{op}}$, com quatro estados (q_0, q_1, q_2 e q_3) e dois eventos gerenciais: τ_1 é vocalizado em q_1 e τ_2 vocalizado em q_2 e q_3. O mapa de desabilitações do operador C^{op}, construído para a planta $\mathbf{G^{op}}$, faz o cruzamento de todos os estados $q \in Q$ com os eventos gerenciais $\tau \in T$. Esse mapa pode ser construído de maneira genérica, com todos os cruzamentos possíveis, independente da estrutura de $\mathcal{S}^{ge}$.

Figura 5 – Exemplo de planta operacional com vocalizações.



Fonte: Elaborado pelo autor.

A representação de C^{op} para a planta $\mathbf{G^{op}}$ é realizada como na Tabela 1. Na primeira coluna constam os estados da planta do operador $\mathbf{G^{op}}$: (q_0, q_1, q_2 e q_3). Na primeira linha, cada elemento é um evento gerencial a ser desabilitado, ou seja, os sinais de desabilitação provenientes de $\mathcal{S}^{ge}$ (τ_1 e τ_2). Nas demais células da tabela são relacionados, a cada estado de $\mathbf{G^{op}}$, quais são os eventos operacionais ($\sigma_0, \sigma_1, \sigma_2$) que devem ser desabilitados para evitar a ocorrência de eventos de $\mathbf{G^{ge}}$. De acordo com os sinais γ_{ge}, que são as saídas de $\mathcal{S}^{ge}$ indicando quais são os eventos gerenciais a desabilitar, são analisadas as colunas da tabela, relacionando com cada estado de $\mathbf{G^{op}}$ os eventos que devem ser desabilitados no nível do operador para que sejam atingidos os objetivos de $\mathcal{S}^{ge}$.

Tabela 1 – Representação de C^{op} por meio de uma tabela.

$q \in Q$	τ_1	τ_2
q_0	$\{\sigma_0\}$	$\emptyset$
q_1	$\emptyset$	$\{\sigma_2\}$
q_2	$\{\sigma_1\}$	$\{\sigma_0, \sigma_2\}$
q_3	$\emptyset$	$\emptyset$

Fonte: Elaborado pelo autor.

A fim de propor uma padronização para a notação relacionada ao controle hierárquico de SEDs, para a planta do operador define-se, a partir do seu mapa de desabilitações, um supervisor induzido pelo gerente.

Definição 2.3.6. ***Supervisor Induzido:***

Em uma estrutura de controle supervisório hierárquico, formada por uma planta do operador $\mathbf{G^{op}}$, uma estrutura de controle do operador $\Delta^{op} = 2^{\Sigma_c}$, um mapa repórter θ, um supervisor gerencial $\mathcal{S}^{ge}$ e um mapa de desabilitações do operador C^{op}, o supervisor induzido $\mathcal{S}^{ge \to op} : L(\mathbf{G^{op}}) \to \Delta^{op}$, com linguagem de marcação $M^{ge \to op} =$

$\theta^{-1}(M^{ge})$*, é definido como:*

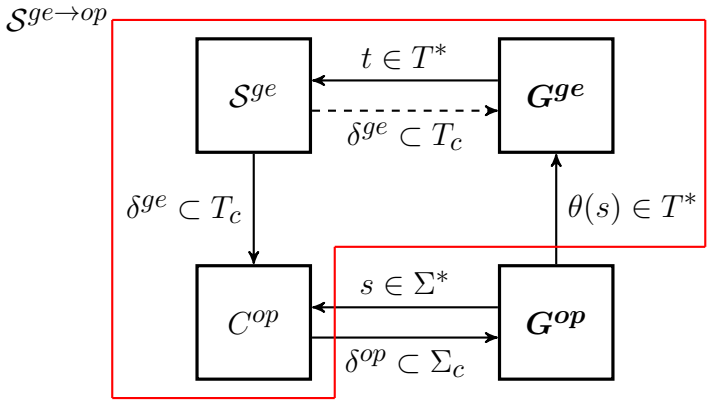
$$\mathcal{S}^{ge\to op}(s) := C^{op}(s, S^{ge}(\theta(s))), \tag{2.5}$$

onde $s \in L(\mathbf{G^{op}})$*.*

Desta forma, as linguagens gerada e marcada de malha fechada de $\mathbf{G^{op}}$ sob supervisão de $\mathcal{S}^{ge\to op}$ são representadas por $L(\mathcal{S}^{ge\to op}/\mathbf{G^{op}})$, que contém todas as cadeias de $\mathbf{G^{op}}$ que não são desabilitadas por $\mathcal{S}^{ge\to op}$, e $L_m(\mathcal{S}^{ge\to op}/\mathbf{G^{op}}) = L_m(\mathcal{S}^{ge\to op}/\mathbf{G^{op}}) \cap M^{ge\to op}$ respectivamente.

Diante desses elementos, a arquitetura hierárquica pode ser melhor detalhada como na Figura 6. Nesta estrutura, Σ e Σ_c são alfabeto e conjunto de eventos controláveis da planta operacional, T e T_c são alfabeto e eventos controláveis do gerente, $\theta(s)$ é o mapa repórter que sinaliza eventos relevantes para o gerente, δ^{ge} são desabilitações provenientes do supervisor do gerente e δ^{op} desabilitações do operador. A linha pontilhada com as desabilitações do gerente (δ^{ge}) indica que a supervisão nesse nível é virtual, ou seja os comandos do supervisor do gerente são enviados para tradução pelo operador para executar as desabilitações de eventos no nível operacional. O supervisor induzido pelo gerente é representado como um agente que recebe cadeias $s \in \Sigma^*$ e age diretamente no operador com as desabilitações $\delta^{op} \subset \Sigma_c$.

Figura 6 – Arquitetura detalhada para controle hieráquico.



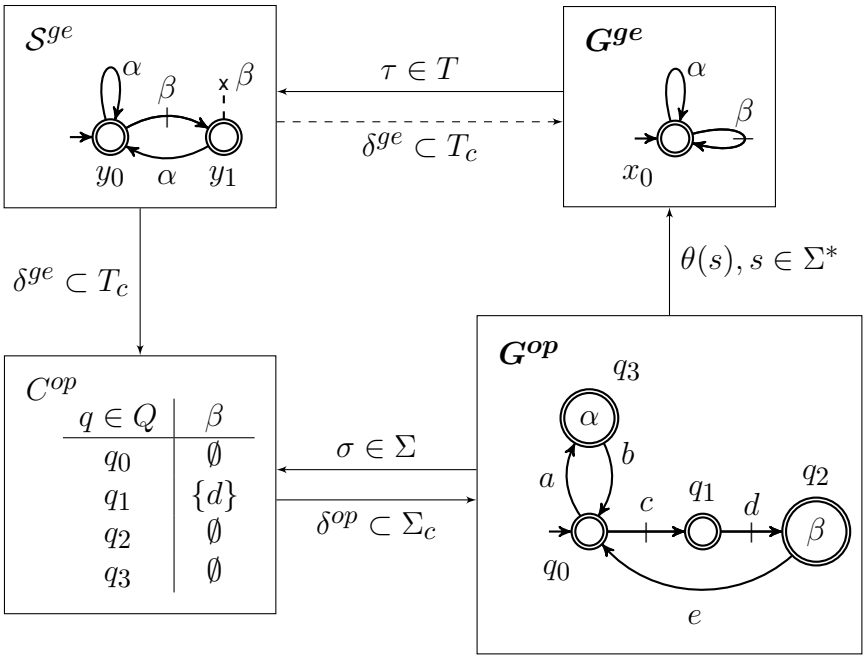
Fonte: Elaborado pelo autor.

O exemplo 2.3.3 a seguir apresenta como é a construção da estrutura completa de controle hierárquico, com a planta do operador, planta do gerente, supervisor gerencial e, fechando a malha de controle, o supervisor operacional.

Exemplo 2.3.3. ***Arquitetura Completa de Controle Hierárquico:***

Como exemplo de arquitetura completa de um sistema com controle hierárquico, podem ser observados os modelos da Figura 7. Os autômatos $\mathbf{G^{op}}$ *e* $\mathbf{G^{ge}}$ *são os mesmos da Figura 4. O supervisor* $\mathcal{S}^{ge}$ *é construído de modo que, no nível gerencial, sempre depois da ocorrência do evento* β*, haja a ocorrência do evento* α*.*

Figura 7 – Exemplo de arquitetura completa de controle hierárquico.



Fonte: Elaborado pelo autor.

Observa-se que a diretiva de comando de $\mathcal{S}^{ge}$ (desabilitar evento β), pode ser traduzida de maneira direta para a estrutura de controle do nível operacional. Neste exemplo, observa-se que a única linha da tabela com desabilitações é referente ao estado q_1, desabilitando o evento d. É importante notar que, segundo a definição de C^{op}, em uma cadeia de eventos controláveis como no exemplo em questão, o evento d é o último evento controlável antes de atingir o estado vocal q_2, por esta razão, d é escolhido como evento a desabilitar ao invés do evento c. Neste exemplo, nota-se também que a ocorrência do evento α em $\mathbf{G^{ge}}$, apesar de estar elegível nessa planta, pode ser incerta dependendo do estado ativo em $\mathbf{G^{op}}$.

Em um sistema de controle hierárquico deseja-se que o comportamento em malha fechada desempenhado pelo operador, ao ser reportado ao gerente por meio do mapa repórter, canal Inf_{og}, seja o mais próximo possível do comportamento esperado pela malha fechada do gerente. De modo a atingir esse objetivo da arquitetura de controle hierárquico serão analisadas algumas definições que compreendem a estrutura do modelo de $\mathbf{G^{op}}$, que podem ser citadas como consistência de controle e consistência de controle estrita. Dependendo da estrutura do modelo da planta do operador, $\mathbf{G^{op}}$, pode-se atingir diferentes níveis de consistência da estrutura hierárquica, como consistência hierárquica de baixo nível e consistência hierárquica propriamente dita.

2.3.1 Consistência Hierárquica de Baixo Nível

Ao projetar os supervisores em uma arquitetura de controle hierárquico, é desejável que o comportamento em malha fechada do operador, ao ser transmitido ao gerente, seja o mais próximo possível do comportamento esperado na malha fechada virtual do nível gerencial. Para atingir tal objetivo, os aspectos que devem ser analisados referem-se à estrutura do modelo da planta do operador e mapa repórter associado. A fim de examinar a estrutura do autômato do operador, é utilizado o conceito de trechos silenciosos ($\mathcal{X}_\tau$), conforme Definição 2.3.3.

O primeiro requisito a ser analisado é o de consistência de controle. Diz-se que o par formado pela planta do operador e seu mapa repórter $(\mathbf{G^{op}}, \theta)$ possui *consistência de controle* sempre que é possível determinar com precisão a controlabilidade de todos os eventos vocalizados para o nível gerencial, de acordo com a Definição 2.3.4. Em outras palavras, esse conceito indica o particionamento do alfabeto do gerente (T) em eventos controláveis (T_c) e não controláveis (T_u), podendo ser expresso por $T = T_c \cup T_u$, em que $T_c \cap T_u = \emptyset$. Se, para algum evento do gerente, houver alguma ambiguidade na definição da controlabilidade, essa relação não é satisfeita e a propriedade de consistência não é atingida.

Definição 2.3.7. ***Consistência de Controle (ZHONG; WONHAM, 1990):***

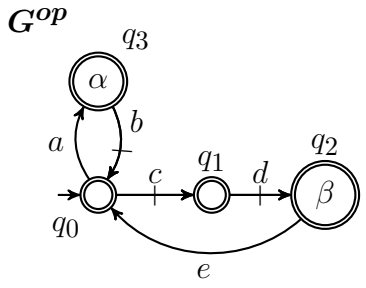
O par formado por uma planta operacional $\mathbf{G^{op}}$ *e seu mapa repórter associado* θ *possui consistência de controle se:*

$$T = T_c \ \dot{\cup} \ T_u$$

No exemplo 2.3.3, Figura 7, observa-se que os eventos gerenciais α e β podem ser precisamente particionados em T_c e T_u respectivamente, pois $\mathcal{X}_\alpha = \{a, ba, ea\}$ possui cadeias de eventos unicamente não controláveis, e as cadeias de $\mathcal{X}_\beta = \{cd, ecd, bcd\}$ que contêm ao menos um evento controlável. Para exemplificar um caso em que não se atinge a consistência, altera-se a planta do operador $\mathbf{G_{op}}$ da figura anterior, modificando o evento b para controlável, como na Figura 8. Nesse caso, a controlabilidade de α se torna indeterminada. No conjunto $\mathcal{X}_\alpha$, referente ao evento gerencial α, existem cadeias não controláveis (a, ea) e existe uma cadeia que passa a ser controlável (ba), tornando ambígua sua controlabilidade.

Conforme proposto por Zhong e Wonham (1990), para casos como do exemplo, é possível refinar o modelo para que seja adquirida consistência de controle. A ideia básica é encontrar um novo modelo que mantenha a linguagem do nível operacional e crie novos estados e novos eventos gerenciais que possibilitem particionar os eventos do gerente em controláveis e não controláveis. Tomando como exemplo o modelo da Figura 8, o evento α é dividido em outros dois: α_c controlável e α_u não controlável e criado mais um estado vocal para possibilitar a construção do novo modelo apresen-

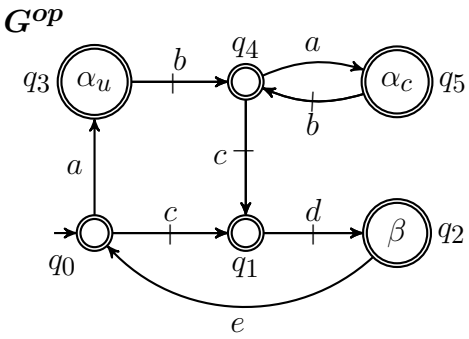
Figura 8 – Planta operacional e mapa repórter sem consistência de controle.



Fonte: Elaborado pelo autor.

tado na Figura 9. Nesse novo modelo percebe-se que todos os trechos silenciosos de α_u são não controláveis e os de α_c são controláveis. Com essas alterações, é correto afirmar que o par formado pela planta $\mathbf{G^{op}}$ e o mapa repórter associado possuem consistência de controle.

Figura 9 – Planta operacional e mapa repórter com consistência de controle.



Fonte: Elaborado pelo autor.

Para o projeto dos supervisores, primeiramente leva-se em conta uma especificação para a planta do gerente E^{ge}, ou seja, uma linguagem alvo que representa o comportamento esperado em malha fechada em nível gerencial. Contudo, como a supervisão de $\mathbf{G^{ge}}$ é feita de forma virtual, deseja-se que a síntese de um supervisor para o operador corresponda a $Sup\mathcal{C}(\theta^{-1}(E^{ge}))$, em que $\theta^{-1}(E^{ge})$ corresponde à versão de E^{ge} no nível do operador. A definição da θ-imagem inversa $\theta^{-1} : 2^{T^*} \rightarrow 2^{L(\mathbf{G^{op}})}$ de uma linguagem pode ser expressa por:

$$E^{op} = \theta^{-1}(E^{ge}) = \{s \in L(\mathbf{G^{op}}) : (\exists t \in E^{ge})\ \theta(s) = t\} \tag{2.6}$$

Conforme demonstrado em Zhong e Wonham (1990), em uma arquitetura de controle hierárquico, se o par formado por uma planta do operador $\mathbf{G^{op}}$ e seu mapa repórter associado θ possui consistência de controle, então o par $(\mathbf{G^{op}}, \mathbf{G^{ge}})$ possui *consistência hierárquica de baixo nível*.

Proposição 2.3.1. ***Consistência hierárquica de baixo nível (ZHONG; WONHAM, 1990):*** *Seja uma estrutura de controle hierárquico formada por uma planta do operador* $\mathbf{G^{op}}$*, seu mapa repórter associado* θ *e uma planta do gerente* $\mathbf{G^{ge}}$*. Se o par (*$\mathbf{G^{op}}$*,* θ*) possuir consistência de controle, então para qualquer especificação* $E^{ge} \subseteq L(\mathbf{G^{ge}})$ *não vazia, prefixo-fechada e controlável, a ação do supervisor induzido no operador será tal que:*

$$L(\mathcal{S}^{ge \to op}/\mathbf{G^{op}}) = Sup\mathcal{C}(\theta^{-1}(E^{ge})).$$

Por outro lado, a consistência de controle não garante que o comportamento em malha fechada do operador ($Sup\mathcal{C}(\theta^{-1}(E^{ge}))$), ao ser transmitido para o gerente ($\theta(Sup\mathcal{C}(\theta^{-1}(E^{ge})))$, seja igual ao comportamento esperado pelo gerente (E^{ge}). Existem situações em que pode haver uma característica denominada de palavras vocais parceiras (detalhada na próxima seção) que faz com que haja efeitos colaterais ao se desabilitar um estado gerencial. Somente a título de ilustração, tomando como exemplo o modelo da Figura 9, nota-se que para desabilitar o evento gerencial α_c é preciso desabilitar o evento b, seja em q_3 ou q_5. Entretanto esta diretiva de comando acaba por desabilitar, involuntariamente, o evento β o que reduz as possibilidades de execução pelo supervisor em malha fechada. Esta característica faz com que o comportamento transmitido pelo operador seja apenas uma sublinguagem do comportamento esperado pelo gerente:

$$\theta(Sup\mathcal{C}(\theta^{-1}(E^{ge}))) \subseteq E^{ge}.$$

De todo modo, a consistência hierárquica de baixo nível garante que o comportamento em malha fechada transmitido pelo operador sempre pode satisfazer requisitos de alguma especificação controlável para o gerente, ou seja, garante que não ocorram eventos proibidos no gerente. Por exemplo, tomando como ilustração o modelo da Figura 9, se a especificação a nível gerencial proibe a ocorrência de α_c, esse requisito com certeza será respeitado, apesar de possivelmente ocorrer o efeito colateral da desabilitação do evento gerencial β.

2.3.2 Consistência Hierárquica

Ao analisar a propriedade da consistência hierárquica de baixo nível, observa-se que pode haver especificações controláveis que são realizáveis pelo gerente, mas que não são imagem de comportamentos realizáveis para o operador. Por outro lado, a propriedade de consistência hierárquica estabelece que todo comportamento realizável por um supervisor para o gerente é a imagem de um comportamento realizável por um supervisor do operador.

Definição 2.3.8. ***Consistência Hierárquica (ZHONG; WONHAM, 1990):*** *Em uma estrutura de controle hierárquico formada por uma planta do operador $\mathbf{G^{op}}$, seu mapa repórter associado θ e uma planta do gerente $\mathbf{G^{ge}}$, existe consistência hierárquica entre $\mathbf{G^{op}}$ e $\mathbf{G^{ge}}$ se para qualquer especificação $E^{ge} \subseteq L(\mathbf{G^{ge}})$ não vazia, prefixo-fechada e controlável em relação à $\mathbf{G^{ge}}$*

$$\theta(Sup\mathcal{C}(\theta^{-1}(E^{ge}))) = E^{ge} \tag{2.7}$$

Ao analisar a estrutura formada pela planta do operador e seu mapa repórter associado, percebe-se que pode haver uma característica que leva a efeitos colaterais na desabilitação de eventos gerenciais. Esta particularidade é conhecida na literatura como a existência de palavras vocais parceiras, e aparece quando, ao desabilitar um evento gerencial, acaba-se por desabilitar algum outro evento gerencial involuntariamente.

Definição 2.3.9. ***Palavras vocais parceiras (ZHONG; WONHAM, 1990):*** *Definem-se como palavras vocais parceiras as cadeias $s_1 = s'\sigma_c s'' v_1$ e $s_2 = s'\sigma_c s'' v_2$, com $s' \in \Sigma^*$, $\sigma_c \in \Sigma_c$, $s'' \in \Sigma_u^*$, que apresentam as seguintes características:*

1. *Iniciam no mesmo estado vocal e levam a eventos gerenciais distintos:*

$$\exists q \in Q,\ \exists s \in \Sigma^* : \hat{f}(q_0, s) = q,\ \ s \in L_{G_{op}Voc}\ e\ \hat{\omega}(ss_1) \neq \hat{\omega}(ss_2);$$

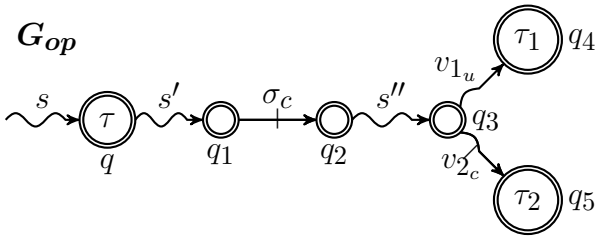
2. *São trechos silenciosos controláveis:*

$$\text{Para } \tau_1 = \hat{\omega}(ss_1) \text{ e } \tau_2 = \hat{\omega}(ss_2),\ s_1 \in \mathcal{X}_{\tau_1}, s_2 \in \mathcal{X}_{\tau_2}, \tau_1\ e\ \tau_2 \in T_c;$$

3. *Dos segmentos distintos (v_1 e v_2), ao menos um é formado exclusivamente de eventos não controláveis ($v_1\ \ ou\ \ v_2 \in \Sigma_u^+$).*

A Figura 10 apresenta a forma como as palavras vocais podem aparecer em um modelo, sendo $v_{1_u} \in \Sigma_u^+$ uma cadeia não controlável, $v_{2_c} \in \Sigma^+ - \Sigma_u^+$ uma cadeia controlável, $s \in \Sigma^*$, $s' \in \Sigma^*$, $\sigma_c \in \Sigma_c$ e $s'' \in \Sigma_u^*$.

Figura 10 – Palavras vocais parceiras.

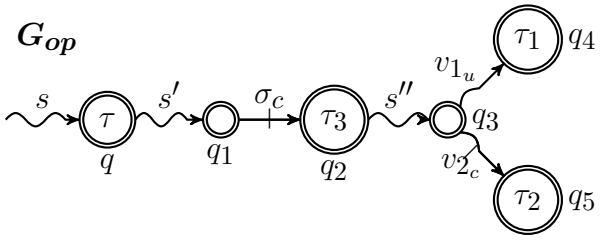


Fonte: Elaborado pelo autor.

Na figura, as palavras (cadeias) são representadas com linhas onduladas, diferentemente da notação para eventos. Para as cadeias controláveis utiliza-se a mesma notação que representa eventos controláveis (*tick*). Pode-se perceber que para impedir a ocorrência do evento gerencial τ_1, deve-se desabilitar σ_c. No entanto, além disto, esta ação causa a desabilitação do evento gerencial τ_2, o que caracteriza s_1 e s_2 como palavras vocais parceiras.

De forma a eliminar as palavras vocais parceiras, Zhong e Wonham (1990) apresentam um algoritmo que acrescenta um evento gerencial adicional, a fim de modificar os eventos vocalizados pelas sequências s_1 e s_2, reduzindo assim o comprimento de seus trechos silenciosos e redefinindo a controlabilidade dos eventos gerenciais, como ilustrado na Figura 11.

Figura 11 – Eliminação das palavras vocais parceiras.



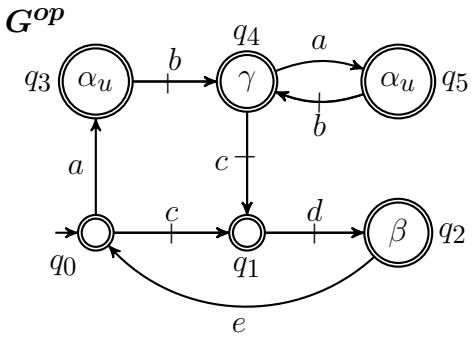
Fonte: Elaborado pelo autor.

No caso do exemplo ilustrado, adiciona-se um evento gerencial τ_3 no estado q_2. Assim, o evento τ_1 se torna não controlável, o que faz com que as palavras vocais que iniciam em q_2 e levam a τ_1 e τ_2 não sejam mais parceiras.

Para ilustrar o conceito, observa-se o autômato da Figura 9 e as palavras vocais $s_1 = aba$ e $s_2 = abcd$. Os eventos gerenciais relacionados a essas cadeias são $\alpha_c = \hat{\omega}(s_1)$ e $\beta = \hat{\omega}(s_2)$. Estas cadeias compartilham a cadeia inicial ab, em que b é o primeiro evento do trecho silencioso compartilhado pelas duas cadeias. Nota-se que no estado q_3, para desabilitar α_c, o supervisor do operador deve desabilitar o evento b. Contudo, esta ação acaba causando a desabilitação do evento β, o que é claramente um efeito colateral causado por estas duas palavras vocais parceiras. Para eliminar as palavras parceiras, adiciona-se um evento $\gamma \in T$ no estado q_4. Esta modificação causa alteração na controlabilidade do evento vocalizado em q_5, que passa a ser não controlável, recebendo a etiqueta α_u. Desta forma, nenhum evento gerencial apresenta ambiguidade na definição da sua controlabilidade, e obtém-se o novo modelo de planta operacional livre de palavras vocais parceiras apresentado na Figura 12.

Em uma estrutura formada por uma planta operacional e seu mapa repórter associado, se o par $(\mathbf{G^{op}}, \theta)$ possuir consistência de controle, ao se eliminar a existência das palavras vocais parceiras, pode-se afirmar que para a estrutura hierárquica atinge-se *consistência de controle estrita*.

Figura 12 – Planta operacional sem palavras vocais parceiras.



Fonte: Elaborado pelo autor.

Definição 2.3.10. ***Consistência de controle estrita (ZHONG; WONHAM, 1990):*** *O par $(\mathbf{G^{op}}, \theta)$ com consistência de controle possui consistência de controle estrita se em sua estrutura não existem palavras vocais parceiras.*

Abaixo afirma-se que se o par $(\mathbf{G^{op}}, \theta)$ possui consistência de controle estrita, então o par $(\mathbf{G^{op}}, \mathbf{G^{ge}})$ possui *consistência hierárquica*.

Proposição 2.3.2. ***Consistência hierárquica (ZHONG; WONHAM, 1990):*** *Seja uma estrutura de controle hierárquico formada por uma planta do operador $\mathbf{G^{op}}$, seu mapa repórter θ e uma planta do gerente $\mathbf{G^{ge}}$. Se o par $(\mathbf{G^{op}}, \theta)$ possuir consistência de controle estrita, então, para qualquer especificação $E^{ge} \subseteq L(\mathbf{G^{ge}})$ não vazia, controlável e.r.a $\mathbf{G^{ge}}$ e prefixo-fechada, haverá consistência hierárquica entre $\mathbf{G^{op}}$ e $\mathbf{G^{ge}}$.*

2.3.3 Controle Hierárquico Não Bloqueante

Ao analisar uma estrutura de controle hierárquico, leva-se em conta que os conceitos de consistência hierárquica de baixo nível e consistência hierárquica não dizem respeito à linguagem marcada do operador, ou seja, não levam em conta a problemática de bloqueio. Por esta razão, faz-se a ressalva de que para a análise desses dois conceitos, considera-se que para a planta do operador $Q_m = Q$. Contudo, ao realizar a análise de sistemas cujas linguagens não são todas prefixo-fechadas, pode aparecer o problema de bloqueio.

Nas seções anteriores, os exemplos analisados foram casos em que $L(\mathbf{G^{op}}) = L_m(\mathbf{G^{op}})$. Nsses casos, as linguagens do gerente são $L(\mathbf{G^{ge}}) = L_m(\mathbf{G^{ge}}) = \theta(L(\mathbf{G^{op}}))$. A partir da presente seção, são analisados casos em que para o operador $Q_m \subseteq Q$, e $L_m(\mathbf{G^{ge}}) \subseteq L(\mathbf{G^{ge}})$, onde $L_m(\mathbf{G^{ge}}) = \theta(L_m(\mathbf{G^{op}}))$ e $L(\mathbf{G^{ge}}) = \theta(L(\mathbf{G^{op}}))$. A definição da linguagem marcada de malha fechada do operador pode ser feita da mesma forma como para um supervisor marcador monolítico, ao se considerar $\theta^{-1}(E^{ge})$ uma linguagem marcada:

$$L_m(\mathcal{S}^{ge \to op}/\mathbf{G^{op}}) = L(\mathcal{S}^{ge \to op}/\mathbf{G^{op}}) \cap \theta^{-1}(E^{ge}) \quad 2.8$$

De uma forma geral, Wong e Wonham (1996) levantam duas situações em que pode aparecer bloqueio em sistemas com dois níveis hierárquicos. Com o objetivo de sanar o problema de bloqueio nesses dois casos, é necessário garantir duas características adicionais ao modelo da planta do operador.

A primeira característica diz respeito à consistência entre as linguagens marcadas dos dois níveis, ou seja, quando o par $(\mathbf{G^{op}}, \mathbf{G^{ge}})$ possui a denominada *consistência de marcação*. Esse conceito pode ser definido como: devem ser marcadas todas as cadeias do operador cuja imagem no gerente seja uma cadeia marcada.

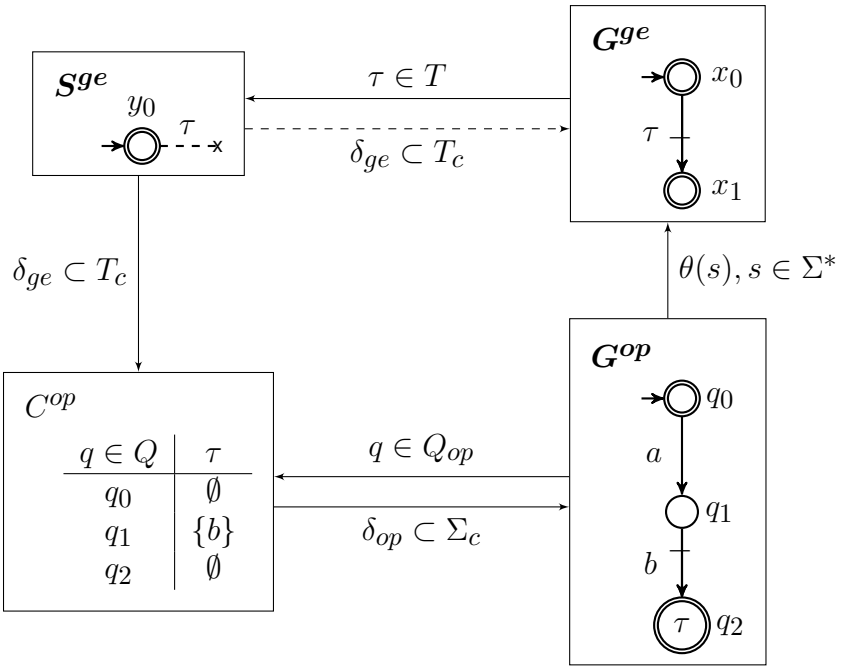
Definição 2.3.11. ***Consistência de marcação (WONG; WONHAM, 1998):*** *Existe consistência de marcação entre* $\mathbf{G^{op}}$ *e* $\mathbf{G^{ge}}$ *quando:*

$$\theta^{-1}(L_m(\mathbf{G^{ge}})) = L_m(\mathbf{G^{op}})$$

O exemplo abaixo ilustra um caso em que não há consistência de marcação na estrutura hierárquica, e a ação do supervisor induzido pode gerar uma situação de bloqueio na planta do operador.

Exemplo 2.3.4. ***Não há consistência de marcação.*** *Como ilustrado na figura 13, com a ocorrência das cadeias* ϵ *ou* a*,* $\mathbf{G^{ge}}$ *permanece no mesmo estado* x_0*.*

Figura 13 – Estrutura de controle hierárquico sem consistência de marcação.



Fonte: Elaborado pelo autor.

Contudo, como o supervisor S^{ge} *tem como objetivo desabilitar a ocorrência do evento* τ*, o mapa* C^{op} *desabilita o evento* b *quando* $\mathbf{G_{op}}$ *encontra-se em* q_1*. Nota-se que com esta ação dos supervisores a planta operacional pode permanecer bloqueada no estado não marcado* q_1 *quando da desabilitação do evento* b*.*

A partir dessa definição, é possível chegar a uma versão da consistência hierárquica em que são consideradas as linguagens marcadas. Esse resultado é obtido a partir das conclusões discutidas nas referências já citadas (WONG; WONHAM, 1996, 1998), apesar de que os autores não o colocam de maneira explícita.

Proposição 2.3.3. ***Consistência hierárquica com marcação:*** *Seja uma estrutura de controle hierárquica formada por uma planta do operador $\mathbf{G^{op}}$, seu mapa repórter associado θ e uma planta do gerente $\mathbf{G^{ge}}$. Se o par ($\mathbf{G^{op}}, \theta$) possuir consistência de controle estrita e existir consistência de marcação entre $\mathbf{G^{op}}$ e $\mathbf{G^{ge}}$, então, para qualquer especificação $E^{ge} \subseteq L_m(\mathbf{G^{ge}})$ não vazia e controlável e.r.a. $\mathbf{G^{ge}}$, garante-se que*

$$\theta(L_m(S^{ge\rightarrow op}/\mathbf{G^{op}})) = E^{ge} \tag{2.9}$$

Demonstração. ($\subseteq$):

Considerando consistência de marcação entre $\mathbf{G^{op}}$ e $\mathbf{G^{ge}}$, Como $E^{ge} \subseteq L_m(\mathbf{G^{ge}})$, pode-se afirmar que $\theta^{-1}(E^{ge}) \subseteq L_m(\mathbf{G^{op}})$.

Assim, conforme equação 2.8, a linguagem marcada do sistema em malha fechada do supervisor induzido é:

$$L_m(\mathcal{S}^{ge\rightarrow op}/\mathbf{G^{op}}) = L(\mathcal{S}^{ge\rightarrow op}/\mathbf{G^{op}}) \cap \theta^{-1}(E^{ge})$$

Aplicando o operador θ:

$$\theta(L_m(\mathcal{S}^{ge\rightarrow op}/\mathbf{G^{op}})) = \theta(L(\mathcal{S}^{ge\rightarrow op}/\mathbf{G^{op}}) \cap \theta^{-1}(E^{ge}))$$

Partindo de

- $\theta(L(\mathcal{S}^{ge\rightarrow op}/\mathbf{G^{op}}) \cap \theta^{-1}(E^{ge})) \subseteq \theta(L(\mathcal{S}^{ge\rightarrow op}/\mathbf{G^{op}}))$ e
- $\theta(L(\mathcal{S}^{ge\rightarrow op}/\mathbf{G^{op}}) \cap \theta^{-1}(E^{ge})) \subseteq \theta(\theta^{-1}(E^{ge})))$,

chega-se a:

$$\begin{aligned}\theta(L_m(\mathcal{S}^{ge\rightarrow op}/\mathbf{G^{op}})) &= \theta(L(\mathcal{S}^{ge\rightarrow op}/\mathbf{G^{op}}) \cap \theta^{-1}(E^{ge})) \\ &\subseteq \theta(L(\mathcal{S}^{ge\rightarrow op}/\mathbf{G^{op}})) \cap \theta(\theta^{-1}(E^{ge})))\end{aligned}$$

Sabe-se da Proposição 2.3.2 que $\theta(L(\mathcal{S}^{ge\rightarrow op}/\mathbf{G^{op}})) = \overline{E^{ge}}$.
Além disso, pode-se afirmar que $\theta(\theta^{-1}(E^{ge})) = E^{ge}$.
Assim:

$$\theta(L_m(\mathcal{S}^{ge\rightarrow op}/\mathbf{G^{op}})) \subseteq \overline{E^{ge}} \cap E^{ge} = E^{ge}$$

($\supseteq$):
Da Proposição 2.3.2, $\theta(L(\mathcal{S}^{ge\rightarrow op}/\mathbf{G^{op}})) = \overline{E^{ge}}$.
Como $E^{ge} \subseteq \overline{E^{ge}}$, então:

$$\theta(L(\mathcal{S}^{ge\rightarrow op}/\mathbf{G^{op}})) \supseteq E^{ge} \tag{1}$$

Mas, como $E^{ge} \subseteq L_m(\mathbf{G^{ge}})$, pela consistência de marcação, a equação (1) torna-se:

$$\theta(L_m(\mathcal{S}^{ge \to op}/\mathbf{G^{op}})) \supseteq E^{ge}$$

□

Outra característica que pode levar a bloqueio na estrutura hierárquica se relaciona ao mapa repórter. A um modelo de planta operacional, está associado um *mapa repórter observador* quando todo prefixo de cadeias do operador que correspondem a um mesmo evento gerencial não deve ser seguido por cadeias que levem a eventos gerenciais distintos entre si.

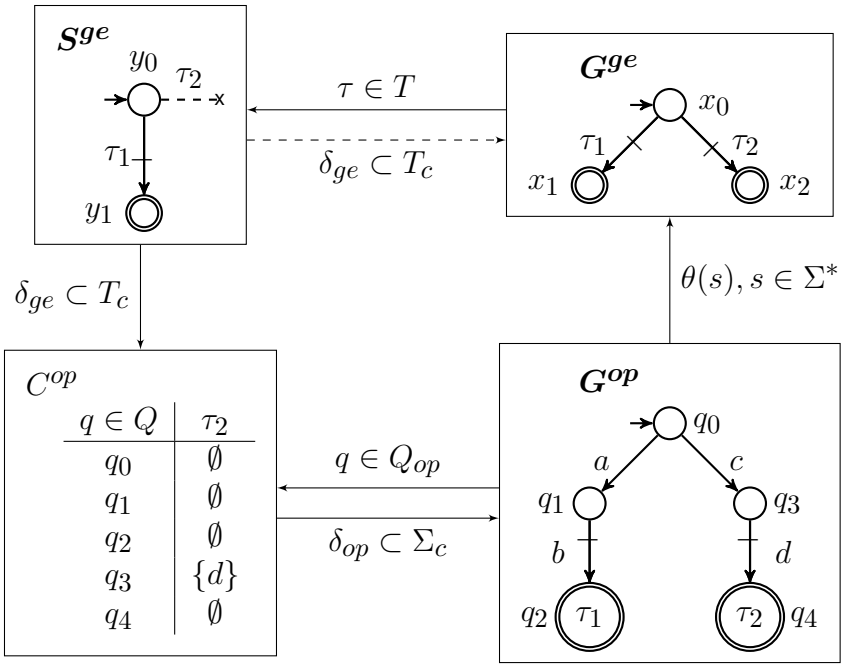
Definição 2.3.12. ***Mapa repórter observador (WONG; WONHAM, 1998):*** *Um mapa repórter θ associado a uma planta do operador $\mathbf{G_{op}}$ possui a propriedade de observador quando:*

$$(\forall s \in L(\mathbf{G^{op}}))(\forall t \in T^+)\ \theta(s)t \in \theta(L(\mathbf{G^{op}})) \to \exists u \in \Sigma^+ : su \in L(\mathbf{G^{op}})\ \&\ \theta(su) = \theta(s)t$$

Essa condição pode ser ilustrada em uma estrutura como a da Figura 14. Neste exemplo, observa-se que a ocorrência das cadeias $s = a$ e $s = c$ não sinaliza alterações no modelo de $\mathbf{G^{ge}}$, que permanece no estado x_0. Ressalta-se que são duas cadeias pertencentes a trechos silenciosos distintos que levam a eventos gerenciais diferentes. Por outro lado, o supervisor $\boldsymbol{S^{ge}}$ tem como objetivo desabilitar a ocorrência do evento τ_2. Para executar esse comando, o operador C^{op} desabilita o evento d quando $\mathbf{G^{op}}$ encontra-se no estado q_3. É exatamente esta ação do supervisor do operador que caracteriza a situação de bloqueio, pois o modelo da planta do operador pode permanecer bloqueado no estado q_3. Em casos similares ao apresentado, quando um prefixo de uma cadeia de eventos gerenciais é a imagem de duas ou mais cadeias que levam a eventos gerenciais distintos, pode-se dizer que o mapa repórter não possui a propriedade de observador.

A condição de controle hierárquico não bloqueante garante que todo comportamento do operador, que é realizável por um supervisor não bloqueante, pode ser mapeado para um comportamento no nível gerente que seja realizável por um supervisor não bloqueante. Em Wong e Wonham (1996) é demonstrado que em uma arquitetura de controle hierárquico é garantido que não há bloqueio quando são respeitadas três condições: o par $(\mathbf{G^{op}}, \theta)$ deve possuir consistência de controle estrita, o par $(\mathbf{G^{op}}, \mathbf{G^{ge}})$ deve possuir consistência de marcação e, além disso, à planta do operador $\mathbf{G^{op}}$ deve ser associado um mapa repórter observador,. Além disso, ressalta-se que, ao considerar as condições para garantir consistência hierárquica, obtém-se controle supervisório hierárquico ótimo.

Figura 14 – Estrutura de controle hierárquico com mapa repórter não observador.



Fonte: Elaborado pelo autor.

Proposição 2.3.4. ***Controle Hierárquico Não Bloqueante (WONG; WONHAM, 1998):*** *Seja uma estrutura de controle hierárquico formada por uma planta do operador $\mathbf{G^{op}}$, seu mapa repórter associado θ e uma planta do gerente $\mathbf{G^{ge}}$. Para qualquer especificação $E^{ge} \subseteq L_m(\mathbf{G^{ge}})$ não vazia e controlável em relação a $\mathbf{G^{ge}}$, tal que existe um supervisor não bloqueante $\mathcal{S}^{ge}$ com $L_m(\mathcal{S}^{ge}/\mathbf{G^{ge}}) = E^{ge}$, se $(\mathbf{G^{op}}, \theta)$ possuir consistência de controle estrita e existir consistência de marcação entre $\mathbf{G^{op}}$ e $\mathbf{G^{ge}}$, pode-se garantir que:*

i) $\theta(L_m(\mathcal{S}^{ge \to op}/\mathbf{G^{op}})) = E^{ge}$ ***e***

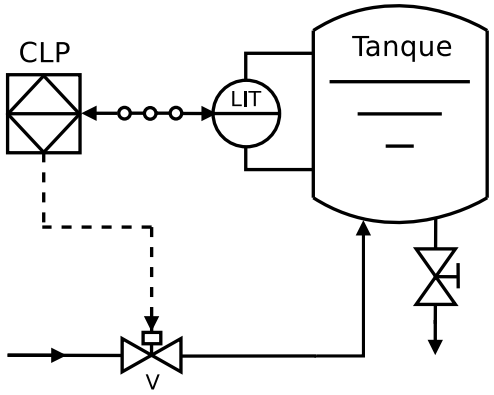
ii) Além disso, se θ possuir a propriedade de observador, o supervisor $\mathcal{S}^{ge \to op}$ será não bloqueante para $\mathbf{G^{op}}$.

2.4 EXEMPLO DE MODELAGEM E SÍNTESE DE SUPERVISORES EM ARQUITETURA DE CONTROLE HIERÁRQUICO

Nessa seção será apresentado um exemplo em que o processo industrial é bastante simplificado, com o objetivo de ilustrar o método de modelagem e síntese de controle supervisório hierárquico não bloqueante. Algumas discussões sobre decisões de modelagem são suprimidas neste exemplo, mas apresentadas em maiores detalhes no Capítulo 3, onde é mostrada uma aplicação real. O processo em questão, como mostra a Figura 15, consiste em um tanque em que ocorre a medição de nível pelo

sensor LIT, variável que é controlada por meio de uma válvula de bloqueio V, único atuador do sistema. De modo ilustrativo, o controle supervisório é implementado em um controlador lógico programável.

Figura 15 – Processo industrial comandado por uma válvula de bloqueio.

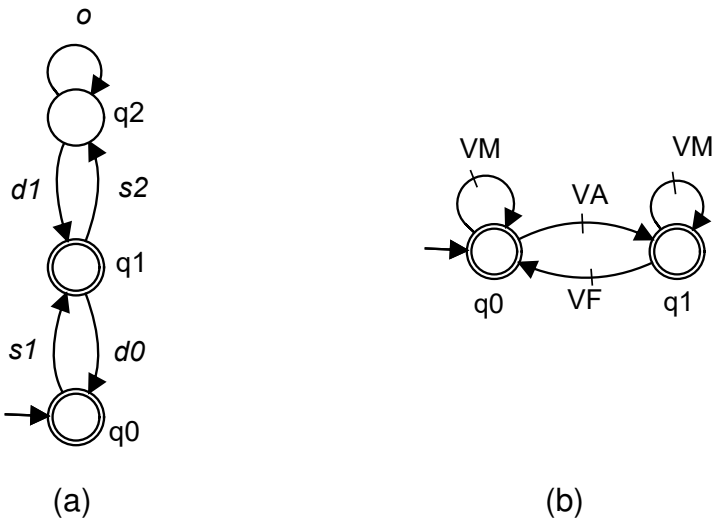


Fonte: Elaborado pelo autor.

O valor do nível no tanque consiste em uma variável contínua e, para o controle supervisório, é realizada uma discretização desses valores. Como apresentado no modelo $\mathbf{G_N}$ (Figura 16 - a), apenas três limiares de nível são relevantes: nível baixo (estado q_0), nível médio (estado q_1) e nível alto (estado q_2). Os eventos $s1$ e $s2$ representam a subida para os níveis médio e alto respectivamente. Os eventos $d1$ e $d0$ representam a descida para os níveis médio e baixo respectivamente. Considera-se que depois de atingir o nível alto, é possível ocorrer *overflow*, evento o, quando o líquido transborda do tanque. Nesse modelo, apenas o estado que representa o nível alto é considerado como não marcado. O modelo da válvula de bloqueio $\mathbf{G_V}$ é apresentado na Figura 16 (b), em que seus dois estados são marcados. A válvula inicia como fechada e em cada estado há um auto-laço com o evento Válvula Mantém (VM) que indica uma ação da válvula de permanecer no mesmo estado. O evento VF significa válvula fecha e VA, válvula abre.

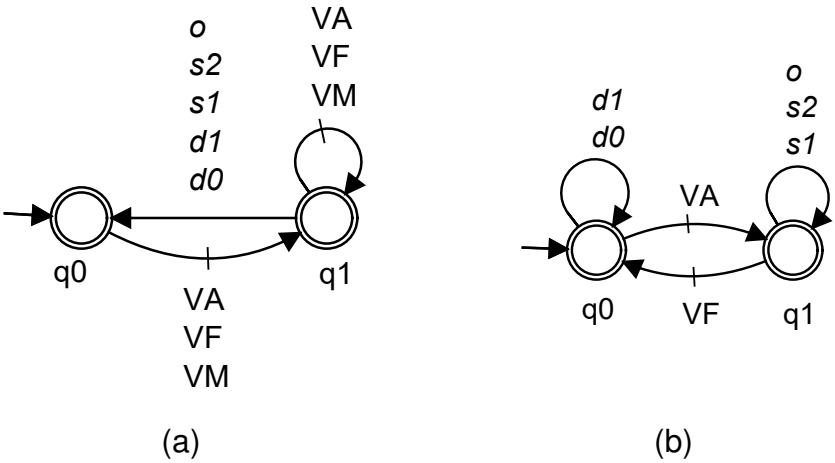
Nesta aplicação, é empregado o conceito da preempção dos níveis do tanque por meio da válvula. Essa é uma hipótese de modelagem que afirma que a cada alteração de nível de líquido no tanque segue-se ao menos uma ação da válvula. O autômato $\mathbf{G_P}$ que modela a preempção é ilustrado na Figura 17 (a). Com isso, torna-se possível garantir a controlabilidade do sistema mesmo considerando que as alterações de nível sejam eventos não controláveis. Nesta seção, essa abordagem é utilizada sem apresentar uma discussão aprofundada, o que é feito no próximo capítulo, onde são expostas suas vantagens e comparação com outros métodos. Na Figura 17 (b) é apresentado o modelo da vazão no tanque, $\mathbf{G_{VAZ}}$. Esse modelo relaciona a cada estado do atuador quais são as possibilidades de variação do nível do tanque, ou seja, com a válvula fechada o nível desce, com a válvula aberta o nível sobe.

Figura 16 – Processo industrial comandado por uma válvula de bloqueio: (a) modelo de níveis no tanque $\mathbf{G_N}$ e (b) modelo da válvula de bloqueio $\mathbf{G_V}$.



Fonte: Elaborado pelo autor.

Figura 17 – Processo industrial comandado por uma válvula de bloqueio: (a) modelo da preempção $\mathbf{G_P}$ e (b) modelo da vazão no tanque $\mathbf{G_{VAZ}}$.

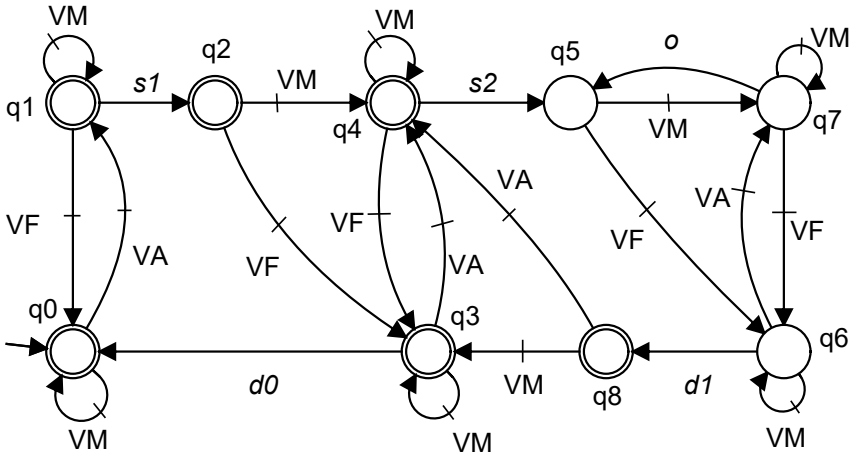


Fonte: Elaborado pelo autor.

Na Figura 18 é apresentado o autômato $\mathbf{G}$, que é a composição paralela dos modelos de $\mathbf{G_N}$, $\mathbf{G_V}$, $\mathbf{G_P}$ e $\mathbf{G_{VAZ}}$. Apenas os estados q_5, q_6 e q_7 não são marcados. A partir do estado q_7 pode ocorrer o evento não controlável de *overflow*. Para ser possível evitar a ocorrência desse evento, por sua natureza não controlável, deve-se impedir atingir o estado q_7. De modo a ilustrar a aplicação do controle hierárquico, sugere-se que a decisão de evitar *overflow* seja direcionada ao nível gerencial, enquanto que a operação mais básica do processo seja reservada ao nível operacional.

Com isso, utilizando a metodologia apresentada nas seções anteriores, deve-se inserir as vocalizações nos estados da planta $\mathbf{G}$, resultando no autômato que representa a planta do operador $\mathbf{G^{op}}$ na estrutura hierárquica (Figura 19). Desta forma, inicia-se pela vocalização do evento O (letra maiúscula), que sinaliza para o gerente a

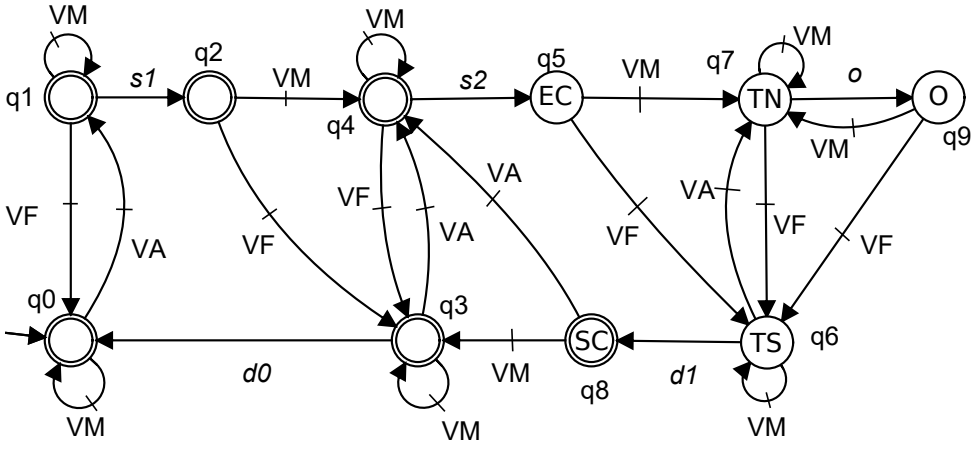
Figura 18 – $\mathbf{G}$: Autômato da planta global de um processo industrial comandado por uma válvula de bloqueio.



Fonte: Elaborado pelo autor.

ocorrência de *overflow*. No autômato $\mathbf{G}$, o evento o leva ao estado q_5, que, entretanto, também é atingido pelo evento $s2$. Para evitar ambiguidade na vocalização, em $\mathbf{G^{op}}$, q_5 é desmembrado em um estado q_9, que recebe o evento o e vocaliza o evento O.

Figura 19 – $\mathbf{G^{op}}$: Modelo da planta operacional com as vocalizações em um processo industrial comandado por uma válvula de bloqueio.



Fonte: Elaborado pelo autor.

A modelagem das vocalizações deve preservar a coerência em relação ao comportamento do processo industrial, mas normalmente permite uma certa liberdade visando atingir as propriedades de consistência na estrutura hierárquica. Para garantir a propriedade de consistência de marcação, como o estado inicial é marcado, todos os estados que formam um trecho silencioso antes de atingir uma próxima vocalização devem também ser marcados. Por essa razão vocaliza-se o estado q_5, que é o primeiro não marcado partindo do estado inicial. Seguindo o mesmo raciocínio, todos os trechos

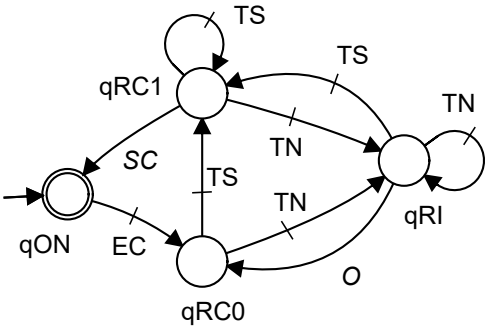
silenciosos que partem de q_5 devem ser não marcados e, por essa razão vocaliza-se o estado q_8. Pode-se interpretar que o sistema Entra em uma região Crítica de operação ao atingir o estado q_5 (vocaliza o evento EC) e Sai dessa região Crítica ao atingir o estado q_8 (evento SC). Fisicamente a região crítica de operação inicia quando o tanque atinge o nível alto com a transição $s2$, quando já está próximo de ocorrer *overflow*, e finaliza quando o tanque volta ao nível médio com a transição $d1$.

Tendo realizado as vocalizações nos estados q_5, q_8 e q_9, mas ainda com os estados q_6 e q_7 silenciosos, observa-se a existência de palavras vocais parceiras e, com isso, não atinge-se a consistência de controle estrita. Observa-se que, partindo do estado q_5, para evitar a ocorrência do evento O deve-se desabilitar o evento VM; entretanto, essa situação acaba por desabilitar também a cadeia $VM\ VF\ d1$ por exemplo, o que caracteriza a existência de palavras vocais parceiras. Para contornar esse problema e ser possível garantir consistência de controle estrita, que leva à consistência hierárquica, deve-se vocalizar também os estados q_6 e q_7. Observa-se que, em uma primeira análise, não haveria problema em desabilitar, mesmo como efeito colateral, a cadeia apresentada nas linhas acima ($VM\ VF\ d1$), até porque, mesmo nessa situação, o evento SC ainda poderia ocorrer no gerente. Mas nesse exemplo segue-se a metodologia apresentada pelos autores citados neste capítulo, em que a consistência de controle estrita é uma das condições para se garantir consistência hierárquica.

Para atingir consistência hierárquica, os eventos gerenciais associados aos estados q_6 e q_7 não precisariam necessariamente ser diferentes. Mas, para conseguir preservar a propriedade de observador do mapa repórter associado à planta $\mathbf{G^{op}}$, devem ser escolhidos eventos diferentes para esses estados. Caso contrário, o gerente não conseguiria distinguir se o operador se encontra em q_6 ou q_7 e, desta forma, haveria ambiguidade para encontrar um supervisor não bloqueante para evitar a ocorrência de *overflow*. Por essa razão, o estado q_6 vocaliza o evento TS representando uma Transição Segura dentro da região crítica, em que o *overflow* ainda pode ser evitado e q_7 vocaliza o evento TN, representando uma Transição Não segura dentro da região crítica, pois o *overflow* não pode ser evitado nesse estado.

Com isso, o modelo da planta do operador $\mathbf{G^{op}}$ e seu mapa repórter associado atingem todos os requisitos para que seja possível garantir, para qualquer especificação controlável do gerente, um controle hierárquico ótimo e não bloqueante (proposição 2.3.4). Na Figura 20 é apresentado o modelo abstrato da planta do gerente. O estado inicial é o único marcado e representa a operação normal do sistema. Os estados $qRC0$ e $qRC1$ representam que o sistema entrou na região crítica. O estado qRI representa que o risco de ocorrer *overflow* é inevitável. Para evitar a ocorrência de *overflow* o supervisor deve evitar que ocorra uma transição não segura (TN), para que não se atinja o estado qRI.

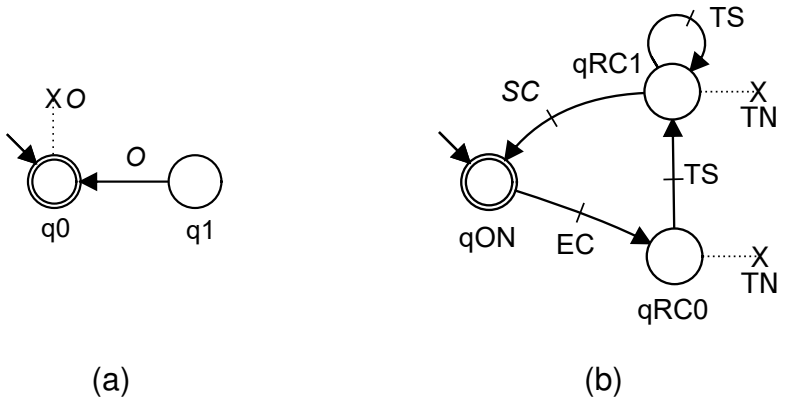
Figura 20 – $\mathbf{G^{ge}}$: Modelo da planta do gerente em um processo industrial comandado por uma válvula de bloqueio.



Fonte: Elaborado pelo autor.

A especificação gerencial E^{ge} para evitar o *overflow* é apresentada na Figura 21 (a). Essa especificação expressa que, no estado inicial, todos os eventos são permitidos, exceto o evento de *overflow*. Em outras palavras, expressa que no sistema em malha fechada deseja-se que esse evento de fato não ocorra em nenhuma situação. Na Figura 21 (b) é apresentado o modelo $\mathcal{S}^{ge}$ do supervisor gerencial que, ao entrar na região crítica, desabilita uma transição não segura (TN).

Figura 21 – Processo industrial comandado por uma válvula de bloqueio: (a) especificação E^{ge} para evitar *overflow*, (b) supervisor gerencial $\mathcal{S}^{ge}$.



Fonte: Elaborado pelo autor.

Como os eventos da planta do gerente são abstratos, os comandos de desabilitação por parte do supervisor gerencial são traduzidos pelo mapa C^{op} como desabilitações reais para a planta do operador (Tabela 2). Assim, para evitar a vocalização de TN, nos estados q_5 e q_6 do operador, respectivamente os eventos VM e VA são desabilitados. Em outras palavras, para evitar TN, que representa uma transição não segura em uma situação em que o tanque já está em um nível alto e com risco de transbordar, é necessário evitar abrir a válvula, ou evitar que a válvula seja mantida aberta.

Tabela 2 – Mapa de desabilitações C^{op} do operador em um processo industrial comandado por uma válvula de bloqueio:.

$q \in Q$	TN	
q_0	$\emptyset$	
q_1	$\emptyset$	
...	...	
q_5	$\{VM\}$	
q_6	$\{VA\}$	

Fonte: Elaborado pelo autor.

2.5 DISCUSSÃO

Neste capítulo foi apresentada a teoria de controle supervisório e algumas extensões para redução da complexidade. Foi apresentado o controle supervisório hierárquico como um método capaz de separar em níveis hierárquicos diferentes tipos de decisão. No exemplo apresentado, foi ilustrada a aplicação do método para obtenção de um controle hierárquico ótimo e não bloqueante para um exemplo simples. Apresentou-se de maneira simplificada alguns aspectos de modelagem para sistemas contínuos, como a utilização do conceito de preempção, que serão melhor discutidos no capítulo 3. Foi mostrado de maneira didática como projetar as vocalizações em uma planta operacional de modo a se atingir as consistências necessárias. Da mesma forma, foi possível observar algumas limitações e restrições dos métodos existentes, no sentido de que em alguns casos as consistências impõem condições demasiadamente conservadoras.

No exemplo apresentado, com o intuito de simplificar, utilizou-se somente uma válvula como atuador. No entanto, ao inserir mais elementos em um circuito de componentes, como outras válvulas ou bombas por exemplo, é possível surgir, no nível do operador, a problemática da explosão combinatória de estados. De forma a viabilizar a modelagem de um circuito de componentes, uma alternativa é a utilização da abordagem por abstrações sucessivas em uma estrutura hierárquica, o que será apresentado no capítulo 4. Por outro lado, constatou-se também no exemplo apresentado que algumas restrições da Proposição 2.3.4 para garantir as consistências necessárias para o controle hierárquico não bloqueante (consistência hierárquica estrita, consistência de marcação e mapa repórter observador) são demasiadamente restritivas. Com esse intuito, como um dos resultados desta tese, será formalizada no capítulo 5 uma nova condição que flexibiliza a propriedade de mapa repórter observador, para permitir a implementação de uma gama maior de especificações em uma estrutura hierárquica.

3 SÍNTESE DE SUPERVISORES PARA UM PROCESSO INDUSTRIAL COM CONTROLE PID E IMPLEMENTAÇÃO EM REDE FOUNDATION FIELDBUS

Este capítulo apresenta resultados sobre a aplicação da teoria de controle supervisório de SEDs em um processo industrial que opera em uma rede Foundation Fieldbus. O processo em questão faz parte de uma planta piloto desenvolvida pela Nova Smar S/A (NOVA SMAR S/A, 2023) situada no Departamento de Automação e Sistemas, na Universidade Federal de Santa Catarina, destinada ao estudo e pesquisa sobre controle de processos e tecnologias de automação. Os objetivos deste estudo são propor uma metodologia de modelagem, sintetizar e implementar um sistema de controle supervisório para garantir restrições de segurança no funcionamento do processo em malha fechada, tanto no modo de regime permanente, quanto nos modos de inicialização e parada. Neste trabalho foram implementados supervisores modulares para garantir os modos de operação, a ação reativa dos atuadores e o intertravamento entre a bomba e a válvula. Além dos supervisores modulares, foi utilizado um coordenador para resolução de conflitos. Nesta aplicação, o controle básico do processo é reservado ao controlador PID, que realiza a regulagem do nível de líquido em torno de um *set point*, enquanto que os supervisores projetados se destinam a garantir o funcionamento seguro do processo dentro de alguns limites de segurança, interferindo somente quando necessário. O presente estudo resultou em um artigo apresentado no evento *Workshop on Discrete Event Systems (WODES) 2020*, sob o título de Síntese de Supervisores para Um Processo Industrial com Controle PID e Implementação em Foundation Fieldbus (*Synthesis of Supervisors for a PID-Controlled Industrial Process and Implementation on Foundation Fieldbus*). Essa aplicação é inspirada em um trabalho de mestrado que resultou na publicação de Muler *et al.* (2018), que implementa um supervisor monolítico para garantir limites de segurança de nível durante o funcionamento em regime permanente do mesmo processo analisado.

A planta piloto (Figura 22) possibilita o controle de variáveis como nível, vazão e temperatura. Possui dois tanques interligados por tubulações, nas quais existem válvulas dispostas em malhas. Seus principais atuadores são bombas de vazão de líquido, válvulas de controle com posicionadores inteligentes e resistências de aquecimento. A planta dispõe de instrumentos inteligentes que se comunicam entre si por meio de uma rede industrial Foundation Fieldbus. Para interface com usuário e comando manual, há um painel de interface humano máquina (IHM) com chaves seletoras, botoeiras e sinalizadores. Um CLP é responsável por realizar a lógica de controle centralizada, fazendo a ponte entre sensores, atuadores, painel e rede Foundation Fieldbus.

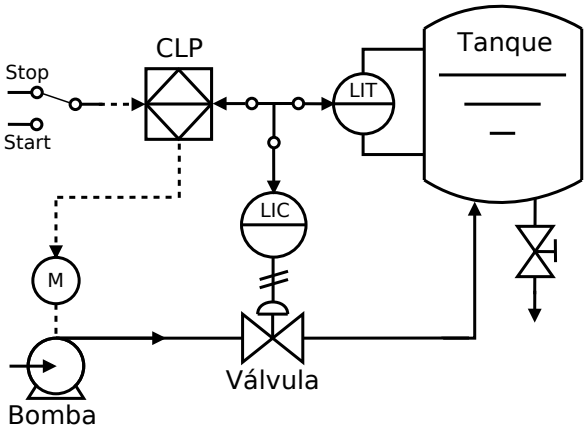
O processo sobre o qual este estudo foi desenvolvido consiste nos elementos ilustrados na Figura 23. A dinâmica contínua se dá pelo controle de nível de líquido no tanque, que é medido por um sensor de nível (LIT) por pressão diferencial. Uma bomba centrífuga fornece líquido para o sistema, que possui também uma válvula de

Figura 22 – Planta piloto situada no Departamento de Automação e Sistemas.

Fonte: Elaborado pelo autor.

controle que regula a quantidade de líquido que é inserida no tanque. Uma válvula manual regula a vazão de líquido na saída do tanque. O CLP recebe comandos de uma chave seletora no painel IHM referentes ao início (*Start*) e finalização (*Stop*) do processo, recebe o valor da medição de nível, bem como a abertura da válvula. Esse controlador envia sinais para o acionamento da bomba e da válvula de controle. A válvula empregada nesse processo é de acionamento pneumático e dotada de um posicionador inteligente que controla a sua abertura. Neste estudo a dinâmica da válvula é projetada com três estados, o que a possibilita se situar totalmente aberta, totalmente fechada e em valores intermediários realizando o controle de nível. A comunicação entre o CLP, sensor de nível (LIT) e posicionador da válvula (LIC) se dá por meio de uma rede industrial Foundation Fieldbus.

Figura 23 – Diagrama de instrumentação do processo estudado.



Fonte: Elaborado pelo autor.

Neste trabalho utilizou-se de forma bastante simplificada uma abstração da dinâmica contínua para obtenção de uma dinâmica discreta aproximada. As características do sistema estudado, bem como os objetivos do controle supervisório projetado, permitem inferir de maneira direta quais são os eventos observados no processo. Este trabalho difere das teorias de sistemas híbridos, onde se aplicam métodos formais para obtenção de abstrações da dinâmica contínua a partir de seu modelo matemático, conforme discussão apresentada na Seção 3.1.

Aproveitando-se das características do processo em estudo, a presente abordagem de modelagem proposta emprega o conceito de preempção dos eventos da dinâmica contínua. Pelo fato de que a dinâmica do sistema contínuo é mais lenta do que o acionamento dos atuadores, é possível garantir que sempre haverá tempo de atuar no sistema antes da ocorrência de algum evento do processo. Esse fato permite o emprego da teoria de controle supervisório, ao desenvolver supervisores de natureza permissiva, o que difere de abordagens que propõem a alteração dessa teoria para utilizar o conceito de eventos forçados, como em Sanchez (1996).

3.1 COMPLEXIDADE DOS SISTEMAS HÍBRIDOS

Conforme já mencionado, comumente os processos industriais apresentam características de dinâmicas contínuas combinadas com dinâmica a eventos discretos, o que os caracteriza como sistemas híbridos. O estudo de sistemas híbridos se divide em algumas vertentes na literatura. Algumas abordagens voltam-se a apropriar a teoria clássica de sistemas contínuos para incorporar sistemas discretos com chaveamentos. Tipicamente, nesses casos são enfatizados resultados sobre estabilidade (PETTERSSON; LENNARTSON, 2000). Outras abordagens buscam representar a dinâmica contínua dos sistemas híbridos em dinâmicas a eventos discretos, buscando a análise e síntese de supervisores. Dentre essas abordagens se destacam as que se baseiam em abstrações discretas da dinâmica contínua, a fim de obter, a partir do sistema contínuo, um sistema a eventos discretos aproximado (ALUR *et al.*, 2000). A dinâmica discreta é determinada por eventos que são gerados quando variáveis do espaço de estados contínuo atingem uma superfície de limiar, o que força transições no estado discreto. Esses são chamados de sistemas híbridos dirigidos por eventos de limiar (GONZÁLEZ *et al.*, 2001).

Ainda no contexto de controle supervisório de sistemas híbridos, existem abordagens cuja intermediação da troca de informações entre a planta e o supervisor é feita por uma interface particular, que é análoga a conversores de sinais analógico-digitais (KOUTSOUKOS *et al.*, 2000). Nessa estrutura, a planta evolui ao longo do tempo até que uma variável de seu espaço de estados contínuo cruza determinado limite e então a interface sinaliza a ocorrência de um evento para o supervisor. Esse, por sua vez, atualiza seu estado discreto e, de acordo com o estado atual, envia um sinal (também

discreto) para a interface, a qual o transforma em um sinal contínuo a ser aplicado na planta. Assim, na perspectiva do supervisor, o conjunto planta-interface é um sistema a eventos discretos, pois recebe e envia apenas sinais discretos e então o controlador é projetado usando metodologias de controle supervisório de SEDs.

Em geral, a dinâmica discreta que deriva do procedimento de obtenção de abstrações discretas de um modelo contínuo não possui um modelo com número finito de estados. As abordagens que trabalham com a obtenção de abstrações discretas, que correspondem a aproximações externas do modelo exato, utilizam-se de hipóteses conservadoras sobre a dinâmica híbrida original (ALUR *et al.*, 1995; CURY *et al.*, 1998; RAISCH; O'YOUNG, 1998; MOOR *et al.*, 2002; CHUTINAN; KROGH, 2003). Formalmente essas abordagens se baseiam na modelagem matemática do comportamento contínuo e na definição de superfícies limites para as variáveis de estado. Assim, o modelo discreto é construído sobre um alfabeto cujos eventos têm como significado o cruzamento desses limites nas variáveis de estado. Os estados do modelo discreto não são um simples particionamento do espaço de estados contínuo, mas mantém uma coerência da dinâmica futura em relação ao estado contínuo. Para a construção do controle supervisório, as hipóteses sobre a dinâmica híbrida para a obtenção do modelo discreto devem garantir que as especificações não sejam violadas, ou seja, que o supervisor para o modelo aproximado seja também correto para o modelo exato.

No caso dos processos industriais considerados nesta tese, a dinâmica contínua é simples o suficiente para que não seja necessário empregar os métodos formais para a obtenção das abstrações discretas, apesar de seguir a mesma ideia conceitual. Consideram-se processos em que a variável de processo varia de forma unidimensional, o que permite definir as superfícies de cruzamento como apenas pontos ao invés de, por exemplo, curvas em um plano. Para esclarecer a ideia, considera-se, por exemplo, um tanque com variação de nível de líquido, em que, para a identificação do cruzamento dos pontos limites, somente é necessário constatar se o nível está aumentando ou diminuindo, o que depende diretamente dos estados dos atuadores. Nesse caso, o conhecimento da dinâmica contínua é necessário somente de forma qualitativa para que sejam elaboradas, sobre o processo industrial, hipóteses de modelagem, como histerese na leitura dos sensores, diferença entre vazão de entrada e de saída do tanque, tempo de resposta dos atuadores, espaçamento entre superfícies limites.

Uma primeira direção a ser tomada neste trabalho diz respeito à modelagem dos processos em questão. No contexto desta pesquisa, é proposta uma abordagem de modelagem para obtenção de modelos de eventos discretos que representem, de maneira condizente com os objetivos do controle supervisório, o processo industrial controlado. Para a abstração da dinâmica contínua, apesar de seguir a mesma ideia conceitual das abstrações discretas, não são empregados métodos formais para sis-

temas híbridos. Visando condições seguras de funcionamento, são definidos limites críticos para as variáveis de processo que servem como superfícies de cruzamento da dinâmica contínua, o que permite a representação do modelo de SEDs.

Como o controle supervisório proposto não visa interferir nas operações básicas do processo, as alterações nas variáveis de processo são consideradas como eventos não controláveis. Sendo assim, as transições relacionadas à variável de processo somente podem ser evitadas de forma indireta pelos supervisores. Com esse objetivo, nessa abordagem é empregado o conceito da preempção da dinâmica contínua por meio dos atuadores discretos. Tal conceito é aplicável considerando-se a hipótese de que a dinâmica dos processos relacionados é mais lenta do que os tempos de acionamento dos atuadores. Para que essa abordagem de modelagem seja viável, devem ser realizadas algumas hipóteses sobre o processo industrial, como por exemplo histerese na leitura dos sensores e espaçamento adequado entre as superfícies limites. Nos processos considerados nesta abordagem, a partir dos estados dos atuadores é simples identificar quais são os eventos discretos gerados em relação à variável de processo. Dessa forma, pode-se obter um modelo de eventos discretos que representa a dinâmica suficientemente simplificada para os objetivos em questão.

3.2 MODELAGEM E SÍNTESE DOS SUPERVISORES

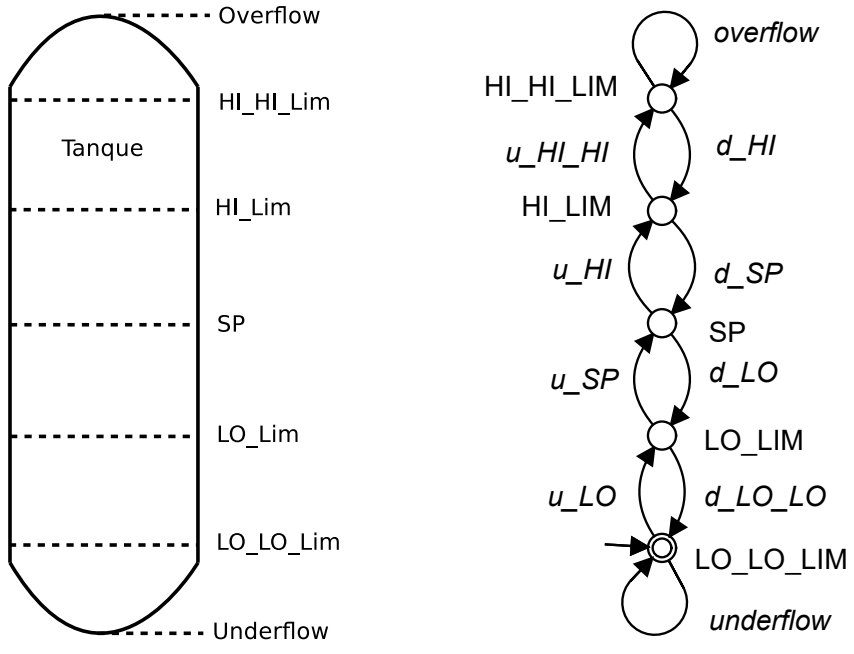
Nesta aplicação, deseja-se projetar supervisores para, em primeiro lugar, garantir quesitos de segurança no funcionamento em regime permanente do processo, mas também a proporcionar procedimentos seguros de inicialização e parada. Os riscos envolvidos em um processo de controle de nível são relacionados basicamente a esvaziamento (*underflow*) e transbordamento (*overflow*) de líquido. Ambas situações podem causar danos nos equipamentos envolvidos e até mesmo aos operadores. Além desses pontos, existe um risco relacionado ao intertravamento entre a bomba e a válvula, devido à forma em que são interligados no sistema, como ilustrado na Figura 23. Não é desejável que a válvula de controle permaneça fechada enquanto a bomba estiver ligada e fornecendo líquido para o tanque, o que pode causar desgaste da bomba e danos no duto.

Modelagem da Planta

Para a modelagem da planta, são considerados sete subsistemas com modelos que dizem respeito aos níveis do tanque ($\mathbf{G_{Níveis}}$), chave de acionamento no painel IHM ($\mathbf{G_{Chave}}$), bomba ($\mathbf{G_{Bomba}}$), preempção na bomba ($\mathbf{G_{PB}}$), válvula ($\mathbf{G_{Válvula}}$), preempção na válvula ($\mathbf{G_{PV}}$), vazão no tanque ($\mathbf{G_{Vazão}}$). A extensão total do tanque é dividida em sete intervalos para operação do nível de líquido, o que segue as recomendações para programação em redes Foundation Fieldbus referente a limites de alarmes para sinais contínuos (FIELDBUS FOUNDATION, 2002). Esses intervalos, ilustrados na Figura 24 (a), são definidos como segue: *overflow* e *underflow* correspondem a

situações de transbordamento e esvaziamento do tanque, respectivamente; HI_HI_Lim e LO_LO_Lim correspondem a situações próximas de *overflow* e *underflow* respectivamente; HI_Lim e LO_Lim são regiões de alerta; SP é um intervalo intermediário em que, no geral, é definido um valor de *set point* para o controle de nível. Os tamanhos e limites utilizados para definição desses intervalos são discutidos na Seção 3.3. O modelo que representa o comportamento do nível de líquido no tanque ($\mathbf{G_{Níveis}}$) é apresentado na Figura 24 (b). São definidos cinco estados, representando cinco dos intervalos de operação para os níveis no tanque. O estado inicial é definido como o tanque vazio, representado por LO_LO_LIM, que também é o estado marcado, o que significa que deseja-se um sistema reinicializável. Todos os eventos desse modelo são considerados como não controláveis, pois não é possível impedir, de forma direta, uma mudança de nível. Cada evento nesse modelo representa que o nível cruza um limite em um intervalo de operação do nível. Os eventos que se iniciam com u referem-se ao aumento do nível no tanque, já os que se iniciam com d referem-se à diminuição do nível. O nome de cada evento indica para qual intervalo o nível está se dirigindo, como por exemplo o evento d_LO indica que o nível de líquido está diminuindo rumo à região LO_Lim.

Figura 24 – (a) Diagrama com intervalos de operação para os níveis no tanque e (b) autômato $\mathbf{G_{Níveis}}$: que representa as mudanças de níveis no tanque.

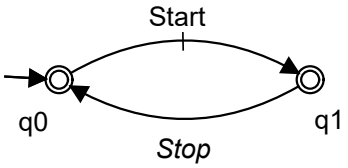


(a) (b)

Fonte: Elaborado pelo autor.

O autômato **G_{Chave}** modela o comportamento da chave seletora presente no painel IHM (Figura 25). São definidos dois estados interligados pelos eventos $Start$ e $Stop$. O evento $Stop$ é definido como não controlável, pois a qualquer momento o operador pode solicitar a parada do processo. Já o evento $Start$ é definido como controlável, pois considera-se que o supervisor pode evitar os efeitos do operador solicitar a inicialização em algum momento inadequado.

Figura 25 – **G_{Chave}**: autômato que modela o comportamento da chave seletora.

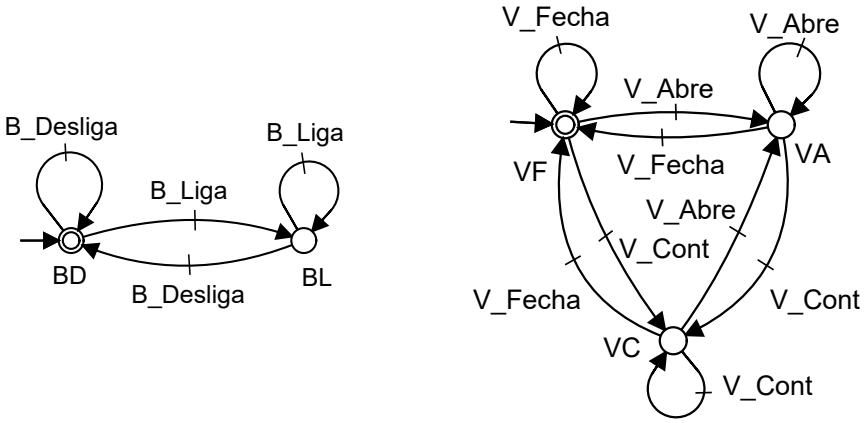


Fonte: Elaborado pelo autor.

O comportamento da bomba é modelado pelo autômato **G_{Bomba}**, apresentado na Figura 26 (a). São definidos dois estados, BD indica que a bomba está desligada e BL indica que a bomba está ligada. Em cada estado é inserido um auto-laço, o que indica que os eventos referentes aos comandos de ligar e desligar a bomba, B_Liga e $B\_Desliga$ respectivamente, podem ocorrer a qualquer momento sem modificar o estado do modelo. O modelo que representa a válvula, autômato **$G_{Válvula}$**, é apresentado na Figura 26 (b). São definidos três estados, onde VF se refere à válvula fechada, VA se refere à válvula aberta e VC correponde à válvula em modo de controle PID regulando o nível no tanque. Nesse modelo também são representados auto-laços, indicando que os eventos de comando podem ocorrer sem alterar o estado da válvula. Os eventos de comando da válvula são todos controláveis, são definidos como V_Fecha, que indica fechamento total da válvula, V_Abre indica a abertura total, e V_Cont indica que a válvula entra no modo de controle. No exemplo da Seção 2.4 foi utilizada uma válvula de bloqueio, que possui somente os estados totalmente aberta ou totalmente fechada. Além disso, em seu modelo, em cada estado consta o evento VM, que indica que a válvula se *mantém* no mesmo estado. Entretanto, na presente aplicação os eventos da bomba e da válvula que indicam a permanência no mesmo estado são os próprios eventos de comando dos autômatos, como observado nos auto-laços da figura abaixo.

Como a dinâmica do nível de líquido no tanque é mais lenta do que os comandos de acionamento da bomba e da válvula, é possível garantir que sempre haja a ocorrência de um evento de comando nestes dois atuadores entre a ocorrência de dois eventos não controláveis de mudança de nível no tanque. Esse é o conceito da preempção dos eventos de nível aplicado neste estudo. Com isso é possível evitar a ocorrência de algum evento de mudança de nível, mesmo de maneira indireta, por meio

Figura 26 – (a) $\mathbf{G_{Bomba}}$: autômato que modela o comportamento da bomba e (b) $\mathbf{G_{Válvula}}$: autômato que representa a o comportamento da válvula.

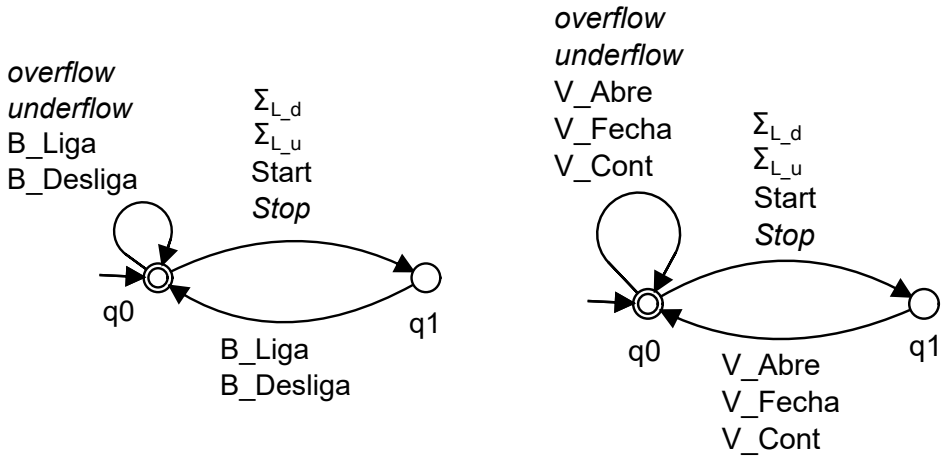


(a) (b)

Fonte: Elaborado pelo autor.

da preempção pelos comandos nos atuadores. Os modelos que representam a preempção pelos eventos da bomba $\mathbf{G_{PB}}$ e da válvula $\mathbf{G_{PV}}$, são representados na Figura 27, em que $\Sigma_{L\_u} = \{u\_LO, u\_SP, u\_HI, u\_HI\_HI\}$ contém os eventos de aumento de nível e $\Sigma_{L\_d} = \{d\_HI, d\_SP, d\_LO, d\_LO\_LO\}$ contém os eventos de diminuição de nível no tanque.

Figura 27 – (a) $\mathbf{G_{PB}}$: preempção pelos eventos da bomba e (b) $\mathbf{G_{PV}}$: preempção pelos eventos da válvula.

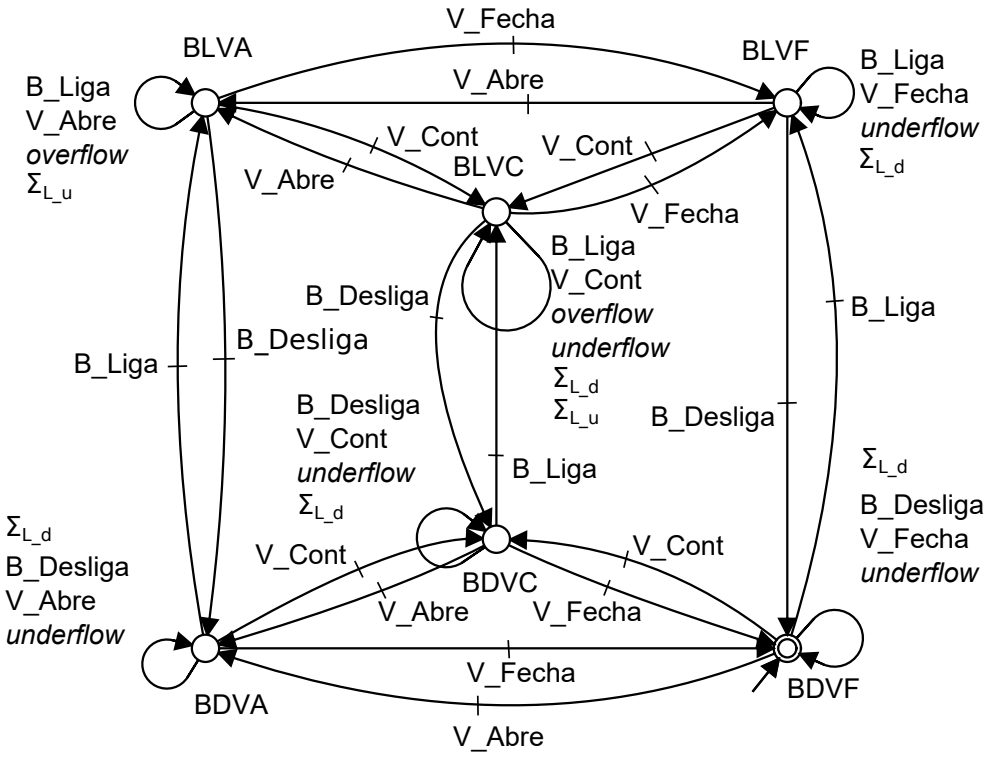


(a) (b)

Fonte: Elaborado pelo autor.

O modelo $\mathbf{G_{Vazão}}$, que relaciona as possíveis mudanças no nível do tanque ao estado dos atuadores é apresentado na Figura 28. Nesse modelo, cada combinação dos estados da bomba e da válvula é relacionado às possíveis alterações no nível. Por exemplo, o estado $BDVF$ indica que a bomba está desligada e a válvula fechada, onde é possível a diminuição no nível, enquanto que $BLVC$ indica bomba ligada e válvula regulando, onde existem todas as possibilidades de mudança de nível.

Figura 28 – **$G_{Vazão}$**: modelo que representa a vazão no tanque.



Fonte: Elaborado pelo autor.

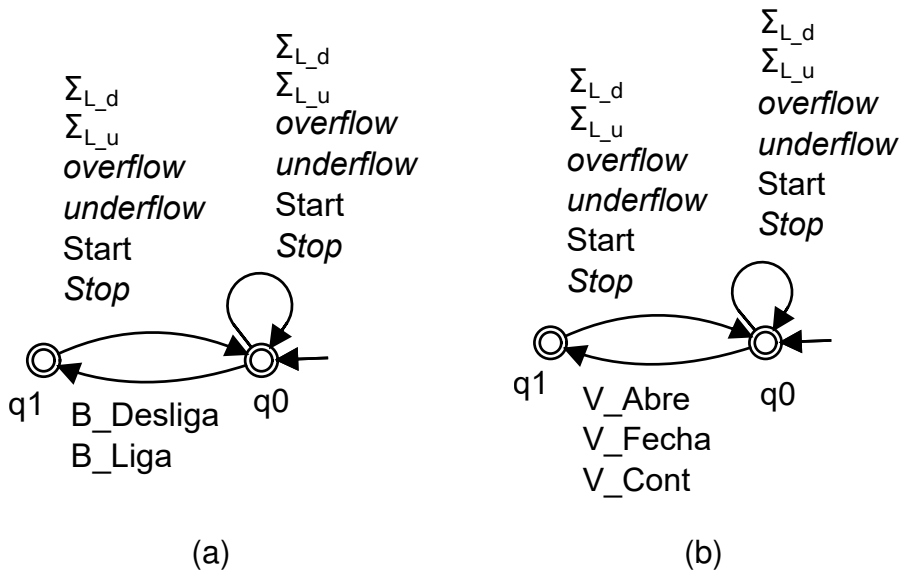
Modelagem das Especificações

Com o objetivo de assegurar restrições de segurança no sistema, são desenvolvidas quatro especificações. Para garantir que os supervisores apresentem características reativas aos eventos do sistema, são criadas as especificações de ação reativa da válvula, E_{AV}, e ação reativa na bomba, E_{AB} (Figura 29). Esses modelos impõem a restrição de que, após qualquer evento de comando de acionamento dos atuadores, somente haja um novo evento de comando depois de ocorrer um evento na planta (mudança de nível ou comando na chave seletora).

Para impedir desgaste na bomba e danos no duto é desenvolvida a especificação de intertravamento entre bomba e válvula, E_{IBV}, apresentada na Figura 30. Esse modelo impede que a bomba permaneça ligada enquanto a válvula estiver fechada. Para que seja habilitado o comando de acionamento da bomba, primeiramente a válvula deve ser aberta ou entrar em modo de regulagem. Esse é um modelo de exclusão mútua entre os estados referentes à bomba ligada e válvula fechada.

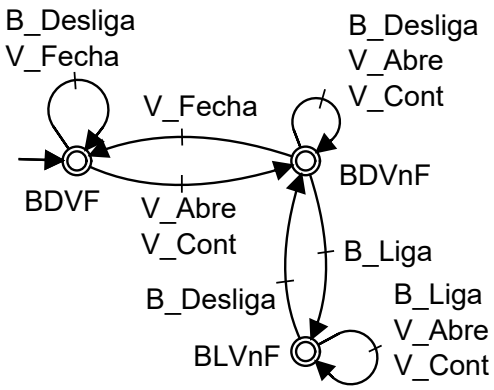
A especificação E_M (Figura 31) define como são os modos de operação do sistema e as alterações de nível esperadas em cada modo. No estado Fin o sistema está em processo de finalização, ou estado inicial, e define o procedimento de parada onde é permitido ocorrer o *underflow*. O estado Ini é atingido após o comando $Start$ proveniente da chave seletora, define o procedimento de inicialização, onde é permitido

Figura 29 – Especificação de ação reativa na bomba E_{AB} (a) e na válvula E_{AV} (b).



Fonte: Elaborado pelo autor.

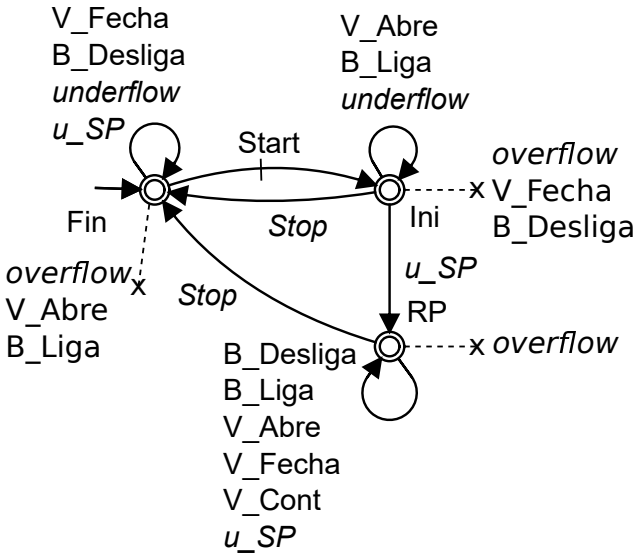
Figura 30 – E_{IBV}: Especificação de intertravamento entre bomba e válvula.



Fonte: Elaborado pelo autor.

underflow. Nesse estado a bomba liga e a válvula abre. O procedimento de inicialização é concluído quando o nível atinge o intervalo próximo ao *set point*, representado pelo evento u_SP. O estado RP define o modo de regime permanente de controle de nível. Nesse estado evita-se a ocorrência de *underflow* e *overflow*, e todos os comandos na bomba e na válvula são permitidos. Essa especificação impõe que o sistema deve sair do seu modo de regime permanente ou modo de inicialização quando houver o comando $Stop$. Em todos os modos de operação deseja-se evitar *overflow*.

Figura 31 – E_M: Especificação de modos de operação.



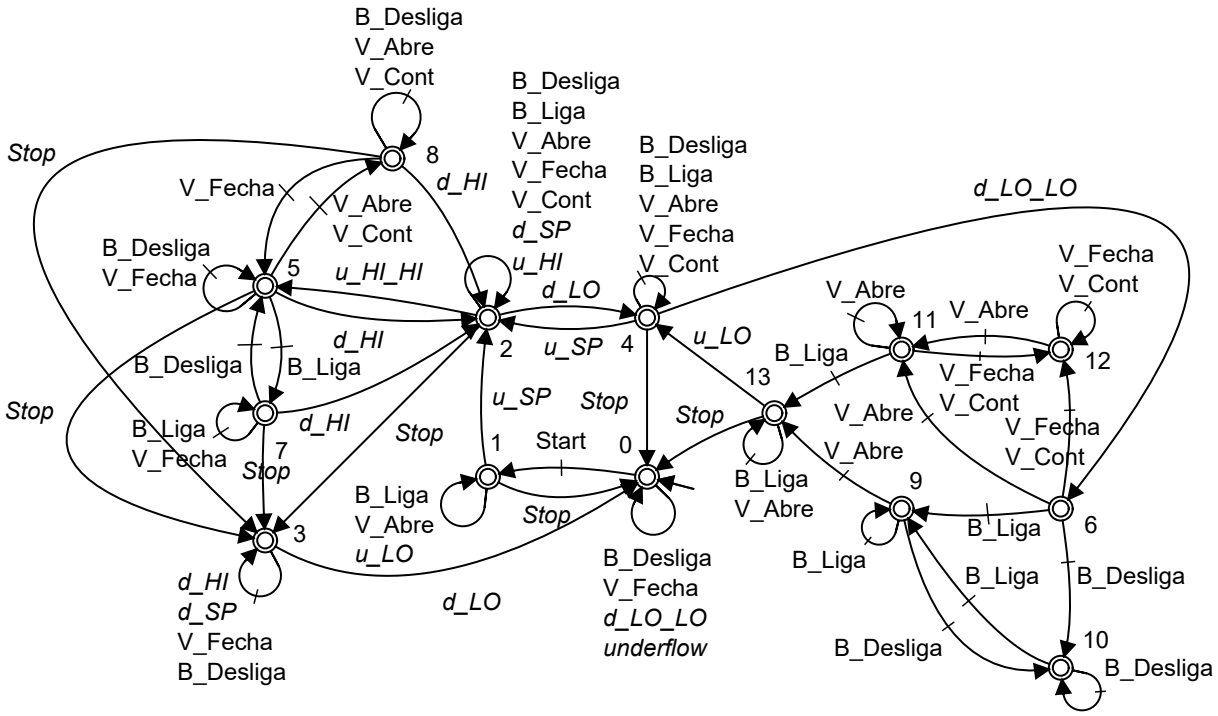
Fonte: Elaborado pelo autor.

Síntese dos Supervisores

Para realizar a síntese dos supervisores, a planta é considerada como a composição dos sete submodelos **G** = $\mathbf{G_{Níveis}}$ || $\mathbf{G_{Chave}}$ || $\mathbf{G_{Bomba}}$ || $\mathbf{G_{PB}}$ || $\mathbf{G_{Válvula}}$ || $\mathbf{G_{PV}}$ || $\mathbf{G_{Vazão}}$, o que resulta em um autômato de 240 estados sem bloqueio. Para a síntese dos supervisores é utilizada a abordagem modular, onde para cada especificação é obtido um supervisor não bloqueante e não bloqueante, por meio da máxima linguagem controlável. As especificações E_{AV}, E_{AB} e E_{IBV} são verificadas como controláveis e não bloqueantes em relação à planta **G**, portanto podem ser usadas diretamente como os supervisores $\mathcal{S}_{\text{AVR}}$, $\mathcal{S}_{\text{ABR}}$, $\mathcal{S}_{\text{IBVR}}$. As ações de desabilitação desses supervisores são, em cada estado, os eventos do alfabeto do modelo que não estão definidos no estado. Em relação à especificação dos modos de operação, é projetado o supervisor $\mathcal{S}_{\text{M}}$, por meio da máxima linguagem controlável, resultando em um modelo com 167 estados. Utilizando o algoritmo de Su e Wonham (2004) esse modelo é reduzido para um supervisor com 14 estados, denominado de $\mathcal{S}_{\text{MR}}$, ilustrado na Figura 32. Os eventos desabilitados em cada estado são aqueles eventos do alfabeto que não estão definidos no estado.

Ao analisar o sistema global, é possível observar que os supervisores modulares são conflitantes, ou seja, o sistema em malha fechada apresenta bloqueio. Nesse caso, a estratégia utilizada é projetar um coordenador que desabilita os eventos do sistema em malha fechada que levam a alguma situação de bloqueio. O coordenador é considerado como um supervisor que deve agir sobre o sistema em malha fechada, projetado sobre a especificação de ausência de bloqueio (WONG; WONHAM, 1998; QUEIROZ; CURY, 2005). Dessa forma, o sistema em malha fechada é tomado como uma planta

Figura 32 – $\mathcal{S}_{\text{MR}}$: Supervisor de modos de operação reduzido.

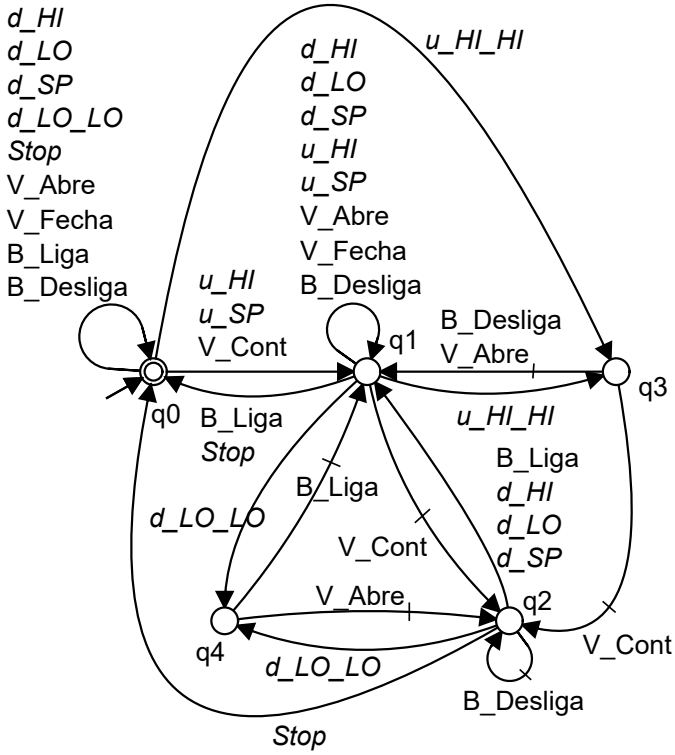


Fonte: Elaborado pelo autor.

$\mathbf{G_{Conf}} = \boldsymbol{G||S_{AVR}||S_{ABR}||S_{IBVR}||S_{MR}}$, com 142 estados. O coordenador $\mathcal{S}_{\text{Coord}}$ é sintetizado, por meio da máxima linguagem controlável, como um supervisor de 134 estados. Utilizando o argoritmo de Su e Wonham (2004), esse supervisor é reduzido para um modelo com cinco estados, denominado de $\mathcal{S}_{CoordR}$, ilustado na Figura 33. Suas ações de desabilitação, em cada estado, são os eventos do alfabeto que não estão definidos no estado.

Resumidamente constata-se que, para o processo industrial apresentado, foram obtidos quatro supervisores modulares, mais um coordenador para resolução de conflito. Os supervisores modulares reduzidos apresentam um número relativamente pequeno de estados, comparando com seus tamanhos originais. Esse fator facilita a implementação dos modelos na linguagem do controlador lógico programável. A título de comparação, para esse processo industrial, utilizando as mesmas especificações, o supervisor monolítico apresenta 134 estados, enquanto que o supervisor monolítico reduzido, apenas 38. Analisando esse supervisor, observa-se que sua implementação é viável, apesar de que é preferível a implementação dos supervisores modulares devido às vantagens trazidas pela modularidade. Na Tabela 3 constam o número de estados dos supervisores, onde K_x = **G**$||E_x$, $\mathcal{S}_x = SupC(E_x$,**G**), e $\mathcal{S}_{xR}$ é o supervisor $\mathcal{S}_x$ reduzido.

Figura 33 – $\mathcal{S}_{CoordR}$: Coordenador reduzido de resolução de conflito.



Fonte: Elaborado pelo autor.

Tabela 3 – Números de estados dos modelos dos supervisores

x	E_x	K_x	S_x	S_{xR}
AV	2	260	260	2
AB	2	258	258	2
IBV	3	200	200	3
M	3	199	167	14

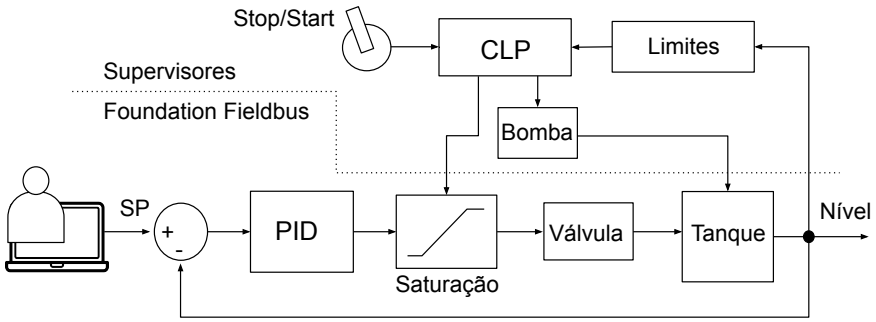
Fonte: Elaborado pelo autor.

3.3 IMPLEMENTAÇÃO

O sistema de controle projetado para o processo industrial em questão foi implementado de acordo com a arquitetura apresentada na Figura 34. A implementação dos supervisores modulares, com suas principais funções programadas diretamente no CLP, é independente do controle PID, implementado nos dispositivos da rede Foundation Fieldbus (FF). O operador pode interagir com o sistema de controle por meio da chave seletora, selecionando os comandos de inicialização (*Start*) e finalização (*Stop*) do processo, e por meio de uma interface IHM, selecionando os valores de *set point* (SP). Os supervisores, implementados no CLP, observam as transições de nível, bem como os comandos da chave seletora, e atuam no acionamento da bomba e na

saturação da válvula, somente quando necessário, de acordo com as especificações. O CLP gera os sinais das transições discretas de nível, no modelo $\mathbf{G_{Níveis}}$, comparando o valor do transdutor de nível com os limites críticos dos intervalos de operação dessa variável. Esses intervalos são definidos como: HI_HI_Lim, 80%; HI_Lim, 70%; LO_Lim, 30%; LO_LO_Lim, 20%; *overflow*, 95% e *underflow*, 5%. Uma histerese de 1% foi considerada em cada um desses limites. O valor de SP pode variar em toda extensão do tanque, mesmo fora desses limites, o que pode ser considerado como uma situação que pode forçar a atuação dos supervisores.

Figura 34 – Arquitetura de implementação dos supervisores e controle PID.

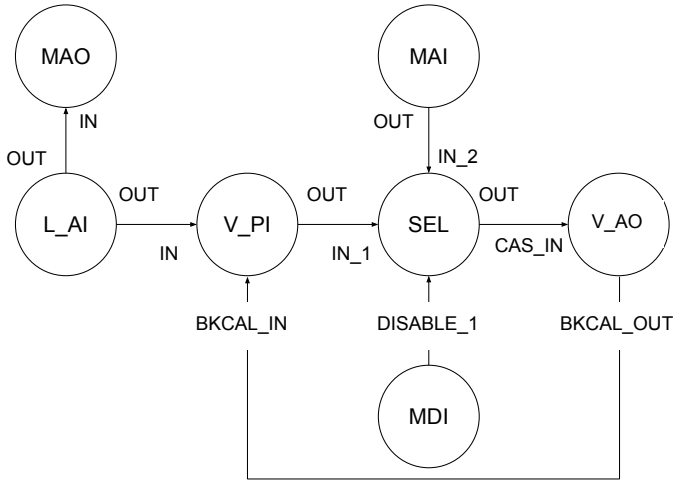


Fonte: Elaborado pelo autor.

A estratégia de controle é implementada de forma distribuída nos diferentes instrumentos inteligentes da rede FF, de acordo com a estratégia apresentada na Figura 35. A válvula com posicionador inteligente e o transdutor de nível são instrumentos da rede FF, onde são implementados blocos com funções da malha de controle. Para a troca de informações entre o CLP e a rede FF é implementado um dispositivo de interface fieldbus, onde são configurados os blocos MAO, MAI, MDI. O bloco MAO envia sinais analógicos para o CLP, ao passo que os blocos MAI e MDI recebem do CLP sinais analógicos e digitais respectivamente. O bloco L_AI é configurado no transdutor de nível, sua função é disponibilizar os valores da variável de nível para o controlador PID (V_PI) e para os supervisores implementados no CLP, por meio do bloco MAO. Na válvula de controle é instalado o bloco do controlador PID (V_PI), cuja função configurada é de controle proporcional integral (PI) e o bloco V_AO, que tem como função disponibilizar sinais analógicos correspondentes à abertura da válvula. O bloco SEL é configurado na interface fieldbus e funciona como um multiplexador. Recebe os sinais analógicos do controlador PID e do bloco MAI, que corresponde aos valores definidos pelo controle supervisório. Recebe também dos supervisores modulares o sinal digital do bloco MDI, que serve como entrada de seleção para o multiplexador, definindo, dessa forma, o valor que deve ser escolhido para a abertura da válvula.

Os modelos construídos são programados em CLP, utilizando a linguagem de programação Ladder, de acordo com Vieira *et al.* (2017), que define camadas de imple-

Figura 35 – Estratégia de controle na rede Foundation Fieldbus.



Fonte: Elaborado pelo autor.

mentação de código. Os supervisores são implementados como máquinas de estado concorrentes, cujas desabilitações são mapeadas nos estados correspondentes. A planta **G** também é implementada como máquinas de estado concorrentes, referentes aos submodelos do processo industrial apresentados anteriormente, com o objetivo de selecionar os eventos habilitados pelos supervisores para execução. A fim de traduzir as entradas e saídas do CLP em eventos abstratos utilizados pelos supervisores, são implementadas sequências operacionais.

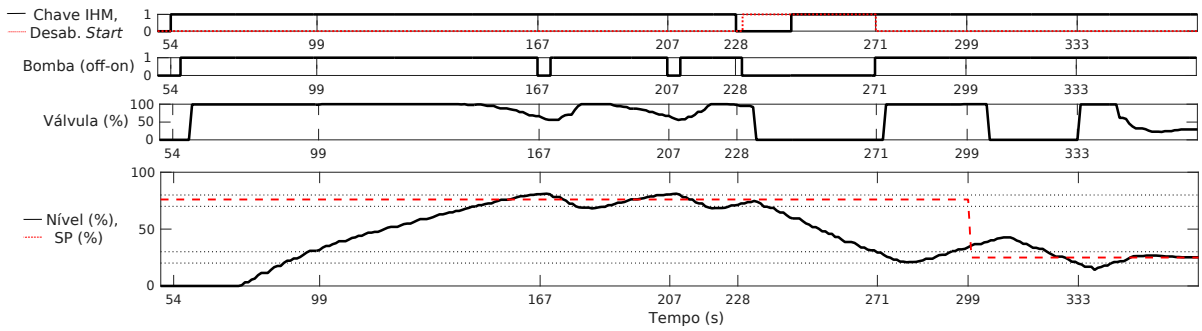
3.4 RESULTADOS OBTIDOS

A partir de testes realizados, a operação da planta piloto sob a atuação dos supervisores modulares e controle PID mostrou-se segura. Enquanto o controle de nível do processo contínuo ocorre normalmente por meio do controlador PID, o controle supervisório reage, de acordo com as especificações, aos comandos da chave seletora do painel IHM e às mudanças nos limites do nível de líquido no tanque. De acordo com a situação, os supervisores selecionam valores seguros para a válvula de controle e para a bomba, de forma a manter a planta em uma região segura de operação. Para fins de demonstração da operação do controle supervisório, o controlador PID foi ajustado com um sobresinal significativo e o valor de *set point* foi selecionado para próximo do limite HI_HI_Lim. Com essas configurações foram realizadas algumas operações com a chave seletora e alterações no *set point*, atingindo valores de interesse da variável de nível para visualizar a atuação dos supervisores.

A Figura 36 apresenta os resultados experimentais com sinais obtidos da planta, onde observa-se, de cima para baixo: evolução do comando da chave seletora, em preto, desabilitação do sinal de *Start* (*DStart*), em vermelho pontilhado; sinal discreto

de atuação na bomba; evolução da abertura da válvula; evolução do nível de líquido no tanque, em preto, e do valor de *set point*, em vermelho tracejado. No estado inicial a bomba encontra-se desligada e a válvula totalmente fechada, com o tanque vazio, ou seja, nível em 0%. Em 54s a chave seletora no painel IHM é acionada e sua posição alterada de *Stop* para *Start*, o que implica no começo do procedimento de inicialização. Nesse estado, a bomba é ligada e a válvula totalmente aberta, até que o nível atinja o intervalo de atuação intermediário, indicado pelo evento *u_SP*, nível em 31%, em 99s. Nesse intervalo o supervisor $\mathcal{S}_{\text{MR}}$ entra em modo de controle PID, onde a bomba permanece ligada e a válvula pode variar livremente para regular o nível em torno do *set point*. A ação reativa dos supervisores é garantida pela atuação de $\mathcal{S}_{\text{AVR}}$ e $\mathcal{S}_{\text{ABR}}$, que impedem comandos nos atuadores até que um evento na planta, ou chave seletora, seja observado. Como resultado do sobressinal gerado pelas configurações do controlador PID, nos instantes 167s e 207s o nível excede o valor de 81%, sinalizado pelo evento *u_HI_HI*. Nestas duas situações, os supervisores $\mathcal{S}_{\text{IBVR}}$ e $\mathcal{S}_{\text{CoordR}}$ agem conjuntamente para que a bomba seja desligada, impedindo o transbordamento do tanque, até que o nível retorne para intervalo *HI_Lim*.

Figura 36 – Gráfico com resultados experimentais. De cima para baixo: evolução da chave seletora no painel IHM e desabilitação da ação de *Start*, evolução da bomba, válvula de controle, nível e SP.



Fonte: Elaborado pelo autor.

Em 228s a chave seletora é alterada para a posição *Stop*, ativando o procedimento de finalização, o que faz com que a bomba seja desligada, a válvula seja fechada e seja desabilitada uma nova ação de *Start* (*DStart*). O procedimento de finalização pode continuar até que o tanque seja totalmente esvaziado, porém *DStart* permanece ativado até o instante 271s. Durante esse intervalo do procedimento de finalização, não é considerado seguro habilitar um novo procedimento de inicialização, o que é permitido somente quando o nível diminui de 29%, sinalizado pelo evento *d_LO*. Para a realização do experimento, logo após 228s a chave seletora é alterada novamente para *Start*, mas seu efeito não é habilitado nesse momento, devido à atuação dos supervisores. Ressalta-se que essa restrição não é definida de forma direta nas espe-

cificações, mas é resultado da síntese do supervisor $\mathcal{S}_{\text{MR}}$, que prevê algumas ações de controle para garantir controlabilidade e ausência de bloqueio. Em 229s, o valor de *set point* é ajustado para 25%, o que muda a ação do controlador PID alterando a abertura da válvula. Como consequência do ajuste desse controlador, no instante 333s ocorre uma nova situação de sobressinal, o que leva, nesse caso, o nível para uma região de alerta, próximo de *underflow*, abaixo de 19% (*d_LO_LO*). Para contornar essa situação, $\mathcal{S}_{\text{IBVR}}$ e $\mathcal{S}_{\text{CoordR}}$ agem abrindo totalmente a válvula, fazendo com que o nível volte para uma região segura. Por fim, os supervisores modulares retornam para o modo de controle PID, mantendo o nível próximo do valor de *set point*.

3.5 CONCLUSÃO

Neste capítulo foi apresentada uma metodologia para aplicação da teoria de controle supervisório em sistemas contínuos, que utiliza o conceito da preempção da dinâmica contínua por meio de atuadores discretos. Com essa aplicação, o controle supervisório, por meio da síntese formal, garante um comportamento discreto não bloqueante e seguro em um processo industrial com controle PID distribuído em rede Foundation Fieldbus. Os modelos discretos propostos permitem abordar um típico processo contínuo como um problema de controle supervisório. Resultados experimentais demonstram a ação antecipatória, reativa e minimamente restritiva dos supervisores modulares. Por meio da síntese dos supervisores permite-se projetar procedimentos seguros de inicialização e finalização, além da supervisão em modo de regime permanente.

4 MODELAGEM HIERÁRQUICA POR ABSTRAÇÕES SUCESSIVAS

No capítulo anterior, foi discutido como a natureza dos processos industriais abordados nesta tese possibilita hipóteses de modelagem, empregando a preempção dos eventos do processo por meio dos atuadores, que acabam por evitar a complexidade gerada pelos métodos formais dos sistemas híbridos. No entanto, ao abordar processos industriais comandados por circuitos de componentes, o projeto do controle supervisório pode se tornar bastante complexo devido à explosão de estados gerada na composição dos modelos. Nesses casos, além da complexidade computacional envolvida, existe ainda a complexidade de modelagem da planta e das especificações. Tais processos industriais podem ser formados por um certo número de equipamentos como bombas centrífugas e por diversos tipos de válvulas industriais atuando conjuntamente na forma de um circuito. Tipicamente essas estruturas são construídas para proporcionar maior segurança aos sistemas ao permitir redundância no acionamento dos atuadores no caso de falhas.

Como circuitos de componentes são estruturas bastante interconectadas devido ao seu acoplamento, as abordagens da teoria de controle supervisório que exploram a modularidade horizontal, como o controle modular, ou o controle modular local, não trazem vantagens na redução da complexidade envolvida. Com esses métodos, os modelos resultantes acabam por apresentar grande número de estados, sendo comparáveis ao sistema global, como será visto nos exemplos abaixo. Nestas circunstâncias, considera-se que o desenvolvimento de uma abordagem multinível seja eficiente no sentido de proporcionar a redução da complexidade de modelagem em uma direção vertical ao possibilitar o projeto de supervisores para diferentes níveis de abstração.

Neste capítulo será proposta uma estratégia de modelagem por abstrações sucessivas de circuitos de válvulas empregados em processos industriais, explorando métodos de controle supervisório hierárquico. Com a estratégia proposta, pretende-se obter o controle supervisório com menor complexidade de modelagem e síntese para esse tipo de sistema em comparação com os métodos existentes. Nesta proposta, lança-se mão de abstrações em níveis hierárquicos a fim de simplificar a síntese do controle supervisório por meio da obtenção de um modelo de válvula equivalente através de associações sucessivas em série ou em paralelo. Nesta abordagem são estudadas válvulas de bloqueio e válvulas de controle sujeitas a falhas de travamento, considerando-se as falhas como eventos observáveis. Com o método proposto, o modelo abstrato de válvula equivalente é utilizado como elemento que compõe o processo industrial, o que permite calcular seu controle supervisório. Esta estratégia segue a mesma ideia do cálculo de um resistor equivalente em um circuito de resistores, em que, com associações sucessivas em série e paralelo, encontra-se um resistor equivalente que representa a estrutura do circuito (NILSSON; RIEDEL, 2015).

Para efeito de exemplificar a metodologia proposta, nesta tese serão abordados somente circuitos com válvulas industriais. No exemplo da seção 2.4, foi utilizado o modelo de uma válvula de bloqueio, sem a possibilidade de falhas. Nesse modelo foi utilizado o evento "mantém" (VM) como comando para a válvula permanecer no mesmo estado. No capítulo 3 foi utilizado o modelo de uma válvula de controle, também sem a possibilidade de falhas. No modelo, como uma tentativa de simplificação, não foi utilizado o evento "mantém" como comando para a válvula permanecer no mesmo estado, mas sim os próprios comandos de acionamento da válvula (V_Fecha, V_Abre, V_Cont). Para abordar o método de abstrações sucessivas, deste capítulo em diante, nos modelos de válvulas serão empregados o evento "mantém", como comando para a válvula permanecer no mesmo estado, o que traz mais possibilidades para o projeto das especificações. Além disso, serão consideradas válvulas de bloqueio e de controle, ambas com possibilidade de falha de travamento.

Em relação à modelagem de circuitos de válvulas e aplicações em processos industriais, destacam-se os trabalhos de Yamalidou e Kantor (1991), que desenvolve a modelagem e controle de processos industriais por meio de redes de Petri, e Yeh e Chang (2012) que desenvolve uma proposta para supervisores de resposta a emergências em processos em batelada, por meio da TCS. Entretanto, esses trabalhos não lidam com a complexidade que advém de sistemas com múltiplas válvulas. Nessa última proposta, os métodos lançam mão da modularidade horizontal, por meio do controle modular. Mas, ainda assim, é necessário considerar todas as válvulas de uma malha ao projetarem-se as especificações, devido a sua interconexão.

4.1 MODELAGEM DE CIRCUITOS DE COMPONENTES SEM A UTILIZAÇÃO DE NÍVEIS HIERÁRQUICOS

Nesta seção serão apresentados exemplos de circuitos de componentes empregando o controle modular de SEDs, com o objetivo de ilustrar o problema da complexidade. O primeiro exemplo consiste em um processo industrial controlado por somente uma válvula de bloqueio com possibilidade de falha. O segundo exemplo traz uma estrutura com duas válvulas e outra com três válvulas, ambas com possibilidade de falha. São apresentados alguns modelos ilustrativos para fins de comparação.

Embora o método proposto possa ser aplicado para circuitos de componentes de forma geral, incluindo bombas industriais por exemplo, nesta tese os exemplos utilizados serão voltados a válvulas industriais. As válvulas são dispositivos mecânicos projetados para direcionar, misturar, bloquear ou regular fluidos em um processo. Podem ser classificadas basicamente quanto a sua função, como de bloqueio e de controle, e quanto ao seu tipo de deslocamento, podendo ser lineares ou rotativas (SKOUSEN, 2011). Nesta tese serão abordadas válvulas de bloqueio e de controle, conforme simbologia apresentada na Figura 37. As válvulas de bloqueio, também co-

nhecidas como válvulas *on-off* têm como função impedir, liberar, ou alterar a direção do fluxo em uma tubulação. Sua abertura pode ser considerada como totalmente aberta ou totalmente fechada. Devido a suas características funcionais, podem ser utilizadas em tubulações como válvulas de manobra, quando se altera a direção da passagem de fluxo em um sistema mais complexo, ou quando se bloqueia ou libera o fluxo em um duto. As válvulas de controle, também conhecidas como válvulas reguladoras, são utilizadas como atuadores em malhas de controle com o objetivo de regular a variável de processo (PV) em torno de um *set point*. Esses dois tipos de válvulas podem atuar associadamente em um circuito, combinando as funções de bloqueio e de controle conforme as necessidades do processo.

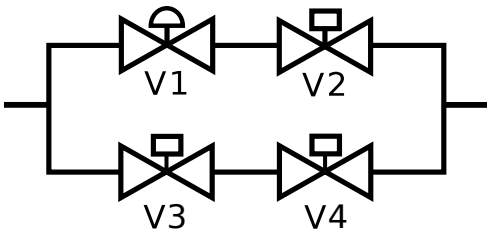
Figura 37 – Simbologia em Diagramas ISA: (a) válvula de bloqueio, (b) válvula de controle.

(a) (b)

Fonte: Elaborado pelo autor.

Em muitos processos industriais é comum encontrar mais de uma válvula atuando em conjunto, como em um circuitos de válvulas (Figura 38), cujo objetivo é possibilitar redundância no acionamento dos atuadores no caso de travamentos. Os tipos de configurações de tubulações mais comuns são válvulas em série em um mesmo duto, ou em paralelo em diferentes dutos.

Figura 38 – Circuito de válvulas representado em um diagrama.



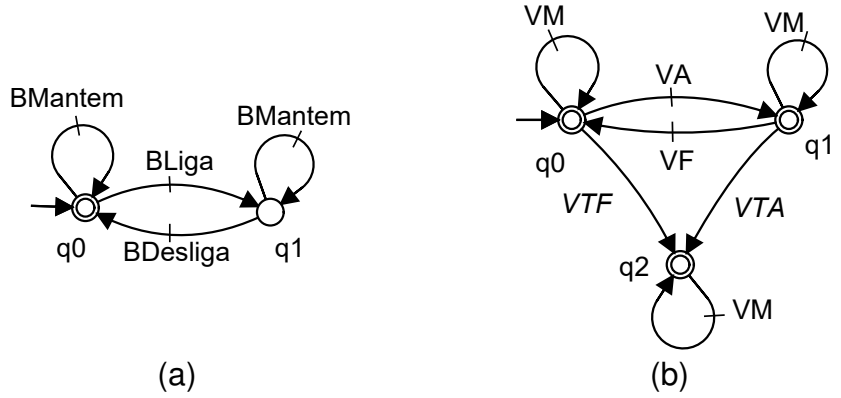
Fonte: Elaborado pelo autor.

Exemplo 4.1.1. ***Processo industrial comandado por uma válvula de bloqueio com falha.***

O processo industrial deste exemplo segue a mesma estrutura básica utilizada no Capítulo 3, mas utilizando agora uma válvula de bloqueio com possibilidade de falha de travamento. A válvula pode travar tanto aberta, quanto fechada. A discretização dos níveis no tanque, modelo G_{Niveis}*, segue o mesmo padrão da Figura 24, com os seguintes limiares de mudança de nível: LO_LO_Lim, LO_Lim, SP, HI_Lim, HI_HI_Lim, underflow e overflow. O modelo da chave seletora,* G_{Chave}*, permanece o mesmo apresentado na Figura 25, com o evento start controlável e stop não controlável.*

O modelo da bomba utiliza o evento $BMantem$ como um comando para permanecer no mesmo estado (Figura 39 - a). O modelo da válvula de bloqueio é apresentada na Figura 39 (b), em que VM indica um comando para permanecer no mesmo estado. Os eventos de travamento na válvula são VTF, válvula trava fechada e VTA, trava aberta. Ambos eventos de travamento são não controláveis. Depois da ocorrência de um evento de travamento o único comando que pode ocorrer na válvula é VM.

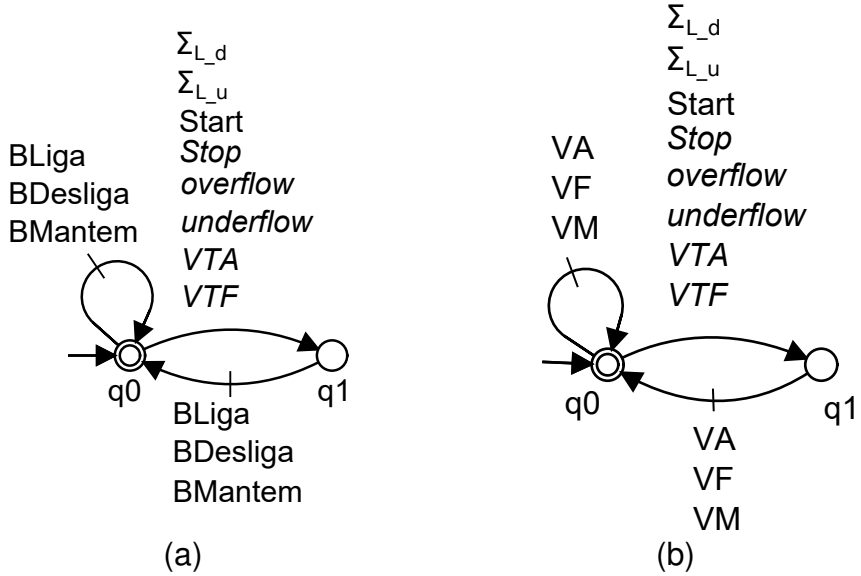
Figura 39 – (a) **G_{Bomba}**: Modelo de bomba centrífuga com evento $BMantem$ e (b) **$G_{Valvula}$**: modelo de válvula de bloqueio com possibilidade de falha.



Fonte: Elaborado pelo autor.

*Como os eventos de mudança de nível são não controláveis, para evitar sua ocorrência empregam-se os modelos de preempção por eventos da bomba **GPB** (Figura 40 - a) e da válvula **GPV** (Figura 40 - b). Utilizam-se os alfabetos $\Sigma_{L\_d} = \{d\_HI, d\_SP, d\_LO, d\_LO\_LO\}$ e $\Sigma_{L\_u} = \{u\_LO, u\_SP, u\_HI, u\_HI\_HI\}$ com os eventos de mudança de nível, como no Capítulo 3. São sincronizados também Start, Stop, overflow, underflow, VTA e VTF, como hipótese de modelagem.*

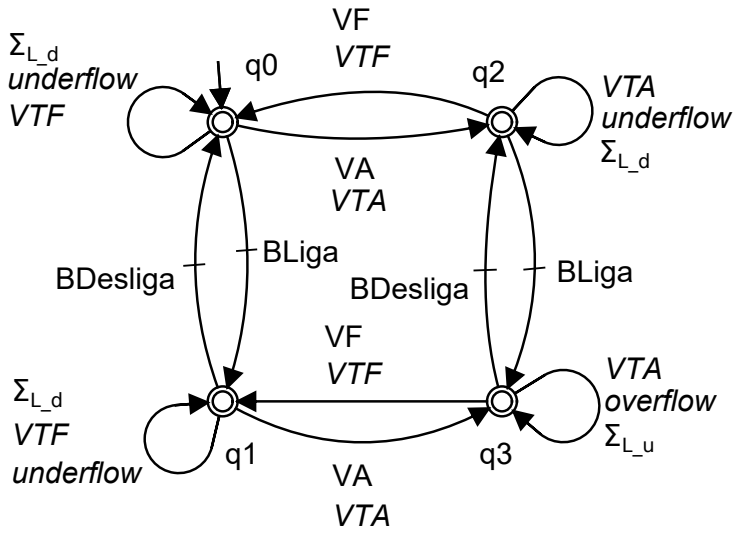
Figura 40 – Modelos de preempção da bomba: **G_{PB}** (a) e da válvula: **G_{PV}** (b).



Fonte: Elaborado pelo autor.

Na Figura 41 apresenta-se o modelo de vazão no tanque, de acordo com o estado dos atuadores. No estado inicial, $q0$, a bomba encontra-se desligada e a válvula fechada, então o nível somente pode descer. Já no estado $q3$, por exemplo, a bomba está ligada e a válvula aberta, então o nível somente pode subir.

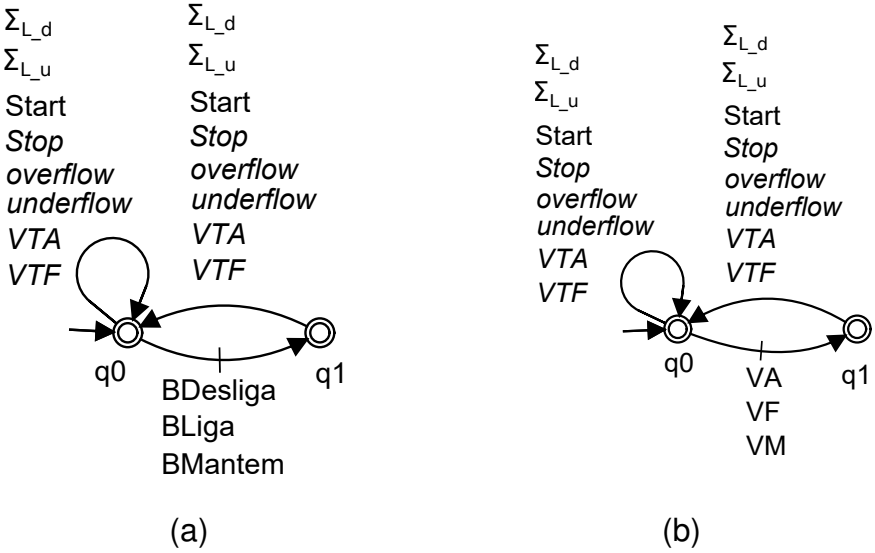
Figura 41 – $\mathbf{G_{Vazao}}$: Modelo de vazão no tanque



Fonte: Elaborado pelo autor.

Na Figura 42 (a) e (b) são apresentadas respectivamente as especificações de ação reativa da bomba e da válvula. Sua função é a mesma das especificações apresentadas no capítulo anterior, que impõem a restrição de que o atuador somente aja em resposta a alguma alteração da planta, ou de travamento da válvula.

Figura 42 – (a) E_{AB}: Especificação de ação reativa da bomba (b) E_{AV}: Especificação de ação reativa da válvula.

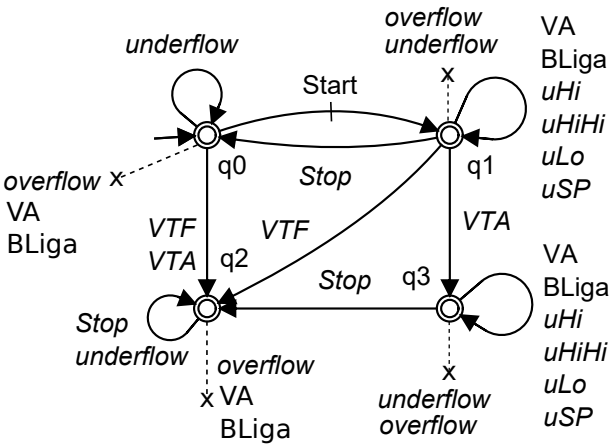


Fonte: Elaborado pelo autor.

A especificação dos modos de operação é apresentada na Figura 43. No estado inicial e de finalização, $q0$, é permitido underflow. Depois do comando Start o processo

entra em modo de inicialização e de regime permanente $q1$, em que não é permitido underflow e overflow. Desse estado, se a válvula travar aberta atinge-se o estado $q3$, em que o controle de nível é feito utilizando-se unicamente a bomba e também não é permitido underflow e overflow. O estado $q2$ indica a finalização do processo depois da ocorrência de travamento na válvula. Em nenhum estado é permitida a ocorrência de overflow.

Figura 43 – (a) E_M: Especificação de modos de operação.



Fonte: Elaborado pelo autor.

Para a síntese do supervisor foi utilizada a planta monolítica como $\mathbf{G = G_{Niveis}||\ G_{Chave}||\ G_{Bomba}||\ G_{Valvula}||\ G_{PB}||\ G_{PV}||\ G_{Vazao}}$, que apresenta 320 estados. Como especificação monolítica utilizou-se $E = E_{AB}||E_{AV}||E_M$, com 16 estados. A composição $Lm(G)||E$ apresenta 323 estados e o supervisor monolítico obtido apresenta 290 estados.

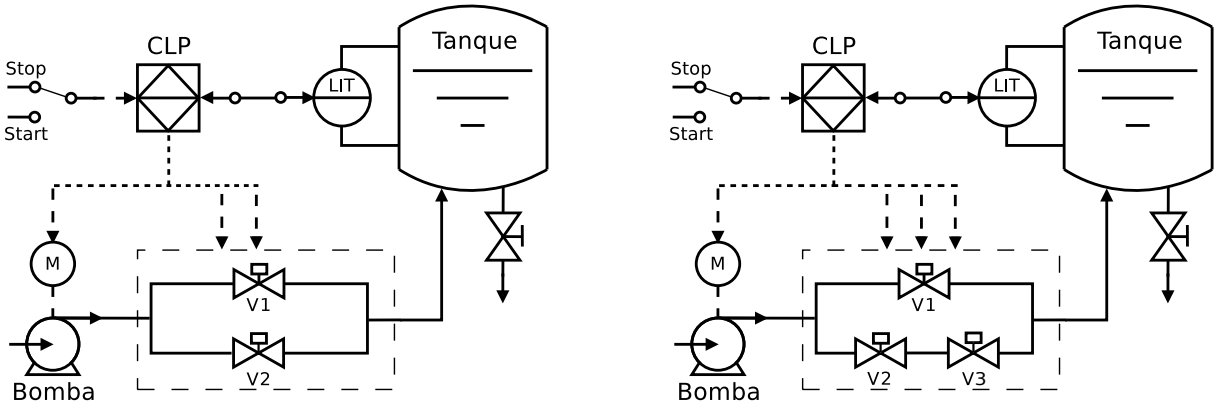
Abaixo apresenta-se um exemplo comparativo com o mesmo processo industrial, mas controlado por um circuito de duas válvulas e por outro circuito de três válvulas.

Exemplo 4.1.2. ***Comparativo do processo industrial comandado por diferentes circuitos de válvulas***

Neste exemplo, para efeito de comparação, é utilizado o mesmo processo industrial do exemplo anterior mas comandado, em primeiro lugar, por um circuito formado por duas válvulas de bloqueio em série (Figura 44 - a) e, na sequência, por três válvulas de bloqueio, sendo uma em paralelo com outras duas em série (Figura 44 - b), ambas com possibilidade de falha de travamento. Para a construção desses modelos e das especificações foram preservadas as mesmas restrições utilizadas no exemplo anterior com uma só válvula.

Para o sistema com duas válvulas em paralelo, ambas têm seu estado inicial como fechada. Com as duas válvulas fechadas, o nível tende a descer, com uma das válvulas abertas, tende a subir. Em relação ao exemplo anterior, o modelo de vazão do tanque dobra de tamanho, contendo agora oito estados. A especificação de modos de

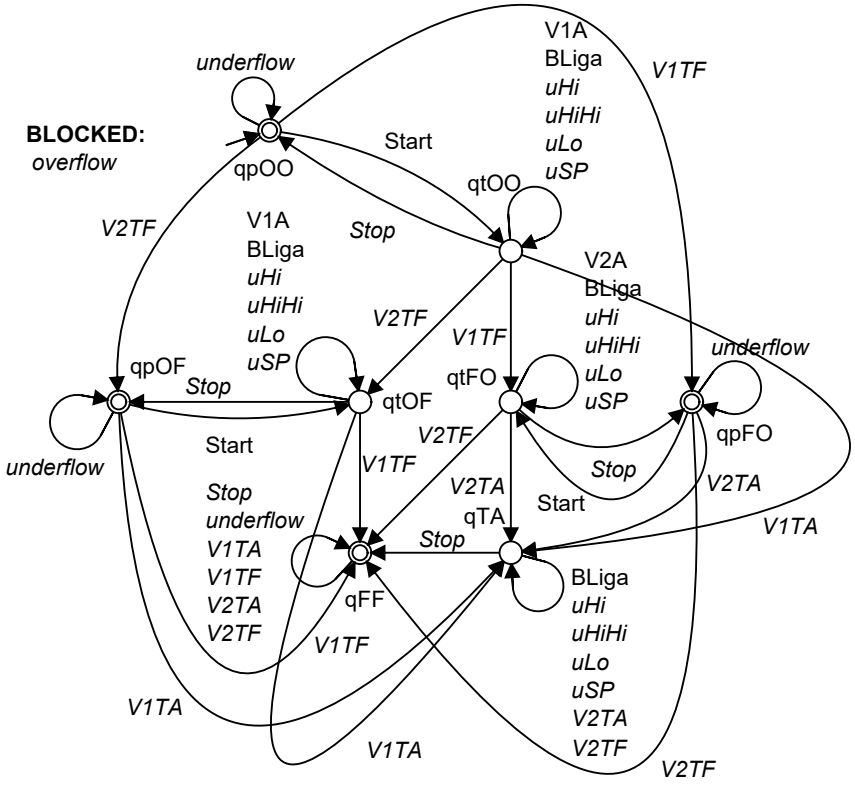
Figura 44 – Diagrama industrial de planta com duas válvulas de bloqueio em paralelo (a) e com três válvulas de bloqueio, sendo uma em paralelo com duas em série (b).



Fonte: Elaborado pelo autor.

operação contém também oito estados, conforme apresentado na Figura 45. Apesar de não ser um modelo com muitos estados, já é possível notar um aumento na sua complexidade de modelagem, comparando com o exemplo anterior. A legenda Blocked: overflow indica que em nenhum estado é permitida a ocorrência desse evento.

Figura 45 – E_M: Especificação de modos de operação para processo com duas válvulas em paralelo.

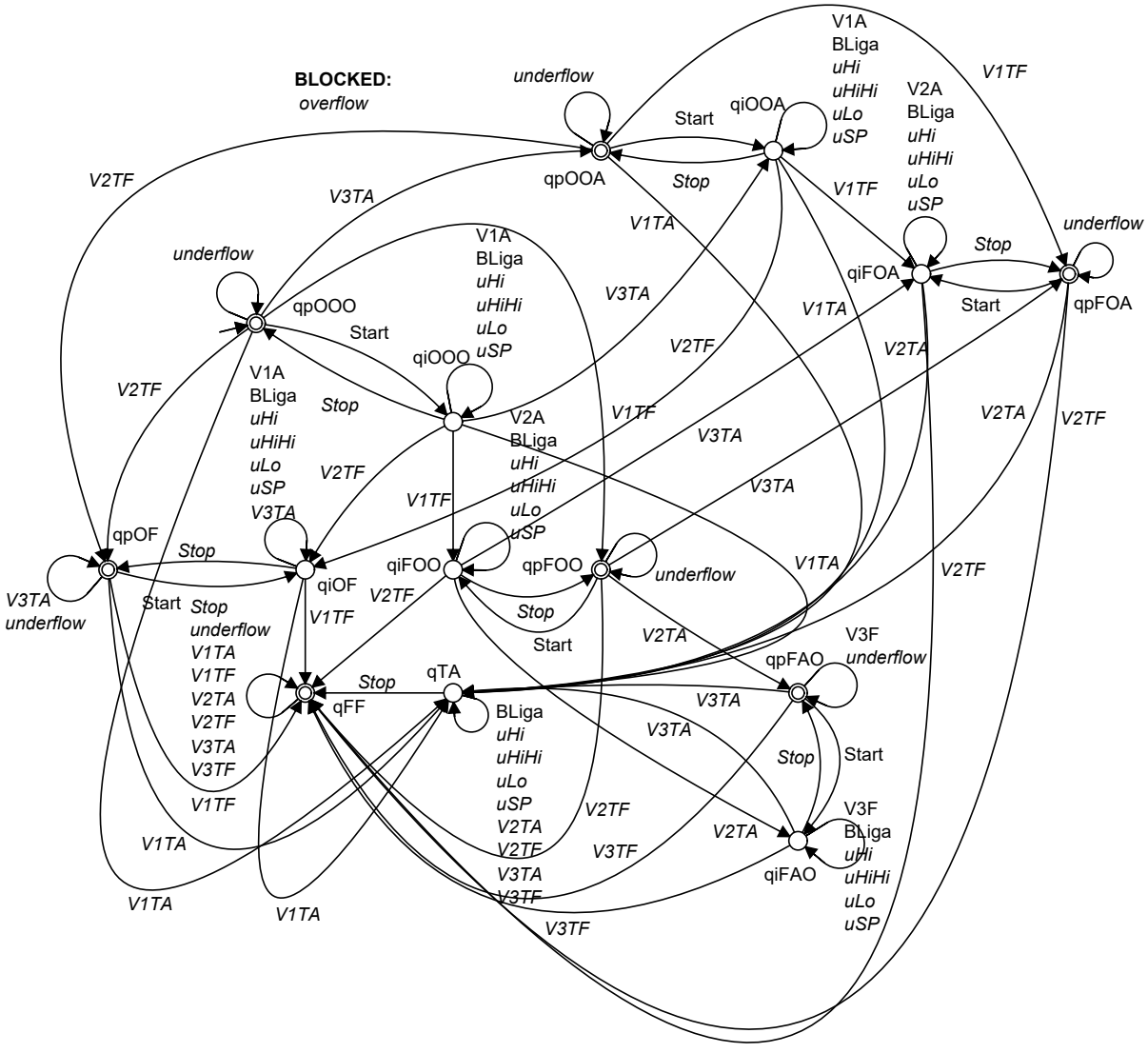


Fonte: Elaborado pelo autor.

Para a síntese do supervisor, o modelo composto da planta contém 1280 estados, a especificação 32 estados, a composição $Lm(G)||E$ contém 883 estados e o supervisor obtido contém 658 estados.

Para o sistema com três válvulas de bloqueio, sendo uma em paralelo com outras duas em série, o estado inicial de $V1$ e $V3$ é aberta, e $V2$ é fechada. De acordo com a configuração da Figura 44 (b), com a válvula $V1$ aberta o nível tende a subir. Com essa válvula fechada, mas $V2$ e $V3$ abertas, o nível também tende a subir. Com $V1$ fechada e somente uma das duas em série aberta ($V2$ ou $V3$) o nível tende a descer. O maior modelo da planta é o de vazão, que contém 16 estados e apresenta uma certa complexidade de modelagem. O modelo da especificação E_M contém 14 estados (Figura 46), com grande complexidade de modelagem e propensão a erros.

Figura 46 – E_M: Especificação de modos de operação para processo com uma válvula em paralelo com outras duas em série.



Fonte: Elaborado pelo autor.

Nesse modelo devem ser consideradas todas as possibilidades de acionamento dos atuadores, bem como as possibilidades de travamento das válvulas. Blocked: overflow indica que em nenhum estado esse evento é permitido.

Para a síntese do supervisor, o modelo composto da planta contém 5120 estados, a especificação 56 estados, a composição $Lm(G)||E$ contém 1963 estados e o supervisor obtido contém 1480 estados.

Ao analisar os exemplos acima, pode-se perceber que para o processo controlado por duas válvulas em paralelo há um aumento representativo nas dimensões dos modelos. Para o processo controlado por três válvulas, observa-se que a especificação monolítica E apresenta 56 estados e 848 transições, com grande propensão a erros de modelagem. O modelo da vazão no tanque, para o processo com três válvulas, $\mathbf{G_{Vazao}}$, de 16 estados, também cresce com o número de válvulas no circuito pela abordagem monolítica. Para o mesmo processo industrial comandado com quatro válvulas, os modelos se tornam complexos demais para serem definidos manualmente e não foram desenvolvidos. Os dados comparativos dos exemplos acima constam na Tabela 4, onde pode-se constatar o aumento considerável dos modelos, com o crescimento do circuito de componentes. Comparando com a abordagem do controle modular, não foram obtidas vantagens em relação à complexidade de síntese, devido ao forte acoplamento entre os modelos da planta.

Tabela 4 – Número de estados na síntese monolítica para diferentes circuitos.

	$\mathbf{G}$	E	$E\|\|L_m(\mathbf{G})$	$\mathbf{S}$
Circuito com 1 válvula	320	16	327	290
Circuito com 2 válvulas	1280	32	883	658
Circuito com 3 válvulas	5120	56	1963	1480

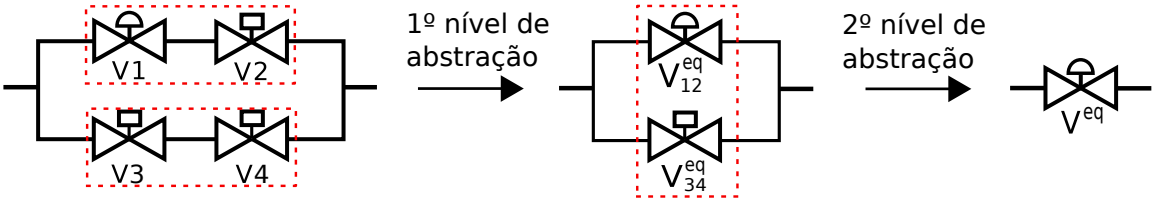
Fonte: Elaborado pelo autor.

4.2 ARQUITETURA MULTINÍVEL PARA CIRCUITOS DE COMPONENTES COM ABSTRAÇÕES SUCESSIVAS

Na seção anterior foi apresentado o problema da complexidade em um processo industrial comandado por um circuito de componentes. Para exemplificar, foi utilizado um circuito com três válvulas de bloqueio. Nesta seção, para apresentar a metodologia proposta, será utilizado o processo industrial conforme ilustrado na introdução desta tese (Figura 1) com um circuito de três válvulas de bloqueio e uma de controle. Como ideia geral propõe-se utilizar níveis hierárquicos para realizar a associação de componentes aos pares e, sucessivamente, obter um modelo equivalente para ser utilizado no comando do processo industrial. Essa estratégia está ilustrada na Figura 47, onde o duto de cima contém uma válvula de controle ($V1$) em série com uma de

bloqueio ($V2$) e no duto de baixo, duas válvulas de bloqueio em série ($V3$ e $V4$). A associação da válvula de controle com a de bloqueio resulta em um modelo abstrato de uma válvula de controle (V_{12}^{eq}). A associação das duas válvulas de bloqueio resulta em um modelo abstrato de uma válvula de bloqueio (V_{34}^{eq}). Por fim, os dois modelos abstratos são ainda associados como uma válvula de controle em paralelo com uma válvula de bloqueio o que, em um novo nível de abstração, resulta em uma válvula de controle.

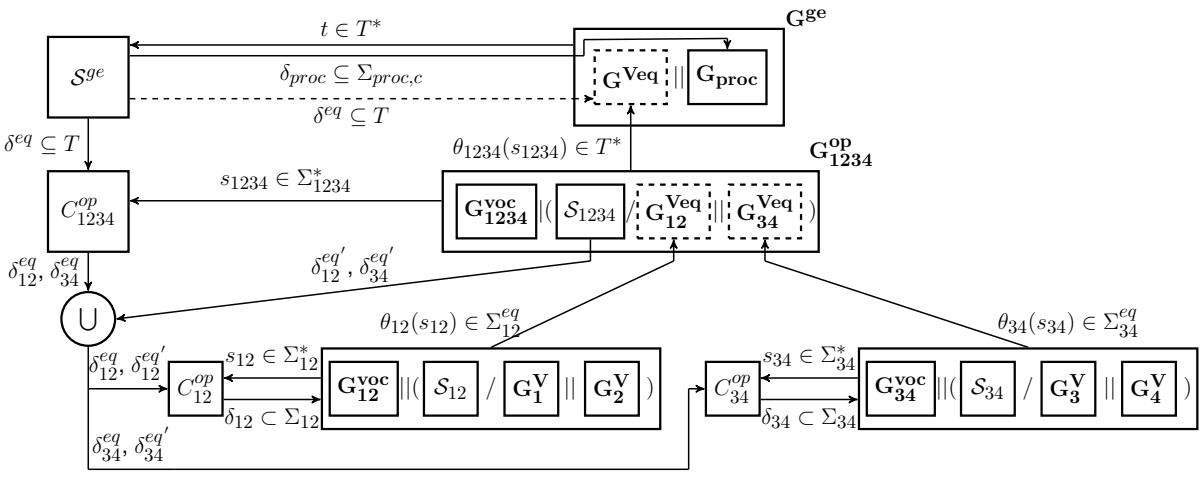
Figura 47 – Abstrações sucessivas em um circuito de componentes.



Fonte: Elaborado pelo autor.

Para formalizar a estratégia proposta é empregado o controle supervisório hierárquico de SEDs. A arquitetura multinível proposta para tratar o problema estudado é apresentada na Figura 48.

Figura 48 – Arquitetura multinível para circuito de válvulas, onde $\mathbf{G_{12}^{op}}$ e $\mathbf{G_{34}^{op}}$ são as plantas do operador associando as válvulas em série, $\mathbf{G_{1234}^{op}}$ representa a associação em paralelo, $\mathbf{G^{Veq}}$ é a abstração do circuito numa válvula equivalente e $\mathbf{G_{proc}}$ modela os demais componentes do processo industrial.



Fonte: Elaborado pelo autor.

Nessa arquitetura, os modelos $\mathbf{G_{12}^{op}}$ e $\mathbf{G_{34}^{op}}$ correspondem às associações de válvulas em série, enquanto que $\mathbf{G_{1234}^{op}}$ corresponde à associação dos modelos abstratos ($\mathbf{G_{12}^{Veq}}$ e $\mathbf{G_{34}^{Veq}}$) em paralelo. O modelo abstrato $\mathbf{G^{Veq}}$ corresponde ao modelo de válvula equivalente utilizado para comando do processo industrial representado pelo modelo $\mathbf{G_{proc}}$. A composição $\mathbf{G^{Veq}} \| \mathbf{G_{proc}}$ forma a planta do gerente $\mathbf{G^{ge}}$. Para

o controle supervisório, no nível gerencial o supervisor $\mathcal{S}^{ge}$ envia comandos reais de desabilitação para os eventos do processo, alfabeto $\Sigma_{proc,c}$, e comandos virtuais para o modelo da válvula equivalente. As desabilitações reais das válvulas somente podem ser executadas no nível operacional, por meio do mapa de desabilitações dos operadores (C_{12}^{op} e C_{34}^{op}).

No nível operacional, os modelos das plantas operacionais são descritos no formato $\mathbf{G_{12}^{op}} = \mathbf{G_{12}^{voc}}||\mathbf{S_{12}}||\mathbf{G_1^V}||\mathbf{G_2^V}$, onde: $\mathbf{G_1^V}$ e $\mathbf{G_2^V}$ são os modelos de V_1 e V_2; $\mathbf{S_{12}}$ é o modelo de um supervisor local para garantir especificações de prioridade na associação em série; e $\mathbf{G_{12}^{voc}}$ é um autômato de Moore que vocaliza determinados estados para informar os eventos relevantes ao nível hierárquico acima. Já o operador C_{12}^{op} é um mapa que traduz as desabilitações de eventos abstratos recebidas dos níveis acima em desabilitações de eventos operacionais no respectivo nível. Esse padrão é utilizado tanto para as associações do nível operacional ($\mathbf{G_{12}^{op}}$ e $\mathbf{G_{34}^{op}}$), quanto para os modelos abstratos dos níveis operacionais intermediários (no caso, $\mathbf{G_{1234}^{op}}$). Assim, cada associação é abstraída pelos eventos de vocalização em uma válvula equivalente utilizada para associação com outros níveis hierárquicos. Nesse caso, as abstrações das válvulas equivalentes em série, $\mathbf{G_{12}^{Veq}}$ e $\mathbf{G_{34}^{Veq}}$ são utilizadas em uma associação em paralelo, para gerar o modelo de uma válvula equivalente $\mathbf{G^{Veq}}$, que representa o comportamento resultante do circuito de válvulas e é utilizado como componente da planta $\mathbf{G_{proc}}$ no controle gerencial do processo industrial.

Essa estratégia de modelagem multinível, além de proporcionar a redução na complexidade computacional exigida para a síntese dos supervisores, favorece ainda a distribuição da complexidade de modelagem ao longo dos níveis hierárquicos. Com isso, observa-se que no nível gerencial a modelagem das especificações é relativamente simples, devido ao reaproveitamento dos modelos da válvula equivalente, que se assemelha ao modelo das válvulas individuais.

Para as associações de componentes aos pares, como forma de exemplificar o método proposto, nas próximas seções são desenvolvidos modelos para válvulas de controle e de bloqueio em série e em paralelo.

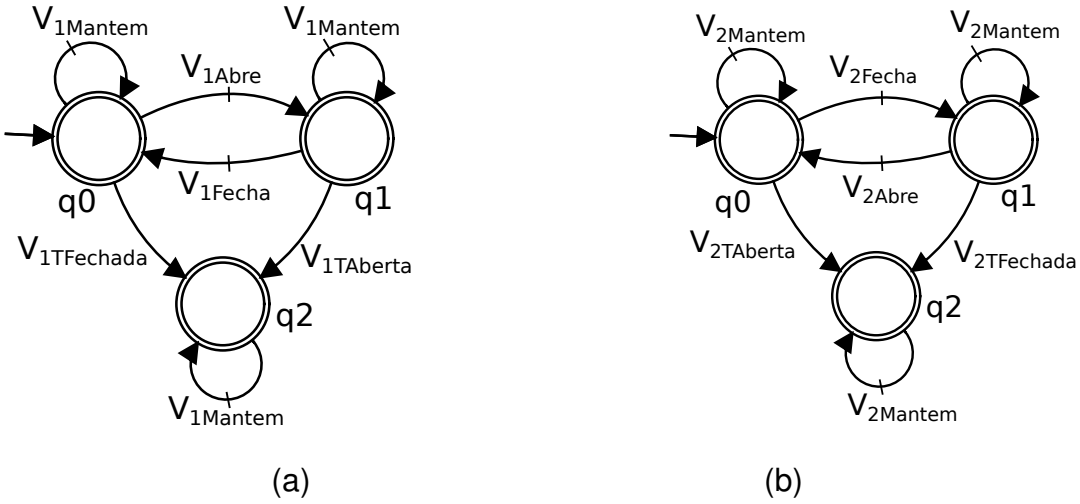
4.3 MODELAGEM PARA DUAS VÁLVULAS DE BLOQUEIO

4.3.1 Modelagem Para Válvulas em Série

O modelo proposto para representar as válvulas de bloqueio com possibilidade de falha de travamento é composto por três estados: válvula fechada, aberta e travada, conforme ilustrado na Figura 49. Nesse caso, como hipótese de modelagem, é considerado que uma válvula somente pode travar aberta se estiver na posição aberta e travar fechada se estiver na posição fechada. Nesse modelo todos os estados são considerados marcados, pois como os eventos que levam a q_2 são não controláveis,

esse estado deve ser definido como marcado para que se evite bloqueio. Sendo assim, considera-se também o estado q_1 marcado, pois essa definição não altera a análise de vivacidade e bloqueio do sistema composto. Para válvulas em série, considera-se que uma inicie na posição fechada e a outra aberta, como os modelos a seguir. Assim, o equivalente para a associação em série tem seu estado inicial como fechado, pois não há vazão no duto.

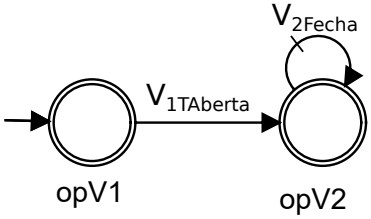
Figura 49 – Modelos para válvulas de bloqueio em série com travamento: (a) $\mathbf{G_1^V}$ com estado inicial fechada e (b) $\mathbf{G_2^V}$ com estado inicial aberta.



Fonte: Elaborado pelo autor.

Nessa abordagem, para cada associação de válvula, obtém-se um supervisor local para garantir restrições locais. Nas associações em série, a especificação de prioridade E_{12}, cujo modelo é ilustrado na Figura 50, habilita a operação da válvula 2 somente após a válvula 1 travar aberta. Como E_{12} é controlável para a planta local $\mathbf{G_1^V}||\mathbf{G_2^V}$, o supervisor local $\mathcal{S}_{12}$ com 9 estados, pode ser reduzido a R_{12} com 2 estados.

Figura 50 – E_{12}: especificação local para válvulas em série.

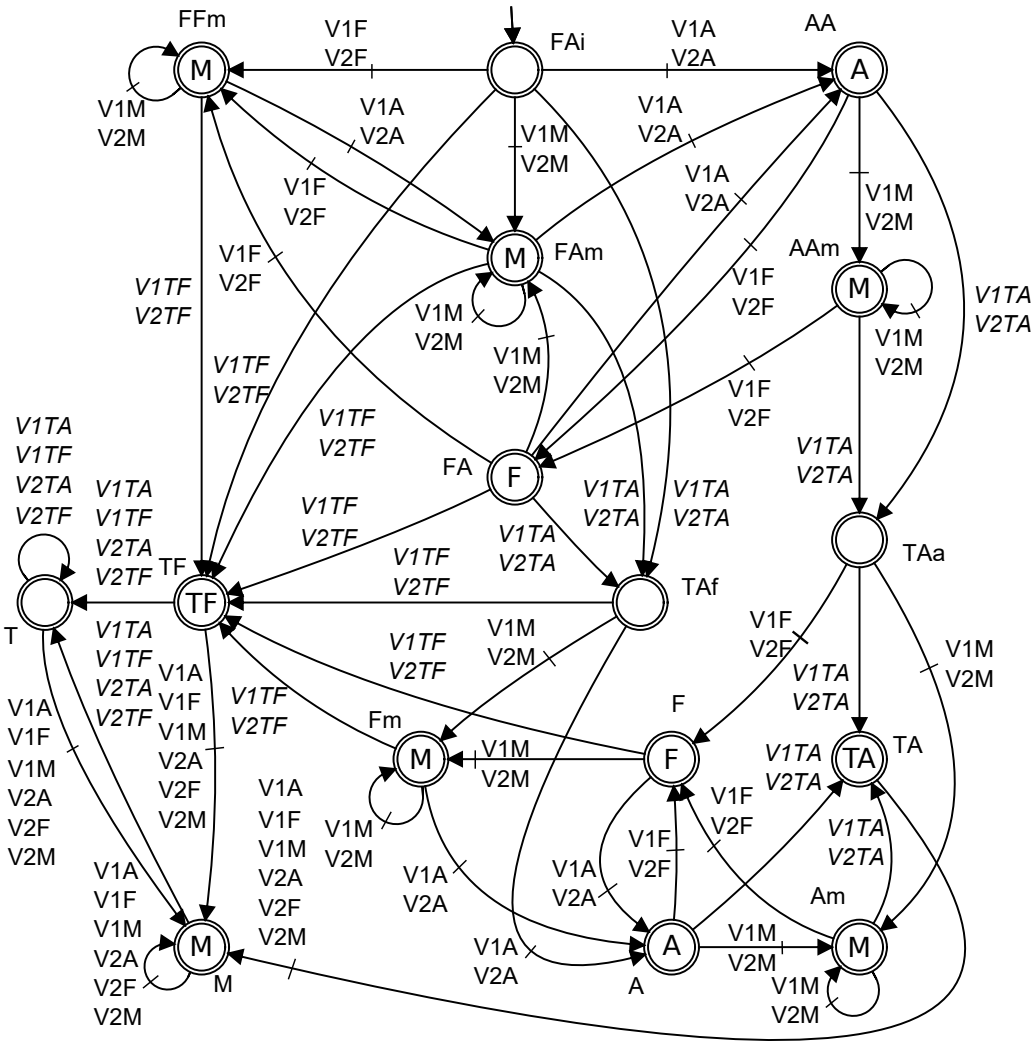


Fonte: Elaborado pelo autor.

Na arquitetura de controle hierárquico, a planta operacional consiste em um autômato de Moore que vocaliza para o nível hierárquico acima os eventos abstratos relevantes. Para facilitar a definição de vocalizações no modelo de malha fechada local ($R_{12}/\mathbf{G_1^V}||\mathbf{G_2^V}$), é criado um autômato de Moore auxiliar $\mathbf{G_{12}^{voc}}$ (Figura 51). Esse modelo associa estados de $\mathbf{G_1^V}||\mathbf{G_2^V}$ a eventos abstratos do equivalente em série (Σ_{12}^{eq})

conforme os eventos das válvulas em série alteram a vazão no duto. Por exemplo, no estado inicial, com V_1 fechada e V_2 aberta, se ocorrer V_{1Abre}, $\mathbf{G_{12}^{voc}}$ vocaliza V_{12Abre}; no mesmo estado, ocorrendo $V_{1TFechada}$, é vocalizado $V_{12TFechada}$; mas, no mesmo estado, ocorrendo $V_{2TAberta}$, nenhum evento é vocalizado, pois para o equivalente em série não há alteração na vazão do duto. Esse modelo contempla todas as possibilidades de acionamento de cada uma das duas válvulas em série e não contém nenhuma restrição para seus eventos.

Figura 51 – $\mathbf{G_{12}^{voc}}$: modelo de vocalizações para válvulas em série, onde V1A, V1F, V1M, V1TA, V1TF correspondem aos eventos da válvula 1 V_{1Abre}, V_{1Fecha}, $V_{1Mantem}$, $V_{1TAberta}$ e $V_{1TFechada}$, análogo também para a válvula 2; e A, F, M, TA, TF correspondem aos eventos a serem vocalizados V_{12Abre}, $V_{12Fecha}$, $V_{12Mantem}$, $V_{12TAberta}$ e $V_{12TFechada}$.

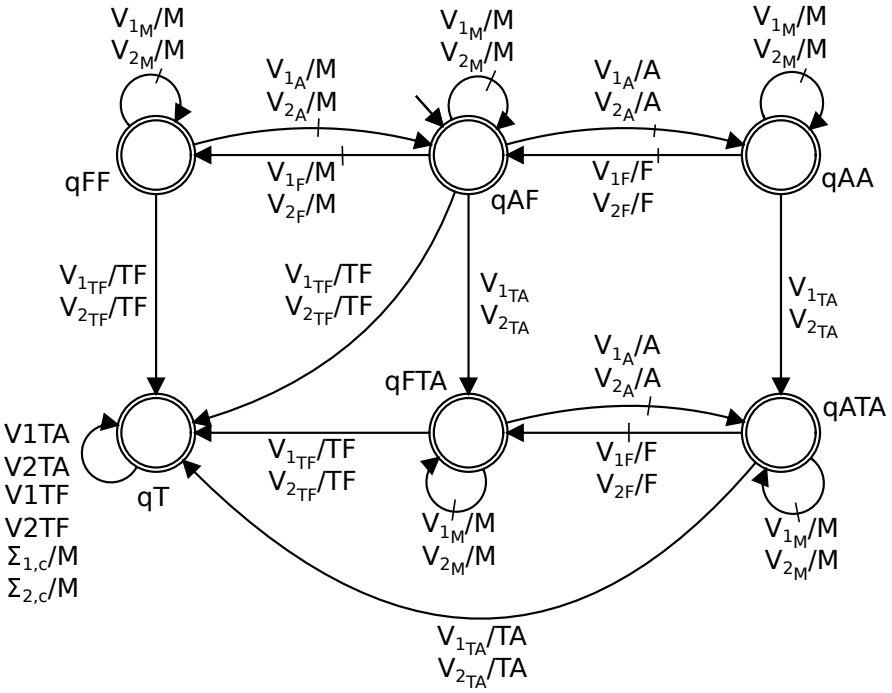


Fonte: Elaborado pelo autor.

Entretanto, o modelo de $\mathbf{G_{12}^{voc}}$ contém 16 estados e sua representação não é muito compacta. Por essa razão, com o objetivo de obter uma representação mais enxuta para os modelos de vocalização, será utilizado o padrão de autômatos de Mealy,

em que a vocalização é representada depois de uma '/' na transição. Dessa forma, o mesmo modelo de vocalizações da figura anterior pode ser reescrito como o autômato de Mealy ilustrado na Figura 52. Todas as transições são padronizadas como σ/τ, em que σ é o evento de baixo nível e τ é o evento abstrato vocalizado. As transições em que aparece somente σ são silenciosas.

Figura 52 – $\mathbf{G_{12}^{voc}}$: modelo de vocalizações para duas válvulas em série representado como autômato de Mealy.

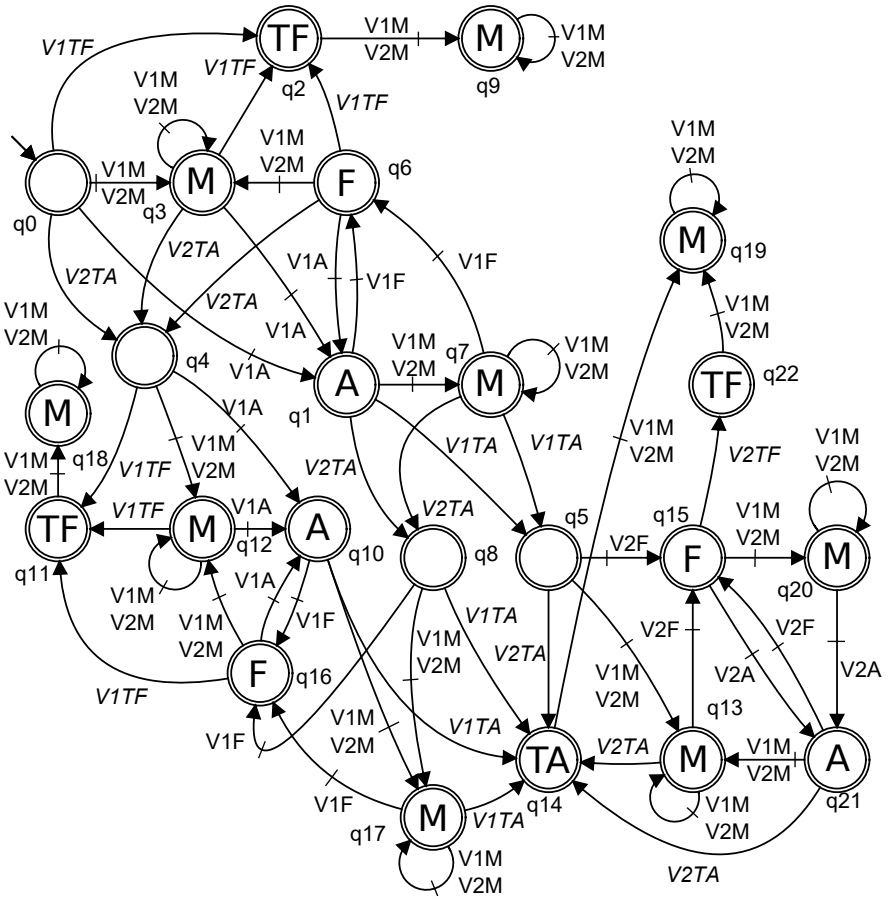


Fonte: Elaborado pelo autor.

Conforme mencionado, o único objetivo desse padrão de representação é obter um modelo mais compacto. Entretanto, todas as operações realizadas utilizam o autômato de Moore correspondente. Assim, do produto síncrono do autômato de Moore $\mathbf{G_{12}^{voc}}$ com o autômato $\mathbf{R_{12}}||\mathbf{G_1^V}||\mathbf{G_2^V}$ resulta o autômato de Moore que corresponde à planta do operador $\mathbf{G_{12}^{op}}$, com 23 estados, e seu mapa repórter associado θ_{12} (Figura 53). O produto de um autômato com um autômato de Moore é definido da mesma forma que o produto síncrono entre dois autômatos, sendo que as vocalizações no autômato de Moore são copiadas para os estados correspondentes no autômato de Moore resultante.

O controle supervisório das válvulas em série é realizado através da tradução das diretivas de comando provenientes do supervisor do nível gerencial, para sinais reais de desabilitação para as válvulas individuais. Essa tradução é feita pelo mapa de desabilitações C_{12}^{op}, que define, em cada estado de $\mathbf{G_{12}^{op}}$, quais são os eventos a serem desabilitados para evitar a ocorrência de determinados eventos vocalizados. Essas desabilitações são definidas, conforme mencionado em (ZHONG; WONHAM, 1990),

Figura 53 – $\mathbf{G_{12}^{op}}$: planta operacional para duas válvulas em série.



Fonte: Elaborado pelo autor.

como o último evento controlável antes de atingir um estado vocal, como na Tabela 5. Na primeira coluna constam os estados de $\mathbf{G_{12}^{op}}$, na primeira linha, os eventos da associação equivalente $\mathbf{G_{12}^{Veq}}$. Nas células da tabela constam quais eventos devem ser desabilitados em cada estado para que o correspondente evento do nível superior seja desabilitado.

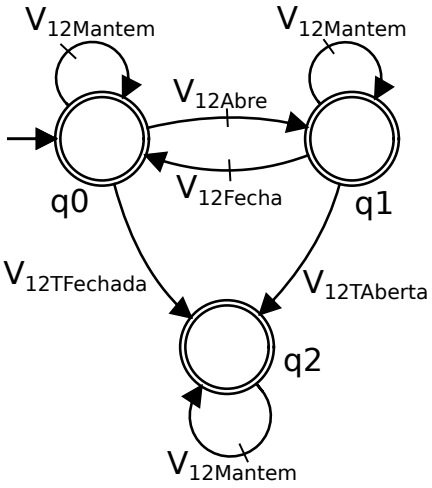
Tabela 5 – Mapa de desabilitações do operador $C_{12}^{op} : Q_{12}^{op} \times \Sigma_{12,c}^{eq} \rightarrow \Delta_{12}$, onde Q_{12}^{op} são estados de G_{12}^{op}, $\Sigma_{12,c}^{eq}$são os eventos controláveis de G_{12}^{Veq}, Δ_{12} são as desabilitações em G_{12}^{op}.

	V_{12Abre}	$V_{12Fecha}$	$V_{12Mantem}$
q_0	$\{V_{1Abre}\}$	{}	$\{V_{1Mantem}, V_{2Mantem}\}$
q_1	{}	$\{V_{1Fecha}\}$	$\{V_{1Mantem}, V_{2Mantem}\}$
...	...	...	...
q_{22}	{}	{}	$\{V_{1Mantem}, V_{2Mantem}\}$

Fonte: Elaborado pelo autor.

Partindo do modelo da planta operacional $\mathbf{G_{12}^{op}}$, o modelo abstrato da válvula equivalente intermediária $\mathbf{G_{12}^{Veq}}$, ilustrado na Figura 54, é obtido por meio do mapa repórter, onde $L(\mathbf{G_{12}^{Veq}}) = \theta_{12}(L(\mathbf{G_{12}^{op}}))$ e $L_m(\mathbf{G_{12}^{Veq}}) = \theta_{12}(L_m(\mathbf{G_{12}^{op}}))$. Observa-se que o modelo $\mathbf{G_{12}^{Veq}}$ tem a mesma estrutura de uma válvula de bloqueio com possibilidade de travamento, com estado inicial fechada. Na estratégia de modelagem por abstrações sucessivas esse modelo pode ser utilizado na associação com outras válvulas, como seria o caso de um modelo abstrato $\mathbf{G_{34}^{Veq}}$, como mostrado na Figura 47.

Figura 54 – $\mathbf{G_{12}^{Veq}}$: abstração de duas válvulas em série.



Fonte: Elaborado pelo autor.

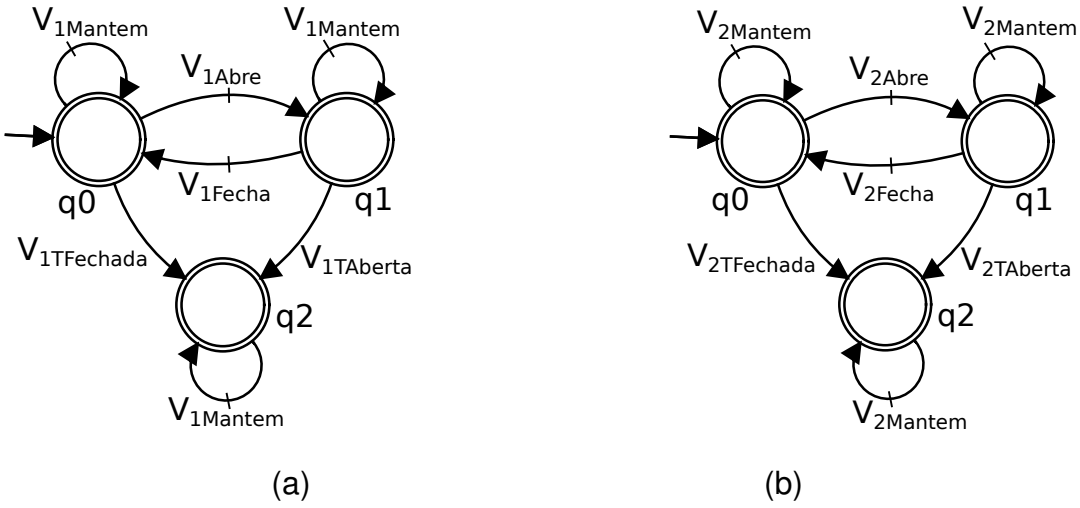
Destaca-se que esse modelo é isomórfico ao modelo de uma válvula de bloqueio simples. Além disso, utilizando esse modelo abstrato em associação com outra válvula de bloqueio em série, resulta novamente um modelo abstrato de uma válvula de bloqueio. Por essa razão, essa estratégia de modelagem pode ser utilizada na representação de um circuito de componentes.

Para analisar se a estrutura hierárquica é capaz de atender as especificações desejadas para o comportamento em malha fechada, devem ser analisadas as propriedades de consistência a partir de $\mathbf{G_{12}^{op}}$, seu mapa repórter associado θ_{12} e o modelo gerencial $\mathbf{G_{12}^{Veq}}$. Assim, nos termos da proposição 2.3.4, verifica-se que $(\mathbf{G_{12}^{op}}, \theta_{12})$ possui consistência de controle estrita, existe consistência de marcação entre $\mathbf{G_{12}^{op}}$ e $\mathbf{G_{12}^{Veq}}$ e θ_{12} possui a propriedade de observador. Com isso, considerando somente o modelo abstrato como o gerente, ou seja, sem considerar o controle de um processo industrial, para qualquer especificação gerencial sobre a válvula equivalente, pode-se garantir um controle supervisório hierárquico ótimo e não bloqueante. O caso em que o processo industrial compõe a estrutura será analisado no final deste capítulo.

4.3.2 Modelagem Para Válvulas em Paralelo

Para o modelo de duas válvulas de bloqueio em paralelo com possibilidade de travamento, considera-se que ambas iniciam na posição considerada fechada, como na Figura 55.

Figura 55 – Modelos para válvulas de bloqueio em paralelo com travamento: (a) $\mathbf{G_1^V}$ com estado inicial fechada e (b) $\mathbf{G_2^V}$ com estado inicial fechada.



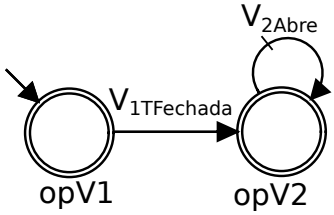
(a) (b)

Fonte: Elaborado pelo autor.

Como o modelo abstrato obtido na seção anterior tem o seu estado inicial representando uma válvula fechada e é isomórfico ao modelo de uma válvula simples, da mesma forma, esse pode ser utilizado na composição em paralelo com outra válvula. Dessa maneira pode-se construir a representação de um circuito de componentes utilizando a estratégia apresentada na seção 4.2 conforme ilustrado na Figura 47 apresentada anteriormente.

Para a obtenção do supervisor local, utiliza-se a especificação E_{12} apresentada na Figura 56. Essa especificação prioriza a operação para V_1, somente permitindo a operação de V_2 quando da ocorrência de travamento fechada de V_1. Assim, obtém-se um supervisor local $\mathcal{S}_{12}$, que contém 9 estados, e sua versão reduzida R_{12} contendo 2 estados.

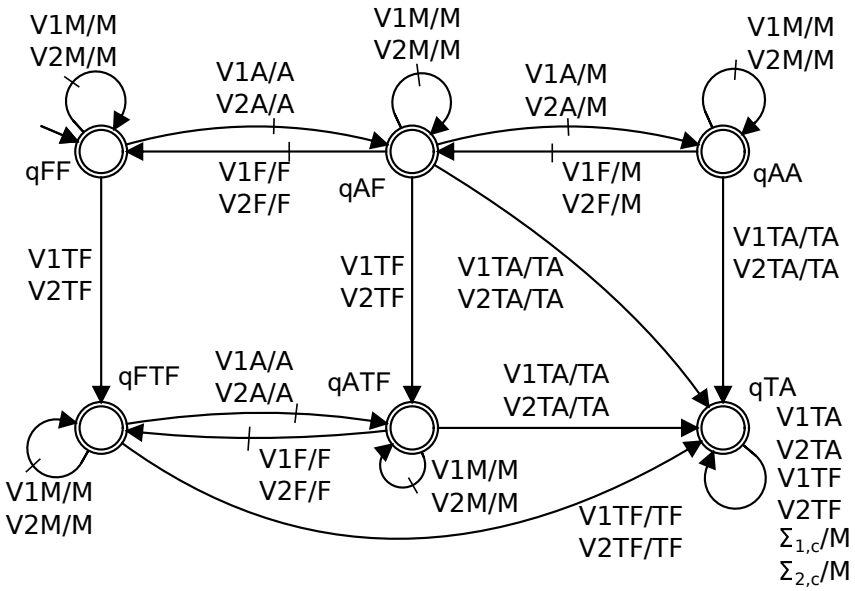
Figura 56 – E_{12}: especificação para duas válvulas de bloqueio em paralelo.



Fonte: Elaborado pelo autor.

Com o objetivo de encontrar o modelo da planta do operador para a associação em paralelo, é construído o modelo de vocalizações $\mathbf{G_{12}^{voc}}$, de forma análoga ao que foi explicado para o caso da associação em série. Na Figura 57 esse modelo é ilustrado como um autômato de Mealy.

Figura 57 – $\mathbf{G_{12}^{voc}}$: modelo de vocalizações para válvulas de bloqueio em paralelo representado como autômato de Mealy.



Fonte: Elaborado pelo autor.

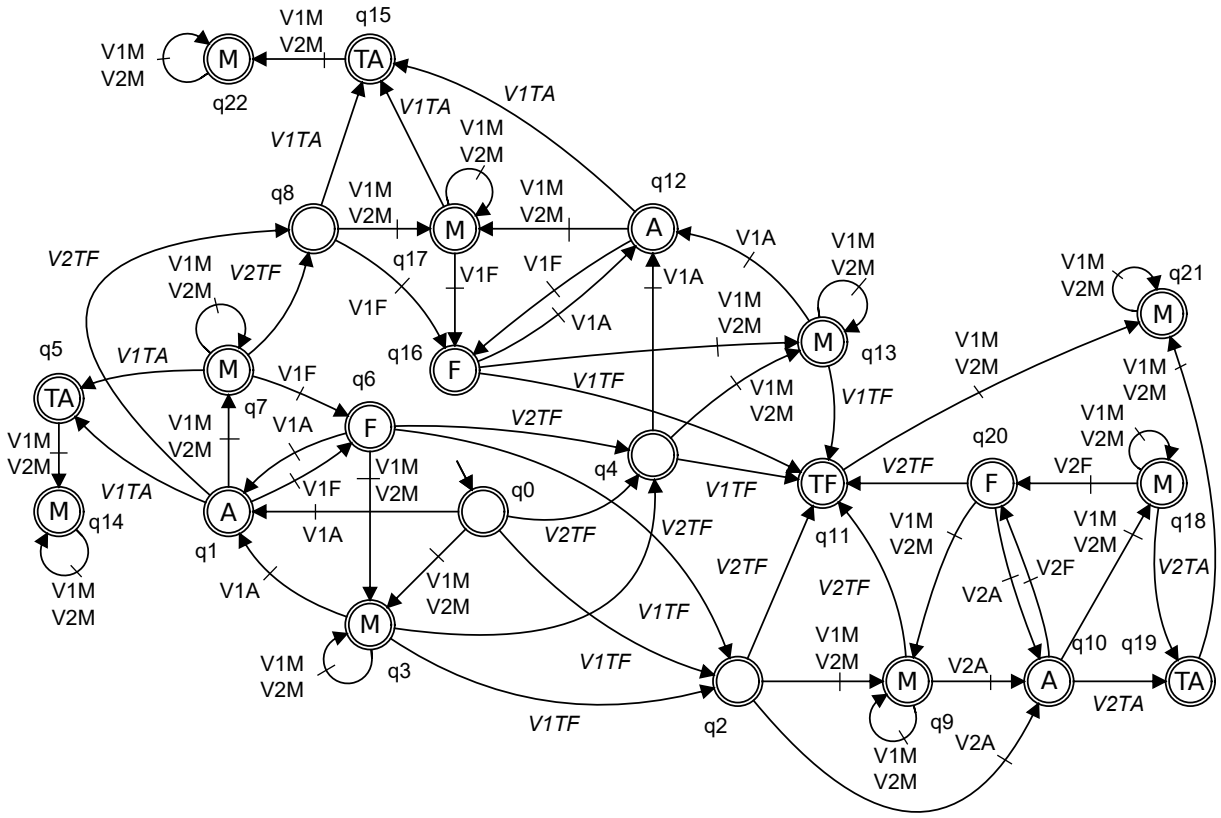
A partir da composição de $\mathbf{G_{12}^{voc}}$ (transformado em um autômato de Moore) com o autômato $\mathbf{R_{12}}||\mathbf{G_1^V}||\mathbf{G_2^V}$ obtém-se a planta do operador $\mathbf{G}_{12}^{op}$, contendo 23 estados, sendo todos eles marcados, e seu mapa repórter associado θ_{12} como apresentado na Figura 58. A partir desse modelo devem ser analisadas as propriedades de consistência necessárias para se garantir o controle hierárquico não bloqueante.

A partir do modelo de $\mathbf{G_{12}^{op}}$ e suas vocalizações, é construído o mapa de desabilitações do operador C_{12}^{op} apresentado na Tabela 6. Essa tabela relaciona os estados da planta do operador com os comandos do supervisor gerencial, resultando nos eventos reais de desabilitação enviados às válvulas.

O modelo $\mathbf{G_{12}^{Veq}}$ (Figura 59), para a associação em paralelo é obtido por meio de θ_{12}, onde $L(\mathbf{G_{12}^{Veq}}) = \theta_{12}(L(\mathbf{G_{12}^{op}}))$ e $L_m(\mathbf{G_{12}^{Veq}}) = \theta_{12}(L_m(\mathbf{G_{12}^{op}}))$. Observa-se que $\mathbf{G_{12}^{Veq}}$ é isomórfico a uma válvula de bloqueio simples inicialmente fechada.

Como esse modelo também é isomórfico ao modelo de uma válvula de bloqueio simples, utilizando esse modelo em associação com outra válvula de bloqueio em paralelo, resulta novamente um modelo abstrato de uma válvula de bloqueio. com isso observa-se que essa estratégia de modelagem pode ser utilizada na representação de um circuito de componentes.

Figura 58 – $\mathbf{G_{12}^{op}}$: planta operacional para duas válvulas em paralelo.



Fonte: Elaborado pelo autor.

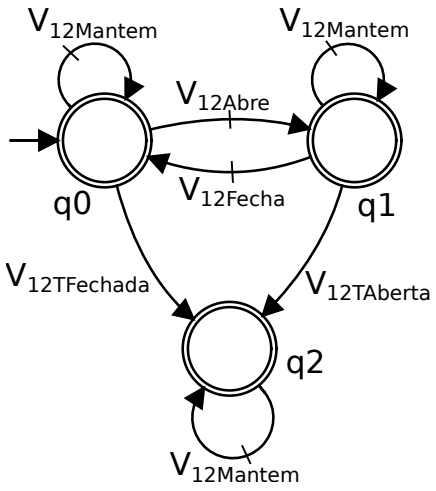
Tabela 6 – Mapa de desabilitações do operador $C_{12}^{op} : Q_{12}^{op} \times \Sigma_{12,c}^{eq} \rightarrow \Delta_{12}$, onde Q_{12}^{op} são estados de G_{12}^{op}, $\Sigma_{12,c}^{eq}$são os eventos controláveis de G_{12}^{Veq}, Δ_{12} são as desabilitações em G_{12}^{op}.

	V_{12Abre}	$V_{12Fecha}$	$V_{12Mantem}$
q_0	$\{V_{1Abre}\}$	{}	$\{V_{1Mantem}, V_{2Mantem}\}$
q_1	{}	$\{V_{1Fecha}\}$	$\{V_{1Mantem}, V_{2Mantem}\}$
...	...	...	...
q_{22}	{}	{}	$\{V_{1Mantem}, V_{2Mantem}\}$

Fonte: Elaborado pelo autor.

Para a associação em paralelo, também devem ser analisadas as propriedades de consistência a partir de $\mathbf{G_{12}^{op}}$, seu mapa repórter associado θ_{12} e o modelo gerencial $\mathbf{G_{12}^{Veq}}$. Da mesma forma como no caso anterior, nos termos da proposição 2.3.4, verifica-se que $(\mathbf{G_{12}^{op}}, \theta_{12})$ possui consistência de controle estrita, existe consistência de marcação entre $\mathbf{G_{12}^{op}}$ e $\mathbf{G_{12}^{Veq}}$ e θ_{12} possui a propriedade de observador. Assim, considerando somente o modelo abtrato como gerente, sem considerar o controle do processo industrial, para qualquer especificação gerencial, pode-se garantir um controle supervisório hierárquico ótimo e não bloqueante.

Figura 59 – $\mathbf{G_{12}^{Veq}}$: abstração de duas válvulas em paralelo.



Fonte: Elaborado pelo autor.

4.4 MODELAGEM PARA UMA VÁLVULA DE CONTROLE EM SÉRIE COM UMA VÁLVULA DE BLOQUEIO

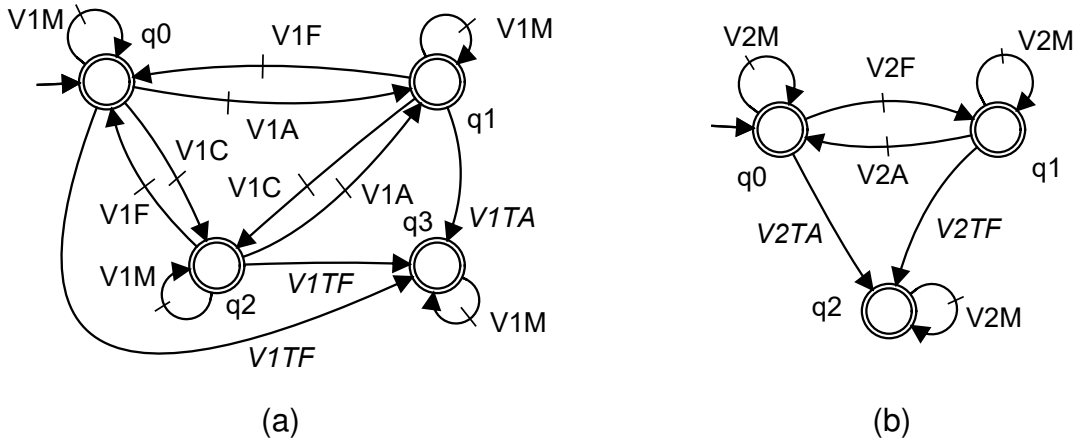
A mesma estratégia de modelagem, quando aplicada a um circuito de componentes contendo uma válvula de controle, apresenta um aspecto relacionado às consistências do modelo do operador que não é visto quando são consideradas somente válvulas de bloqueio. Conforme demonstrado no final desta seção, a condição de mapa repórter observador não é atingida na planta operacional dessa estrutura, o que traz um problema para se conseguir obter o controle hierárquico ótimo e não bloqueante para esse caso.

De forma semelhante aos modelos da Seção 4.3.1 (duas válvulas de bloqueio em série), é considerado para a válvula de controle seu estado inicial como fechada (Figura 60 - a) e para a válvula de bloqueio, seu estado inicial como aberta (Figura 60 - b). Para a válvula de controle, o estado $q2$ indica que a válvula está em modo de controle. Considera-se, como hipótese de modelagem, que nesse estado a única possibilidade de falha para a válvula é travar fechada. Essa hipótese se justifica ao se considerar uma válvula de controle pneumática, como a utilizada no capítulo 3, em que uma falha mecânica leva ao fechamento da mesma (ou ao menos uma vazão resultante insuficiente para aumentar o nível do tanque).

A especificação local para uma associação em série de uma válvula de controle com uma válvula de bloqueio é apresentada na Figura 61. Esse modelo recebe uma atenção maior do que para as válvulas de bloqueio devido às características mais especializadas de uma válvula de controle.

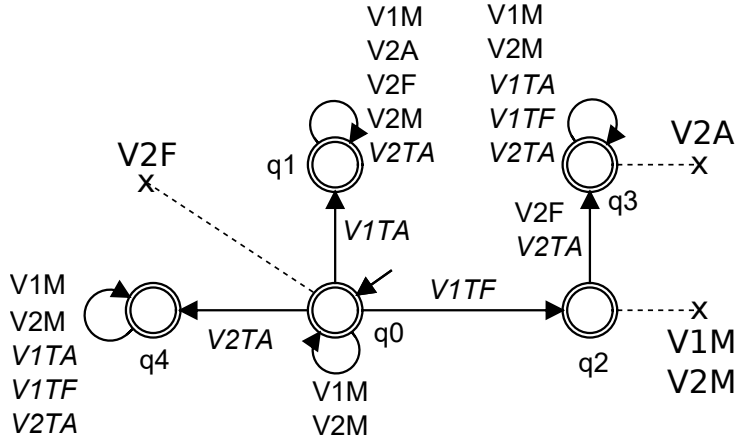
Considera-se que, no estado inicial, a válvula 2 (bloqueio) não pode fechar e, por isso, não pode operar. Essa condição somente é permitida se a válvula 1 travar aberta (estado $q1$). Nesse caso a válvula 2 assume o controle do processo no lugar

Figura 60 – (a) $\mathbf{G}_1^V$: Modelo de uma válvula de controle em uma configuração série. (b) $\mathbf{G}_2^V$: Modelo de uma válvula de bloqueio em uma configuração série.



Fonte: Elaborado pelo autor.

Figura 61 – E_{12}: Especificação local para duas válvulas (controle – bloqueio) em série.



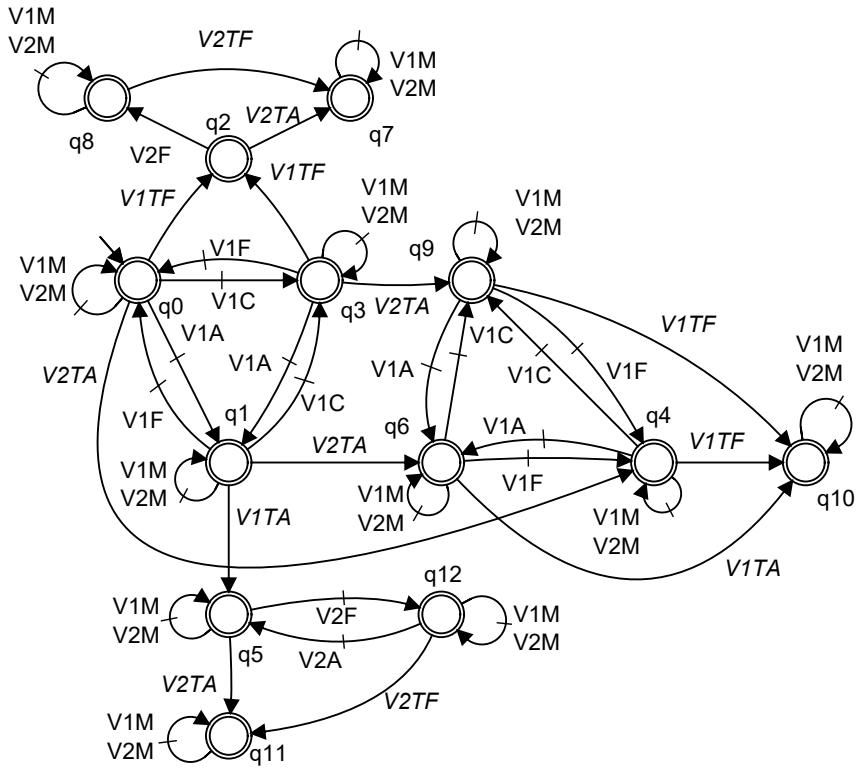
Fonte: Elaborado pelo autor.

da válvula 1. Por outro lado, se a válvula 1 travar fechada (estado $q2$), por questões de segurança do processo, a válvula 2 deverá obrigatoriamente fechar, atingindo o estado $q3$ em que somente ocorre o evento de se manter no mesmo estado. A partir de E_{12} obtém-se o supervisor local $\mathcal{S}_{12}$, representado na Figura 62.

A exemplo das seções anteriores, para a presente análise também se utiliza um modelo de vocalizações (Figura 63) representado como um autômato de Mealy.

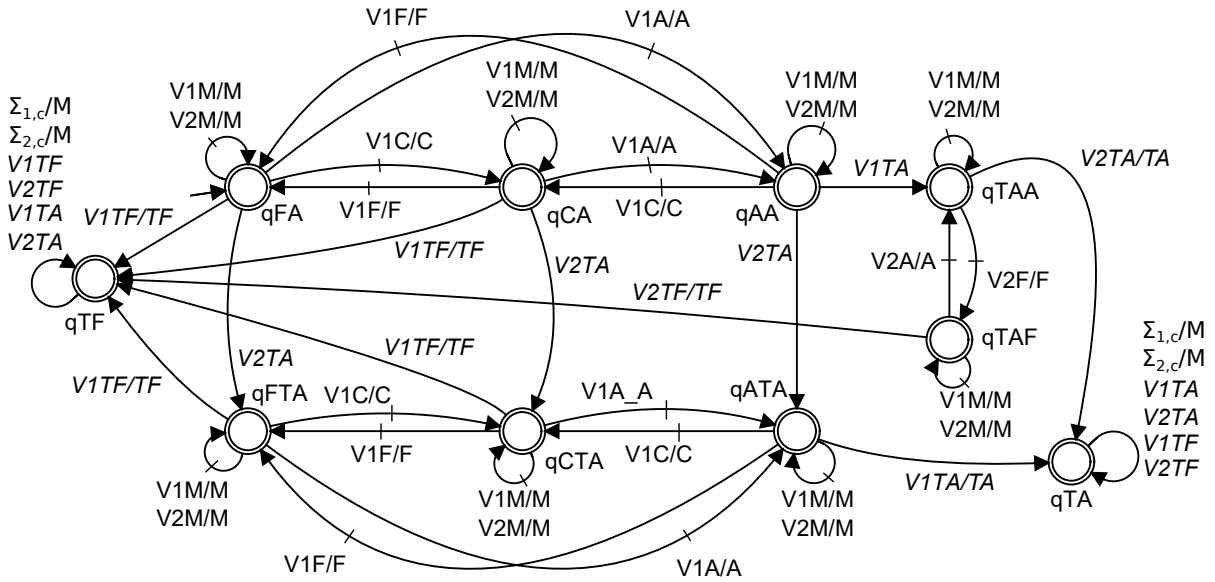
Para esse modelo, diferentemente das seções anteriores, não são consideradas todas as possibilidades de acionamento das duas válvulas individuais, buscando-se uma representação compacta. Para sua construção são levadas em conta as desabilitações que a especificação local E_{12} (Figura 61) promove, ou seja, ess modelo não impede a ocorrência de nenhum evento que o supervisor local permita. A composição desse sistema em malha fechada com o modelo de vocalizações resulta na planta do operador apresentada na Figura 64.

Figura 62 – $\mathcal{S}_{12}$: Supervisor local para duas válvulas (controle – bloqueio) em série.



Fonte: Elaborado pelo autor.

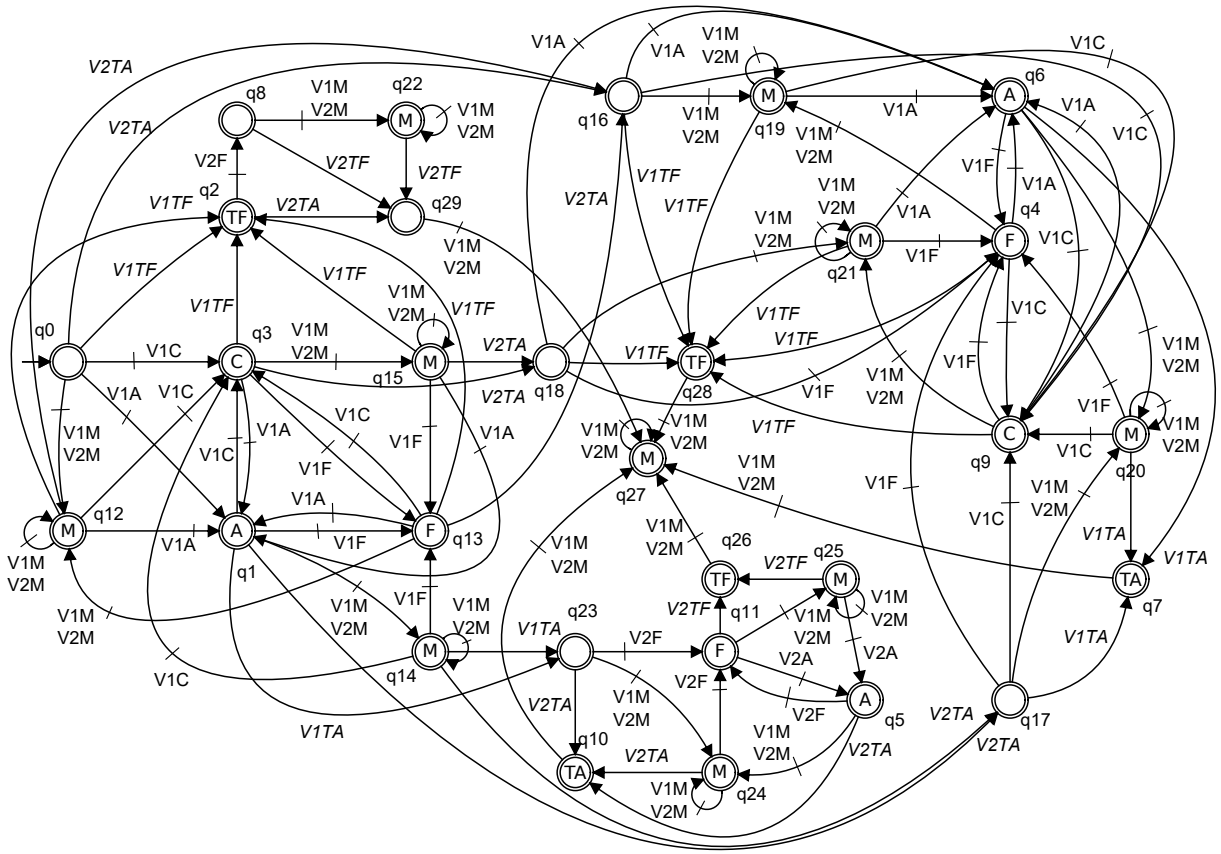
Figura 63 – $\mathbf{G_{12}^{voc}}$: modelo de vocalizações para uma válvula de controle em série com uma de bloqueio representado como autômato de Mealy.



Fonte: Elaborado pelo autor.

Partindo do modelo da planta operacional é construído o mapa de desabilitações do operador, conforme apresentado na Tabela 7.

Figura 64 – $\mathbf{G}^{op}$: Planta do operador para uma válvula de controle em série com uma válvula de bloqueio.



Fonte: Elaborado pelo autor.

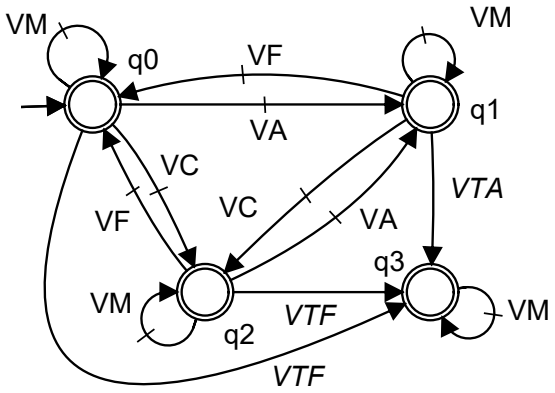
Tabela 7 – Mapa de desabilitações do operador $C_{12}^{op} : Q_{12}^{op} \times \Sigma_{12,c}^{eq} \rightarrow \Delta_{12}$, onde Q_{12}^{op} são estados de $\mathbf{G^{op}}$, $\Sigma_{12,c}^{eq}$são os eventos controláveis de $\mathbf{G_{12}^{Veq}}$, Δ_{12} são as desabilitações em $\mathbf{G^{op}}$.

	V_{12Abre}	$V_{12Fecha}$	$V_{12Controla}$	$V_{12Mantem}$
q_0	$\{V_{1Abre}\}$	{}	$\{V_{1Controla}\}$	$\{V_{1Mantem}, V_{2Mantem}\}$
q_1	{}	$\{V_{1Fecha}\}$	$\{V_{1Controla}\}$	$\{V_{1Mantem}, V_{2Mantem}\}$
...	...	...	...	...
q_{29}	{}	{}	{}	$\{V_{1Mantem}, V_{2Mantem}\}$

Fonte: Elaborado pelo autor.

O modelo $\mathbf{G_{12}^{Veq}}$, representado na Figura 65, para a associação em série de uma válvula de controle com uma válvula de bloqueio é obtido por meio do mapa repórter θ_{12}, onde $L(\mathbf{G_{12}^{Veq}}) = \theta_{12}(L(\mathbf{G^{op}}))$ e $L_m(\mathbf{G_{12}^{Veq}}) = \theta_{12}(L_m(\mathbf{G^{op}}))$. Observa-se que $\mathbf{G_{12}^{Veq}}$ é isomórfico ao modelo de uma válvula de controle. Um dos pontos positivos da abordagem por abstrações sucessivas é a possibilidade de utilizar o mesmo modelo da abstração para a construção de mais níveis hierárquicos, devido ao isomorfismo com os modelos das válvulas individuais. Entretanto, para o modelo abstrato da válvula de controle, surge uma questão relacionada a observabilidade dos eventos.

Figura 65 – $\mathbf{G_{12}^{Veq}}$: Modelo de abstração de uma válvula equivalente para duas válvulas (controle – bloqueio) em série.



Fonte: Elaborado pelo autor.

O modelo equivalente da associação opera inicialmente como uma válvula de controle. Entretanto, no momento em que a válvula de controle trava aberta, a válvula de bloqueio entra em operação e o modelo equivalente opera como uma válvula de bloqueio. Assim, nesse caso, apesar de o evento VC (válvula controla) ser elegível no modelo abstrato, esse evento não é possível de ocorrer, pois no nível operacional já não existe essa possibilidade devido ao travamento da primeira válvula.

Ao analisar o modelo $\mathbf{G^{op}}$ (Figura 64), tal situação pode ser caracterizada pelo mapa repórter não possuir a propriedade de observador. Analisando esse modelo, tomando como exemplo o estado $q1$, a vocalização do evento C (que representa $V_{12Controla}$) é possível. No entanto, ao ocorrer o evento silencioso $V1TA$ ($V_{1TravaAberta}$) o modelo atinge o estado $q23$, em que a vocalização de C já não é mais possível. Dessa forma, apesar desse modelo possuir as propriedades de consistência de controle estrita e consistência de marcação, por não possuir um mapa repórter observador não é possível garantir o não bloqueio na estrutura.

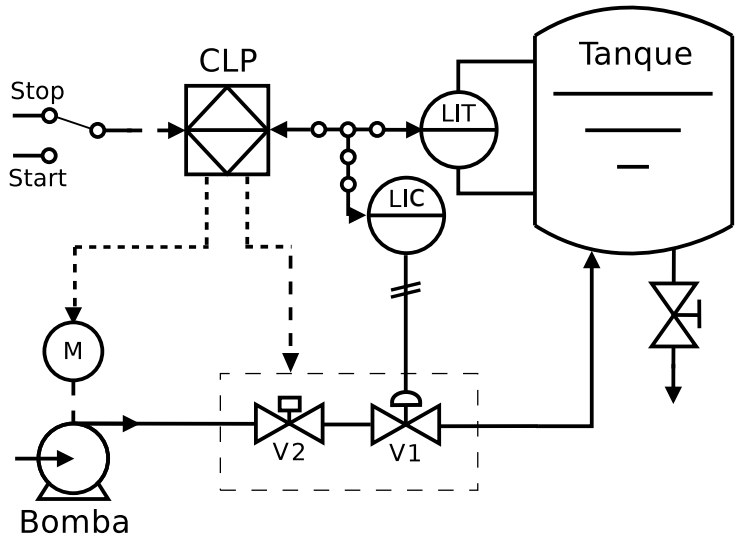
No Capítulo 5 a condição de observador do mapa repórter será analisada de forma mais detalhada. Será observado que eventos que se enquadram de forma similar ao apresentado no parágrafo anterior serão definidos como não confiáveis. Seguindo essa linha, no próximo capítulo será elaborada uma condição baseada nos eventos confiáveis para garantir o controle supervisório hierárquico ótimo não bloqueante.

4.5 APLICAÇÃO DA ESTRATÉGIA DE MODELAGEM

Embora a estrutura analisada na seção anterior, composta por uma válvula de controle em série com uma válvula de bloqueio, apresente uma não conformidade relacionada à propriedade de observador do mapa repórter, essa será utilizada em um exemplo para ilustrar a aplicação do método proposto. Assim, como exemplo de aplicação da estratégia de modelagem por abstrações sucessivas será utilizado o

processo industrial comandado por um circuito de componentes formado por uma válvula de controle em série com uma válvula de bloqueio, conforme ilustrado na Figura 66.

Figura 66 – Diagrama de um processo industrial controlado por uma válvula de controle em série com uma válvula de bloqueio.



Fonte: Elaborado pelo autor.

A abstração do circuito de válvulas em uma válvula equivalente $\mathbf{G^{Veq}}$ simplifica a modelagem de especificações gerenciais e reduz a complexidade computacional da síntese de supervisor. Neste exemplo, a estratégia de modelagem por abstrações sucessivas será utilizada para obter o modelo de uma válvula equivalente, que represente o circuito, para comandar o processo. A arquitetura de modelagem empregada se enquadra na mesma estrutura da Figura 48, mas agora utilizando somente dois níveis. O modelo do operador corresponde à associação das duas válvulas em série e a abstração da válvula equivalente interage com o modelo do processo industrial. Pode-se imaginar a Figura 48 somente com os dois níveis de cima: o superior com a válvula equivalente e o processo; e o intermediário formando o nível do operador com a válvula de controle e a de bloqueio.

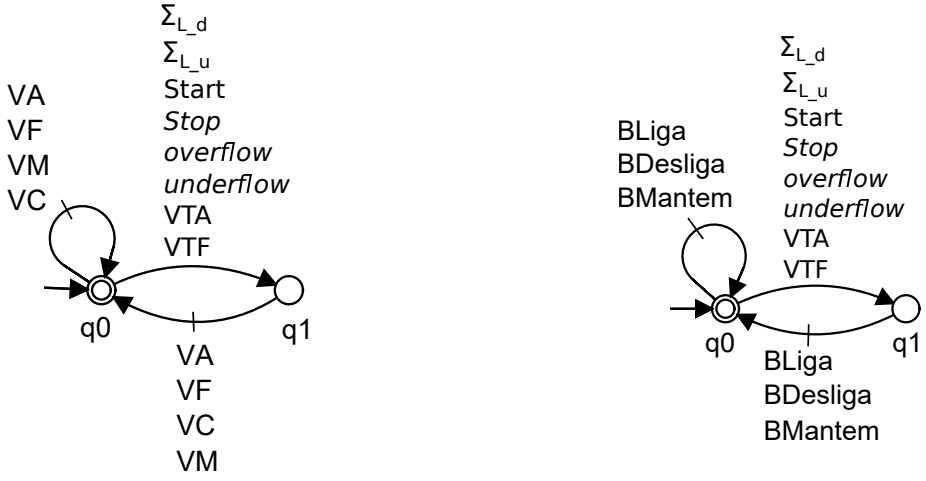
Neste exemplo a planta gerencial $\mathbf{G^{ge}} = \mathbf{G^{Veq}} || \, \mathbf{G_{proc}}$ representa a composição da válvula equivalente com os demais componentes do processo e $\mathcal{S}^{ge}$ representa o supervisor gerencial. Enquanto os eventos de $\Sigma_{proc,c}$ desabilitados por $\mathcal{S}^{ge}$ estão diretamente relacionados com os eventos do processo, as desabilitações de Σ_c^{Veq} são traduzidas pelo mapa do operador em desabilitações sobre os modelos das válvulas operacionais V_1, V_2.

Considera-se que o processo industrial seja composto pelos modelos $\mathbf{G_{Niveis}}$, $\mathbf{G_{Chave}}$, $\mathbf{G_{Bomba}}$, $\mathbf{G_{PB}}$, $\mathbf{G_{PV}}$ e $\mathbf{G_{Vazao}}$, da mesma forma que abordado nos exemplos anteriores, comandado pelo circuito de válvulas representado pelo modelo abstrato da válvula equivalente $\mathbf{G_{Valvula}}$. Os modelos $\mathbf{G_{Niveis}}$, $\mathbf{G_{Chave}}$ e $\mathbf{G_{Bomba}}$ são

representados da mesma maneira que no exemplo 4.1.1 e, por isso, não são aqui reproduzidos. O modelo utilizado para a válvula equivalente segue como um modelo abstrato de uma válvula de controle, da mesma maneira que discutido na seção anterior, ilustrado na Figura 65.

Neste exemplo, o modelo de preempção pela válvula (Figura 67) difere dos demais apresentados anteriormente por considerar uma válvula de controle com possibilidade de travamento. Na figura também é apresentado o modelo de preempção por meio da bomba. O alfabeto $\Sigma_{L\_d} = \{d\_HI, d\_SP, d\_LO, d\_LO\_LO\}$ contém os eventos de diminuição de nível no tanque e $\Sigma_{L\_u} = \{u\_LO, u\_SP, u\_HI, u\_HI\_HI\}$ contém os eventos de aumento de nível.

Figura 67 – (a) $\mathbf{G_{PV}}$: Modelo de preempção por meio da válvula equivalente da associação em série controle-bloqueio. (b) $\mathbf{G_{PB}}$: Modelo de preempção da bomba.

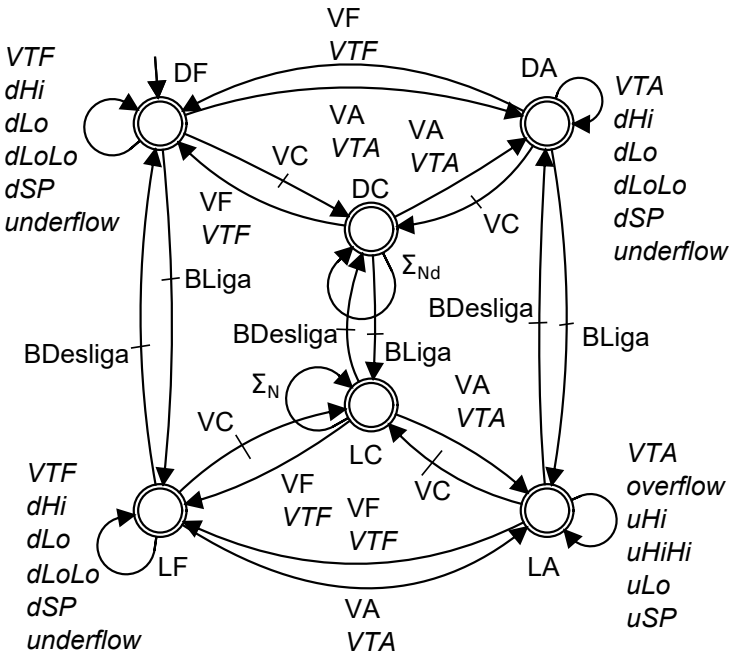


Fonte: Elaborado pelo autor.

O modelo que representa a vazão no tanque, seguindo o mesmo raciocínio dos exemplos das seções anteriores, depende dos estados dos atuadores. No modelo da Figura 68, os estados DC e LC são os que a válvula se encontra em modo de controle. Entretanto, em DC a bomba está desligada e, por essa razão, o nível somente pode descer, o que está representado pelo conjunto Σ_{Nd} = $\{d\_HI$, d_SP, d_LO, d_LO_LO, $underflow\}$. Em LC a bomba se encontra ligada, logo o nível pode tanto subir quanto descer, o que é representado pelo conjunto $\Sigma_N = \{d\_HI$, d_SP, d_LO, d_LO_LO, $underflow$, u_LO, u_SP, u_HI, u_HI_HI, $overflow\}$. Esse modelo não desabilita nenhum evento não controlável que esteja elegível em outros modelos das plantas do operador.

O modelo monolítico da planta do gerente é obtido como $\mathbf{G^{ge}} = \mathbf{G_{Niveis}}||\ \mathbf{G_{Chave}}||\ \mathbf{G_{Bomba}}||\ \mathbf{G_{PB}}||\ \mathbf{G_{PV}}||\ \mathbf{G_{Vazao}}||\ \mathbf{G_{Valvula}}$ e contém 400 estados. Para ob-

Figura 68 – $\mathbf{G_{VAZ}}$: Modelo de vazão do tanque.



Fonte: Elaborado pelo autor.

ter o controle supervisório do processo industrial comandado pelo circuito de válvulas, projetam-se as especificações no nível gerencial. Entretanto duas questões surgem dessa análise. A primeira se refere ao mapa repórter do circuito de válvulas, como exposto no final da seção anterior e que será melhor tratada no Capítulo 5. A segunda questão está ligada à sincronização de eventos no nível do gerente.

De modo a obter supervisores para a estrutura apresentada, poderia se pensar em utilizar as arquiteturas de controle hierárquico apresentadas em Pu (2000) ou Seow (2014). Entretanto, apesar de os modelos do exemplo se encaixarem nestas arquiteturas, em ambos trabalhos são impostas restrições em relação à sincronização de eventos no gerente. Nos dois casos, ao existir um modelo abstrato interagindo com um modelo no nível do gerente, é feita a consideração de que não se pode haver sincronização de eventos entre esses modelos. No exemplo desta seção, o modelo monolítico que compõe o processo contém eventos do modelo da válvula equivalente e, assim, sincroniza esses eventos. Mais especificamente pode-se observar o modelo de preempção $\mathbf{G_{PV}}$ (Figura 67 - a) que sincroniza, por exemplo, os eventos VTA ($V_{12TravaAberta}$) e VTF ($V_{12TravaFechada}$). Fisicamente o modelo da preempção é uma hipótese de modelagem que diz que sempre entre dois eventos não controláveis (mudança de nível ou travamento da válvula) há o comando dos atuadores, por esses serem mais rápidos. Como os eventos de travamento da válvula equivalente são abstratos, sua ocorrência está condicionada a vocalização de cadeias do nível do operador e a sincronização no nível do gerente é incapaz de influenciar sua ocorrência no baixo nível.

Dessa forma, percebe-se que os métodos existentes não são capazes de considerar as condições colocadas para a resolução do exemplo desta seção. Diante desse quadro, nesta tese é desenvolvida a denominada abordagem interníveis apresentada no Capítulo 6. Com a abordagem proposta será levado em conta a sincronização de eventos abstratos no nível gerencial o que impacta na ocorrência de eventos do operador.

4.6 DISCUSSÃO

Neste capítulo é proposta uma de estratégia de modelagem por abstrações sucessivas utilizando níveis hierárquicos, com o objetivo de reduzir as complexidades de modelagem e de síntese em processos comandados por circuitos de componentes. São desenvolvidos modelos para válvulas de bloqueio e de controle com possibilidade de travamento e a obtenção de um modelo abstrato que representa o equivalente para o circuito de componentes.

São apresentadas, entretanto, duas limitações dos métodos de controle hierárquico existentes e que dificultam a aplicação da abordagem proposta. A primeira está relacionada a uma exigência demasiadamente restritiva de que, em uma planta operacional, o mapa repórter associado sempre deve possuir a propriedade de observador. A segunda limitação é uma restrição dos métodos existentes de que no nível gerencial não é possível haver sincronização de eventos abstratos. Essas limitações serão solucionadas por técnicas desenvolvidas nos Capítulos 5 e 6 respectivamente.

5 ARQUITETURA HIERÁRQUICA NÃO BLOQUEANTE BASEADA EM EVENTOS CONFIÁVEIS

Foi apresentada, na Seção 4.4, uma estratégia de modelagem para um circuito de componentes formado por uma válvula de controle em série com uma válvula de bloqueio, com o objetivo de obter um modelo abstrato de uma válvula equivalente. Mostrou-se que para a estrutura proposta o mapa repórter associado à planta do operador não possui a propriedade de observador. Analisando de forma mais detalhada, pôde-se perceber que apenas um dos eventos do nível gerencial apresenta ambiguidade em sua vocalização, devido a essa característica do mapa repórter. A partir dessa análise, no presente capítulo será desenvolvida uma técnica baseada em eventos confiáveis, capaz de garantir um controle supervisório hierárquico ótimo e não bloqueante para determinadas especificações.

Neste capítulo são analisadas estruturas que satisfazem as condições de consistência de controle estrita e de marcação, porém o mapa repórter não possui a propriedade de observador. Se um mapa repórter não possui tal propriedade, significa que ao menos um evento gerencial, apesar de ser elegível, em dado momento pode ficar impossibilitado de ocorrer devido a algum trecho silencioso do operador.

Conforme a Proposição 2.3.4, é garantido que em uma estrutura hierárquica em que haja consistência de controle estrita, consistência de marcação e o mapa repórter possua a propriedade de observador para qualquer especificação gerencial o sistema em malha fechada no nível do gerente será não bloqueante se e somente se o sistema em malha fechada no nível do operador for não bloqueante. A propriedade de mapa repórter observador (WONG; WONHAM, 1996), uma das condições mencionadas, pode ser expressa formalmente por:

$$(\forall s \in L(\mathbf{G^{op}}))(\forall \tau \in T)\theta(s)\tau \in L(\mathbf{G^{ge}}) \rightarrow (\exists u \in \Sigma^{+})\text{: } su \in L(\mathbf{G^{op}}) \ \& \ \theta(su) = \theta(s)\tau$$

Em palavras, essa propriedade pode ser descrita da seguinte forma: para duas ou mais cadeias do operador que possuem a mesma imagem, os próximos eventos gerenciais que as seguem como sua continuação devem ser o mesmo. Neste capítulo, serão desenvolvidas condições para flexibilizar a propriedade de observador, sendo que a questão de bloqueio em estruturas hierárquicas será condicionada também às especificações no nível gerencial.

5.1 EVENTO CONFIÁVEL

A não confiabilidade de um evento no nível gerencial somente é razoável de ser analisada quando o mapa repórter não possui a propriedade de observador. Desta forma, para alguns eventos no nível do gerente, mesmo quando são elegíveis, sua ocorrência pode não ser possível de fato, dada a estrutura do mapa repórter. Um

evento é definido como confiável quando, para toda cadeia do operador cuja imagem tenha como continuação esse evento, sempre é possível atingir um estado que vocaliza esse evento, ou seja sempre vai existir uma continuação na linguagem do operador que vocaliza esse evento. Em outras palavras, se um evento τ é confiável, ao existir $t\tau \in L(\mathbf{G^{ge}})$, não existe nenhuma cadeia com imagem igual a t, mas que não seja possível atingir um estado que vocaliza τ.

Definição 5.1.1. ***Evento Confiável:*** *Seja uma planta $\mathbf{G^{op}}$ e seu mapa repórter associado $\theta : L(\mathbf{G^{op}}) \to T^*$. Um evento $\tau \in T$ é definido como confiável e.r.a. θ se:*

$$(\forall s \in L(\mathbf{G^{op}}))\theta(s)\tau \in L(\mathbf{G^{ge}}) \to (\exists u \in \Sigma^+)\text{: } su \in L(\mathbf{G^{op}}) \;\&\; \theta(su) = \theta(s)\tau$$

Por outro lado, um evento τ é dito não confiável se, ao existir $t\tau \in L(\mathbf{G^{ge}})$, o estado que vocaliza τ pode não ser atingível por alguma cadeia cuja imagem seja t. Em outras palavras, o evento τ pode passar a não ser mais elegível sem que essa informação seja repassada ao gerente.

Quando, em uma dada estrutura hierárquica, o mapa repórter associado possui a propriedade de observador, pode-se dizer que todos os eventos gerenciais são confiáveis.

Proposição 5.1.1. ***Mapa Repórter Observador:*** *Um mapa repórter $\theta : L(\mathbf{G^{op}}) \to T^*$ possui a propriedade de observador se e somente se todo $\tau \in T$ é um evento confiável e.r.a. θ.*

Demonstração. Seja uma estrutura hierárquica formada pelo par $(\mathbf{G^{op}}, \mathbf{G^{ge}})$ e seu mapa repórter associado $\theta : L(\mathbf{G^{op}}) \to T^*$. Ao considerar todos os eventos $\tau \in T$ como confiáveis, pode-se afirmar que:

$$(\forall s \in L(\mathbf{G^{op}}))(\forall \tau \in T)\theta(s)\tau \in L(\mathbf{G^{ge}}) \to (\exists u \in \Sigma^+)\text{: } su \in L(\mathbf{G^{op}}) \;\&\; \theta(su) = \theta(s)\tau,$$

que caracteriza a propriedade de mapa repórter observador.

□

Quando uma cadeia $t \in L(\mathbf{G^{ge}})$ é formada exclusivamente por eventos confiáveis, toda cadeia cuja imagem é prefixo de t sempre pode ser completada em uma cadeia cuja imagem é t. A partir dessa constatação, é possível estender para cadeias a definição de eventos confiáveis.

Proposição 5.1.2. ***Cadeia de eventos confiáveis:*** *Seja uma planta $\mathbf{G^{op}}$, seu mapa repórter associado $\theta : L(\mathbf{G^{op}}) \to T^*$ e um alfabeto $T_{conf} \subseteq T$ formado por eventos confiáveis e.r.a θ. Se $t \in T^+_{conf}$, então*

$$(\forall s \in L(\mathbf{G^{op}}))\; \theta(s) \leq t \to (\exists u \in \Sigma^*)\text{: } su \in L(\mathbf{G^{op}}) \;\&\; \theta(su) = \theta(s)t$$

Demonstração. A demonstração segue por indução no comprimento de $t \in T^{+}_{conf}$.

- Para o caso base $t = \tau' \in T_{conf}$, onde $|t| = n = 1$:

  Pela Definição 5.1.1,

  $(\forall s \in L(\mathbf{G^{op}}))\ \theta(s)\tau' \in L(\mathbf{G^{ge}}) \rightarrow (\exists u \in \Sigma^{+})$: $su \in L(\mathbf{G^{op}})\ \&\ \theta(su) = \theta(s)\tau'$.

- Como hipótese indutiva, para $t \in T^{+}_{conf}$, onde $|t| = n \geq 1$, assume-se que:

  $(\forall s \in L(\mathbf{G^{op}}))\ \theta(s)t \in L(\mathbf{G^{ge}}) \rightarrow (\exists u \in \Sigma^{*})$: $su \in L(\mathbf{G^{op}})\ \&\ \theta(su) = \theta(s)t$.

- Como passo indutivo, para $t \in T^{+}_{conf}$, onde $|t| = n + 1$, $n \geq 1$:

  Seja $t = t'\tau$, onde $t' \in T^{+}_{conf}$ e $\tau \in T_{conf}$, e seja $s \in L(\mathbf{G^{op}})$: $\theta(s)t \in L(\mathbf{G^{ge}})$.

  Então $\exists u' \in \Sigma^{*}$, onde $su' \in L(\mathbf{G^{op}})$: $\theta(su') = \theta(s)t' \in L(\mathbf{G^{ge}})$.

  Como $su' \in L(\mathbf{G^{op}})$, e $\theta(s)t' \in L(\mathbf{G^{ge}})$ então $\theta(s)t'\tau \in L(\mathbf{G^{ge}})$.

  Então, por definição, $\exists u \in \Sigma^{*}$, onde $su'u \in L(\mathbf{G^{op}})$ e $\theta(su'u) = \theta(s)t'\tau = \theta(s)t$

□

Por outro lado, se houver uma cadeia $s \in L(\mathbf{G^{op}})$ cuja imagem ($\theta(s)$) seja prefixo de t, mas que seja impossível completar em uma cadeia t, significa que há algum evento não confiável em t. De acordo com a Proposição 2.3.4, essa condição pode levar a um bloqueio na linguagem do operador, mesmo que na linguagem do gerente tal bloqueio não seja observado.

Para que seja possível elaborar uma condição que seja menos restritiva do que a propriedade de observador do mapa repórter baseando-se no conjunto de eventos confiáveis, é necessário definir uma propriedade para garantir que com esse alfabeto sempre se consiga atingir cadeias marcadas de uma dada linguagem

5.2 ALFABETO SUFICIENTE PARA PREFIXO FECHAMENTO DE UMA LINGUAGEM

O conceito expresso nessa seção descreve um conjunto de eventos (alfabeto) que é suficiente para, a partir de prefixos de uma linguagem, se formarem cadeias completas nessa linguagem. Ou seja, no geral, para uma dada linguagem L, pode-se afirmar que pode existir um sub-alfabeto $\Sigma_S \subseteq \Sigma$, tal que qualquer prefixo de L pode ser completado em alguma cadeia de L apenas com eventos de Σ_S.

Definição 5.2.1. ***Alfabeto Suficiente Para Prefixo Fechamento:*** *Um alfabeto $\Sigma_S \subseteq \Sigma$ é suficiente para prefixo fechamento de uma linguagem $L \subseteq \Sigma^{*}$ se e somente se para toda cadeia $t \in \overline{L}$, existe uma cadeia $t' \in \Sigma_S^{*}$, tal que $tt' \in L$:*

$$(\forall t \in \overline{L})\ \exists t' \in \Sigma_S^{*} \textit{ tal que } tt' \in L.$$

Abaixo seguem algumas propriedades de um alfabeto suficiente para prefixo fechamento que exploram essa definição.

Propriedade I: Para $L \subseteq \Sigma^*$ (não necessariamente prefixo fechada), o alfabeto Σ é suficiente para prefixo fechamento de L.

Demonstração. Pela definição de prefixo fechamento, $(\forall t \in \overline{L})\ \exists t' \in \Sigma^* : tt' \in L$.

□

Propriedade II: Seja $L \subseteq \Sigma^*$, com $L = \overline{L}$ (linguagem prefixo fechada), o sub-alfabeto $\Sigma_S = \emptyset$ é suficiente para prefixo fechamento de L.

Demonstração. Como $L = \overline{L}$, para toda cadeia $t \in \overline{L}$, sempre existe $t' \in \Sigma_S^* = \emptyset^* = \{\epsilon\}$, tal que $tt' \in L$, pois $\forall t \in \overline{L}$, $t\epsilon = t \in L$.

□

Propriedade III: Seja um alfabeto Σ'_S suficiente para prefixo fechamento de $L \subseteq \Sigma^*$. Qualquer alfabeto $\Sigma_S \supseteq \Sigma'_S$ é também suficiente para prefixo fechamento de L.

Demonstração. Como Σ'_S é suficiente para prefixo fechamento de L, então $\forall t \in \overline{L}$, $\exists t' \in \Sigma'^*_S$ tal que $tt' \in L$. Assim, como $\Sigma'_S \subseteq \Sigma_S$, $\forall t \in \overline{L}$, $\exists t' \in \Sigma_S^*$ tal que $tt' \in L$.

□

A definição apresentada acima relaciona, de maneira generalizada, sub-alfabetos a linguagens, mas sem a devida interpretação do que pode resultar na representação de sistemas a eventos discretos. Já a Proposição 5.2.1, por sua vez, permite relacionar esse conceito à co-acessibilidade de um autômato, ou seja, afirma como um alfabeto suficiente para prefixo fechamento de uma linguagem marcada de um autômato pode garantir que sempre sejam atingidos estados marcados desse autômato.

Proposição 5.2.1. *Para um autômato $\mathbf{G}$ não bloqueante, seja Σ_S um alfabeto suficiente para prefixo fechamento da linguagem marcada $L_m(\mathbf{G})$. Então, a partir de todo estado de $\mathbf{G}$, sempre é possível atingir um estado marcado por meio de uma cadeia de Σ_S^*.*

Demonstração. Considerando o autômato $\mathbf{G}$ como não bloqueante, é verdade que $\overline{L_m(\mathbf{G})} = L(\mathbf{G})$. Como Σ_S é um alfabeto suficiente para prefixo fechamento de $L_m(\mathbf{G})$, então para todo $t \in L(\mathbf{G}) = \overline{L_m(\mathbf{G})}$ existe um $t' \in \Sigma_S^*$, tal que $tt' \in L_m(\mathbf{G})$. □

Como consequência da Proposição 5.2.1, se $\Sigma_S \subseteq \Sigma$ é suficiente para prefixo fechamento de $L_m(\mathbf{G})$, sendo $\mathbf{G}$ um autômato *trim* sobre Σ, esse autômato permanece co-acessível mesmo apagando transições com eventos de $\Sigma \setminus \Sigma_S$. Por outro lado, a proposição abaixo afirma que se um conjunto de eventos não controláveis Σ_u é

suficiente para prefixo fechamento de $L_m(\mathbf{G})$, então qualquer supervisor agindo sobre $\mathbf{G}$ é não bloqueante.

Proposição 5.2.2. *Seja $\mathbf{G}$ um autômato não bloqueante, com $L_m(\mathbf{G}) \subseteq \Sigma^*$ e $\Sigma_u \subseteq \Sigma$ um conjunto de eventos não controláveis. Se $\Sigma_u \subseteq \Sigma$ for suficiente para prefixo fechamento de $L_m(\mathbf{G})$, então Σ_u é suficiente para prefixo fechamento de qualquer $K \subseteq L_m(\mathbf{G})$ controlável e.r.a. $\mathbf{G}$.*

Demonstração. Seja $s \in \overline{K}$.

Como K é controlável e.r.a. $\mathbf{G}$, $\nexists u \in \Sigma_u^+$: $su \in L_m(\mathbf{G}) \setminus K$.

Como Σ_u é suficiente para prefixo fechamento de $L_m(\mathbf{G})$, $(\forall s \in \overline{K})\ \exists u \in \Sigma_u^+$: $su \in L_m(\mathbf{G})$.

Então, $(\forall s \in \overline{K})\ \exists u \in \Sigma_u^+$: $su \in K$, o que significa que Σ_u é suficiente para prefixo fechamento de K. □

5.3 CONTROLE HIERÁRQUICO NÃO BLOQUEANTE COM EVENTOS CONFIÁVEIS

Como analisado na associação de uma válvula de controle em série com uma válvula de bloqueio, a condição de mapa repórter observador é apenas suficiente e pode ser demasiadamente restritiva em alguns casos. Para determinadas estruturas é possível projetar especificações E^{ge} no nível do gerente que sejam hierarquicamente não bloqueantes, mesmo que o mapa repórter não possua essa propriedade, ou seja, mesmo que a estrutura possua eventos não confiáveis.

O teorema abaixo, como um dos resultados principais desta tese, permite flexibilizar a condição de observador para garantir o controle hierárquico não bloqueante, baseando-se nos conceitos de eventos confiáveis e alfabeto suficiente para prefixo fechamento apresentados acima. No entanto esse resultado está limitado a apenas um conjunto de especificações gerenciais, dependendo do conjunto de eventos confiáveis.

Teorema 5.3.1. *Seja uma estrutura hierárquica, formada por uma planta no nível operacional $\mathbf{G^{op}}$, seu mapa repórter associado θ, uma planta no nível gerencial $\mathbf{G^{ge}}$ e $T_{conf} \subseteq T$ o conjunto dos eventos confiáveis e.r.a. θ. Para uma especificação gerencial $E^{ge} \subseteq L_m(\mathbf{G^{ge}})$ não vazia e controlável e.r.a. $\mathbf{G^{ge}}$ e um supervisor não bloqueante $\mathcal{S}^{ge}$, tal que $L_m(\mathcal{S}^{ge}/\mathbf{G^{ge}}) = E^{ge}$, se o par $(\mathbf{G^{op}}, \theta)$ possuir consistência de controle estrita, se existir consistência de marcação entre $\mathbf{G^{op}}$ e $\mathbf{G^{ge}}$ e se o alfabeto T_{conf} for suficiente para prefixo fechamento de E^{ge}, pode-se garantir que:*

i) $\theta(L_m(\mathcal{S}^{ge\rightarrow op}/\mathbf{G^{op}})) = E^{ge}$ *e*

ii) O supervisor $\mathcal{S}^{ge\rightarrow op}$ será não bloqueante para $\mathbf{G^{op}}$.

Demonstração. **(Demonstração da afirmação i):**

Utilizando-se o resultado da Proposição 2.3.3 pode-se chegar ao controle supervisório hierárquico ótimo como expressado nessa afirmação.

(Demonstração da afirmação ii):

Um supervisor $\mathcal{S}^{ge\rightarrow op}$ é não bloqueante para $\mathbf{G^{op}}$ quando:

$$\overline{L_m(\mathcal{S}^{ge\rightarrow op}/\mathbf{G^{op}})} = L(\mathcal{S}^{ge\rightarrow op}/\mathbf{G^{op}})$$

Análise da igualdade:

($\subseteq$):

$$L_m(\mathcal{S}^{ge\rightarrow op}/\mathbf{G^{op}}) = L(\mathcal{S}^{ge\rightarrow op}/\mathbf{G^{op}}) \cap \theta^{-1}(E^{ge}) \subseteq L(\mathcal{S}^{ge\rightarrow op}/\mathbf{G^{op}})$$
$$\overline{L_m(\mathcal{S}^{ge\rightarrow op}/\mathbf{G^{op}})} \subseteq \overline{L(\mathcal{S}^{ge\rightarrow op}/\mathbf{G^{op}})} = L(\mathcal{S}^{ge\rightarrow op}/\mathbf{G^{op}})$$

($\supseteq$):

Seja $s \in L(\mathcal{S}^{ge\rightarrow op}/\mathbf{G^{op}})$, pela Proposição 2.3.2, segue-se que,

$$\theta(s) \in \theta(L(\mathcal{S}^{ge\rightarrow op}/\mathbf{G^{op}})) = L(\mathcal{S}^{ge}/\mathbf{G^{ge}}) = \overline{E^{ge}}$$

Seja T_{conf} o alfabeto dos eventos confiáveis de $\mathbf{G^{ge}}$. Como T_{conf} é suficiente para prefixo fechamento de E^{ge}, a partir da proposição 5.2.1 pode-se afirmar que

$$\exists t \in T^*_{conf}, \text{ tal que } \theta(s)t \in E^{ge}$$

Pela proposição 5.1.2, como $t \in T^*_{conf}$ é verdade que $\exists u \in \Sigma^*$, tal que

$$su \in L(\mathbf{G^{op}}) \ \& \ \theta(su) = \theta(s)t \in E^{ge}.$$

Como E^{ge} é controlável e.r.a. $\mathbf{G^{ge}}$ e o par ($\mathbf{G^{op}}$, θ) não possui palavras vocais parceiras, então:

$$su \in L(\mathcal{S}^{ge\rightarrow op}/\mathbf{G^{op}}).$$

Como existe consistência de marcação entre $\mathbf{G^{op}}$ e $\mathbf{G^{ge}}$ e como $\theta(su) \in E^{ge} \subseteq L_m(G^{ge})$, afirma-se que

$$su \in L(\mathcal{S}^{ge\rightarrow op}/\mathbf{G^{op}}) \cap \theta^{-1}(E^{ge}) = L_m(\mathcal{S}^{ge\rightarrow op}/\mathbf{G^{op}})$$

e então

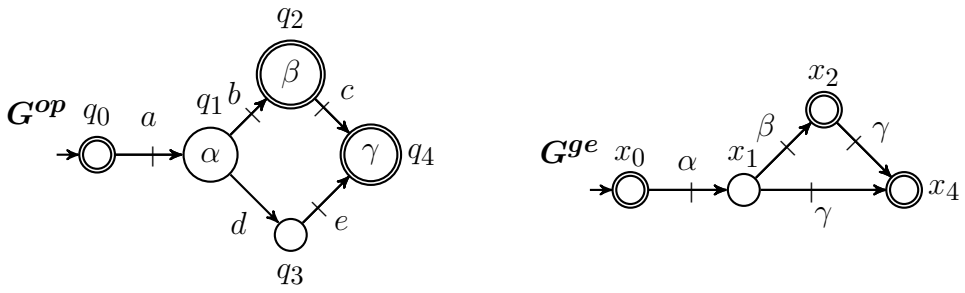
$$s \in \overline{L_m(\mathcal{S}^{ge\rightarrow op}/\mathbf{G^{op}})}$$

□

O resultado acima, apesar da vantagem de flexibilizar a condição de observador do mapa repórter, depende da especificação gerencial analisada, e não somente das plantas do operador e do gerente na estrutura hierárquica. Por essa razão, esse resultado é válido para um dado conjunto de especificações gerenciais controláveis dependendo do alfabeto de eventos confiáveis.

Exemplo 5.3.1. *Seja $\mathbf{G^{op}}$ (Figura 69 - a) uma planta do operador sobre o alfabeto $\Sigma = \{a, b, c, d, e\}$, que vocaliza eventos em $T = \{\alpha, \beta, \gamma\}$ e $\theta : L(\mathbf{G^{op}}) \to T^*$ seu mapa repórter associado. O autômato vocalizador $\mathbf{G^{ge}}$ consiste em sua abstração. O evento abstrato β é não confiável e.r.a. θ, pois com a ocorrência de d em $\mathbf{G^{op}}$, é atingido o estado $q3$, de onde não é mais possível alcançar um estado que vocaliza β. Assim, um supervisor gerencial que depende de β para atingir um estado marcado pode conter bloqueio. O conjunto formado pelos eventos confiáveis é $T_{conf} = \{\alpha, \gamma\}$.*

Figura 69 – Estrutura em que o mapa repórter não é observador: (a) planta do operador $\mathbf{G^{op}}$ e (b) planta gerencial $\mathbf{G^{ge}}$.



(a) (b)

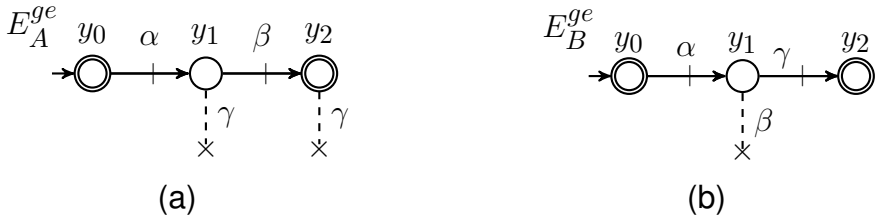
Fonte: Elaborado pelo autor.

Verifica-se que o par ($\mathbf{G^{op}}$, θ) possui consistência de controle estrita e que há consistência de marcação entre $\mathbf{G^{op}}$ e $\mathbf{G^{ge}}$. Como θ não é observador, pelo Teorema 5.3.1 pode-se garantir controle hierárquico não bloqueante dependendo da especificação gerencial analisada, ou seja, dependendo se T_{conf} for suficiente para prefixo fechamento da especificação.

Como exemplo, a especificação no nível gerencial E_A^{ge} (Figura 70 - a) desabilita γ após a ocorrência de α e $\alpha\beta$. Percebe-se que T_{conf} não é suficiente para prefixo fechamento dessa especificação, pois não atinge-se o estado marcado $y2$ apenas com eventos desse alfabeto, portanto não há garantia de ausência de bloqueio nessa estrutura. Por sua vez, a especificação E_B^{ge} (Figura 70 - b) desabilita β depois da ocorrência de α. Para essa especificação, o Teorema 5.3.1 garante um controle supervisório hierárquico não bloqueante, pois, além das condições citadas acima, T_{conf} é suficiente para prefixo fechamento dessa linguagem.

Por outro lado, explorando a Proposição 5.2.2, o Corolário 5.3.1 abaixo impõe duas novas condições, associadas à confiabilidade dos eventos abstratos não controláveis, que dependem somente da planta do operador e do gerente na estrutura hierárquica e do mapa repórter associado. Dessa forma, para qualquer especificação não vazia e controlável no nível do gerente, pode-se garantir o controle supervisório hierárquico não bloqueante para estruturas em que o mapa repórter não é observador.

Figura 70 – Duas especificações gerenciais: (a) o evento γ é desabilitado depois das cadeias α e $\alpha\beta$, (b) o evento β é desabilitado depois da ocorrência de α.



Fonte: Elaborado pelo autor.

Corolário 5.3.1. *Seja uma estrutura hierárquica, formada por uma planta no nível operacional $\mathbf{G^{op}}$, seu mapa repórter associado θ e uma planta no nível gerencial $\mathbf{G^{ge}}$. Seja $T_u \subseteq T$, tal que todo $\tau \in T_u$ é um evento confiável e T_u é suficiente para prefixo fechamento de $L_m(\mathbf{G^{ge}})$. Se o par $(\mathbf{G^{op}}, \theta)$ possuir consistência de controle estrita e existir consistência de marcação entre $\mathbf{G^{op}}$ e $\mathbf{G^{ge}}$, então para toda especificação $E^{ge} \subseteq L_m(\mathbf{G^{ge}})$ não vazia e controlável em relação a $\mathbf{G^{ge}}$ e um supervisor não bloqueante $\mathcal{S}^{ge}$, tal que $L_m(\mathcal{S}^{ge}/\mathbf{G^{ge}}) = E^{ge}$, o supervisor $\mathcal{S}^{ge \to op}$ será não bloqueante para $\mathbf{G^{op}}$.*

Demonstração. Como T_u é suficiente para prefixo fechamento de $L_m(\mathbf{G^{ge}})$, pela Proposição 5.2.2, T_u é suficiente para prefixo fechamento de qualquer $E^{ge} \subseteq L_m(\mathbf{G^{ge}})$ controlável e.r.a. $\mathbf{G^{ge}}$.

Então, nessas condições prova-se no teorema 5.3.1 que $\mathcal{S}^{ge \to op}$ é não bloqueante para $\mathbf{G^{op}}$. □

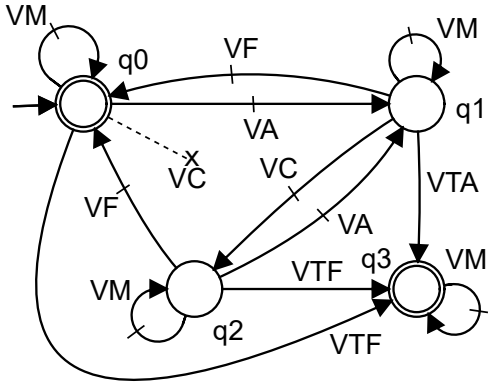
Exemplo 5.3.2. ***Arquitetura não Bloqueante para Válvula Equivalente de Controle***

Este exemplo se baseia no modelo de abstração de uma estrutura em série de uma válvula de controle com uma válvula de bloqueio, conforme a Figura 65 da Seção 4.4. No nível do operador constam os modelos individuais das válvulas, enquanto que no nível gerencial está o modelo da válvula equivalente. Os eventos VA, VF, VC, VTA e VTF significam respectivamente válvula abre, válvula fecha, válvula controla, válvula trava aberta e válvula trava fechada. Conforme apresentado na Figura 64, o evento VC é não confiável, pois considerando que a válvula de controle trava aberta, o que é representado pelo evento silencioso $V1TA$, o evento VC não é mais elegível, o que não é observável para o gerente. Dessa forma, o alfabeto dos eventos não controláveis é $T_u = \{VTA, VTF\}$, contido no alfabeto dos eventos confiáveis dado por $T_{conf} = \{VA, VF, VTA, VTF\}$.

Considerando somente o modelo abstrato da válvula equivalente no nível do gerente, é proposta a especificação gerencial apresentada na Figura 71. Nesse exemplo, a título de ilustração do emprego dos conceitos apresentados, não é considerado o processo industrial. No estado inicial, $q0$, a válvula encontra-se fechada e sem operar.

Nesse estado, a especificação desabilita o evento VC, proibindo que a válvula entre no modo de controle antes de abrir totalmente (evento VA). Observando o modelo apresentado na figura, percebe-se que, a partir de qualquer estado, é possível atingir algum estado marcado com eventos de T_{conf}. Dessa forma, para a especificação analisada, atinge-se todas as condições do Teorema 5.3.1 para garantir o controle supervisório hierárquico não bloqueante.

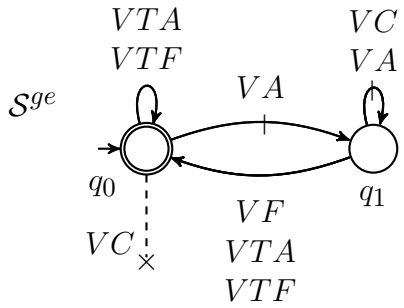
Figura 71 – Autômato que reconhece especificação gerencial E^{ge} para abstração de uma válvula de controle em série com uma de bloqueio.



Fonte: Elaborado pelo autor.

Por outro lado, observa-se que o alfabeto T_u é formado unicamente por eventos confiáveis. Como T_u é suficiente para prefixo fechamento da linguagem marcada da planta gerencial, então, aplicando-se o Corolário 5.3.1, para qualquer especificação gerencial controlável $E^{ge} \subseteq L_m(\mathbf{G^{ge}})$ garante-se o controle supervisório hierárquico não bloqueante. Um supervisor $\mathcal{S}^{ge}$ que implementa a especificação E^{ge} é mostrado na Figura 72.

Figura 72 – $\mathcal{S}^{ge}$: Supervisor gerencial que implementa a especificação E^{ge} para abstração de uma válvula de controle em série com uma de bloqueio.



Fonte: Elaborado pelo autor.

5.4 DISCUSSÃO

Este capítulo reexamina a definição de mapa repórter observador e a analisa na perspectiva dos eventos individuais. A partir desse olhar, é proposta uma nova definição que diz respeito à confiabilidade dos eventos de alto nível, no sentido de que, mesmo que seja um evento elegível, sua ocorrência pode passar a ser incerta devido a algum trecho silencioso do operador. Por outro lado, este capítulo analisa o fechamento de linguagens marcadas por meio de sub-alfabetos dessas linguagens, o que foi definido como alfabetos suficientes para prefixo fechamento de uma linguagem.

Essas duas definições possibilitam o desenvolvimento de novas condições para construção de supervisores não bloqueantes em uma estrutura hierárquica de dois níveis, mesmo para casos em que não atinge-se a propriedade de mapa repórter observador.

Por fim, retoma-se o exemplo do capítulo 4 em que uma válvula de controle é associada em série com uma válvula de bloqueio e a propriedade de mapa repórter observador não é atingida para possibilitar o projeto de um supervisor não bloqueante. Por outro lado, no presente capítulo esse exemplo é resolvido empregando-se o resultado de que o conjunto dos eventos confiáveis da planta de alto nível é suficiente para prefixo fechamento da especificação projetada, o que garante o controle supervisório hierárquico ótimo e não bloqueante.

6 ABORDAGEM INTERNÍVEIS PARA ESTRUTURA HIERÁRQUICA COM COMPOSIÇÃO NO GERENTE

No capítulo anterior abordou-se a estrutura clássica de controle supervisório hierárquico com uma planta e um mapa de desabilitações para o nível do operador e uma planta e um supervisor para o nível gerencial. Neste capítulo será adicionado a essa estrutura um modelo sincronizado no nível gerencial, ou seja, um modelo composto com a planta do gerente. Nessa estrutura, a linguagem do gerente, que é formada por eventos abstratos, é então sincronizada com um novo modelo inserido no nível gerencial. Dessa forma, para a devida coerência desse tipo de sincronização deve-se observar também as cadeias do operador. Como os eventos do gerente são gerados por meio de vocalizações, uma cadeia do operador que vocaliza um evento para o gerente somente pode ocorrer se esse evento estiver sincronizado na composição do gerente. Nessa nova abordagem, percebe-se que os modelos do operador e do gerente são, de certa forma, incompletos, pois não levam em conta a sincronização com o novo modelo composto com o gerente. Em outras palavras, o modelo do operador contém cadeias que, na prática, para realmente ocorrerem dependem do modelo composto no gerente devido à sincronização.

Como exemplo, conforme o apresentado na Seção 4.5, toma-se um processo industrial comandado por um modelo abstrato de duas válvulas em série. Dentre os modelos do processo industrial consta a preempção da válvula, que é uma hipótese sobre o comportamento em que assume-se que entre dois eventos não controláveis, seja mudanças de nível no tanque, seja travamentos da válvula, sempre há uma ação da válvula. Com isso, um evento de travamento da válvula equivalente somente pode ocorrer de forma sincronizada com o modelo da preempção. Dessa forma, os eventos do operador que levam ao travamento da válvula, mesmo se forem elegíveis, somente ocorrem de forma sincronizada com o modelo do processo industrial no gerente.

A estrutura hierárquica com composição no gerente, no entanto, já é uma abordagem utilizada na literatura (PU, 2000; SEOW, 2014). Em contrapartida, esses autores impõem a restrição de que não pode haver sincronização de eventos no nível do gerente, o que impossibilita solucionar alguns tipos de problemas como os tratados nesta tese. De modo a abordar formalmente esse tipo de sincronização, é necessário criar uma nova operação de composição síncrona entre um autômato vocalizador, que representa a planta do operador, e um autômato que representa o novo modelo composto no gerente, conforme apresentado nas próximas seções.

Neste capítulo é proposta a abordagem formal interníveis, que permite solucionar o problema citado. A composição paralela interníveis é criada com o objetivo de representar a sincronização entre eventos vocalizados de uma planta operacional com eventos de um modelo composto no nível do gerente. Mostra-se que com a composição interníveis pode-se chegar a uma estrutura equivalente à estrutura hierár-

quica clássica, com um operador e um gerente. Por fim, como resultado principal, é demonstrado que, ao atingir certas condições na planta do operador, pode-se garantir o controle hierárquico ótimo e não bloqueante mesmo sem o custo computacional de calcular a composição interníveis.

Uma primeira propriedade de consistência a ser buscada para a planta do operador diz respeito à controlabilidade dos trechos silenciosos do operador. Abaixo é definida uma nova propriedade denominada de *consistência de controle persistente*, que leva em conta que para os trechos silenciosos controláveis, o evento controlável deve ser sempre o último da respectiva cadeia. A partir dessa propriedade, este capítulo explora a consistência de controle estrita na composição interníveis, como discutido a seguir.

6.1 CONSISTÊNCIA DE CONTROLE PERSISTENTE

Esta seção explora uma condição primeiramente definida em Zhong (1992 apud WONG; WONHAM, 1998), expressa pela equação 6.1 e chamada pelos autores de liberdade de atraso de controle (*control-delay freedom*). Essa condição estipula que sempre que um evento abstrato é controlável, deve ser controlável também o último evento no operador que atinge o estado em que esse evento abstrato é vocalizado. Essa condição é utilizada também em Schmidt *et al.* (2008) para definir a controlabilidade dos eventos abstratos em um autômato de Mealy. A consistência de controle persistente garante que as decisões de controle continuam válidas qualquer que seja o momento em que são tomadas por C_{op}. Ou seja, mesmo que uma decisão de controle não seja tomada imediatamente ao atingir um estado vocalizador, ela continua válida ao longo do trecho silencioso.

Definição 6.1.1. ***Consistência de Controle Persistente:*** *Uma planta do operador $\mathbf{G^{op}}$ e seu mapa repórter associado θ possuem consistência de controle persistente se o par ($\mathbf{G^{op}}, \theta$) possui consistência de controle e*

$$\forall \tau_c \in T_c, \mathcal{X}_{\tau_c} \subseteq \Sigma^* \Sigma_c \tag{6.1}$$

A condição dessa definição é mais forte do que a consistência de controle estrita. Demonstra-se abaixo que ao existir consistência de controle persistente consegue-se também consistência de controle estrira na estrutura.

Proposição 6.1.1. ***Consistência de controle persistente implica em consistência de controle estrita:*** *Em uma estrutura hierárquica formada por uma planta do operador $\mathbf{G^{op}}$, seu mapa repórter associado θ e uma planta do gerente $\mathbf{G^{ge}}$, se o par ($\mathbf{G^{op}}, \theta$) possui consistência de controle persistente, então ($\mathbf{G^{op}}, \theta$) possui consistência de controle estrita.*

Demonstração. Primeiramente demonstra-se que para o par $(\mathbf{G^{op}}, \theta)$ com consistência de controle persistente não existem palavras vocais parceiras. Pela definição 2.3.9, dois trechos silenciosos $s_1 = s'\sigma_c s'' v_1$ e $s_2 = s'\sigma_c s'' v_2$, onde $s' \in \Sigma^*$, $\sigma_c \in \Sigma_c$, $s'' \in \Sigma^*$, $v_1 \in \Sigma^*$, $v_2 \in \Sigma^*$ são considerados parceiros se ao menos uma das terminações é não controlável: $v_1 \in \Sigma_u^+$ ou $v_2 \in \Sigma_u^+$.

Mas, como o par $(\mathbf{G^{op}}, \theta)$ possui consistência de controle persistente, $\forall \tau_c \in T_c, \mathcal{X}_{\tau_c} \subseteq \Sigma^*\Sigma_c$. Assim, não é possível que exista algum v_1 ou v_2 que pertença a Σ_u^+ e, portanto, não há palavras vocais parceiras.

Com isso, segundo a definição 2.3.10, como o par $(\mathbf{G^{op}}, \theta)$ possui consistência de controle e não existem palavras vocais parceiras, então o par $(\mathbf{G^{op}}, \theta)$ possui consistência de controle estrita.

□

Dessa forma, para uma estrutura hierárquica com consistência de controle persistente, garante-se que é atingida consistência hierárquica.

Corolário 6.1.1. ***Consistência de controle persistente implica em consistência hierárquica:*** *Em uma estrutura hierárquica formada por uma planta do operador* $\mathbf{G^{op}}$*, seu mapa repórter associado* θ *e uma planta do gerente* $\mathbf{G^{ge}}$*, se o par (*$\mathbf{G^{op}}, \theta$*) possui consistência de controle persistente, então existe consistência hierárquica entre* $\mathbf{G^{op}}$ *e* $\mathbf{G^{ge}}$*.*

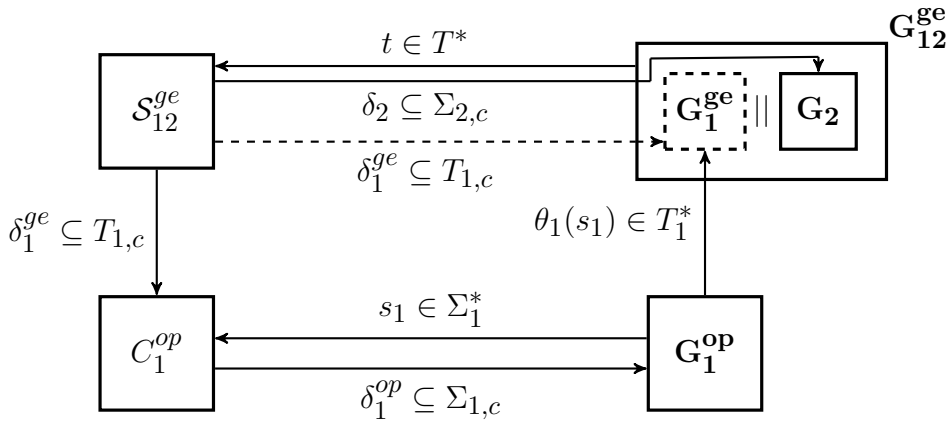
Demonstração. Das proposições 2.3.2 e 6.1.1 chega-se a consistência hierárquica entre $\mathbf{G^{op}}$ e $\mathbf{G^{ge}}$. □

A seguir, define-se a estrutura com composição no gerente e como a propriedade de consistência de controle persistente está relacionada às exigências para o controle hierárquico não bloqueante.

6.2 ESTRUTURA HIERÁRQUICA COM COMPOSIÇÃO NO GERENTE

Nessa estrutura, em um primeiro momento, a planta do gerente será denominada de $\mathbf{G_{12}^{ge}}$. Essa planta consiste na composição de um modelo abstrato $\mathbf{G_1^{ge}}$ com um modelo $\mathbf{G_2}$, ou seja $\mathbf{G_{12}^{ge}} = \mathbf{G_1^{ge}} || \mathbf{G_2}$. Para uma especificação gerencial $E_{ge} \subseteq L_m(\mathbf{G^{ge}})$ não vazia e controlável em relação a $\mathbf{G_{12}^{ge}}$ é obtido um supervisor monolítico não bloqueante $\mathcal{S}^{ge}$. A Planta do operador é definida como um autômato vocalizador $\mathbf{G_1^{op}} = \{Q_1^{op}, \Sigma_1, f_1, q_{0,1}, Q_{1,m}^{op}, T_1 \cup \{\tau_0\}, \omega_1\}$, onde T_1 é o alfabeto de $\mathbf{G_1^{ge}}$ e τ_0 é o evento silencioso. $\mathbf{G_2} = \{Q_2, T_1 \cup \Sigma_2, f_2, q_{0,2}, Q_{2,m}\}$ é um modelo no nível do gerente, que contém eventos exclusivos de um alfabeto próprio (Σ_2), além de todos os eventos de $\mathbf{G_1^{ge}}$ (T_1). Sem perda de generalidade, para fins de simplificar a notação, assume-se que todos os eventos vocalizados por $\mathbf{G_1^{op}}$ estejam no alfabeto de $\mathbf{G_2}$.

Figura 73 – Estrutura hierárquica com composição no gerente.



Fonte: Elaborado pelo autor.

Essa estrutura sincroniza as linguagens no nível do gerente, ou seja, sincroniza os eventos de $\mathbf{G_2}$ com os eventos de $\mathbf{G_1^{ge}}$ (que são eventos abstratos) e que são sinalizados, por sua vez, por $\mathbf{G_1^{op}}$. Ou seja, para um evento do gerente ocorrer, esse deve estar elegível em $\mathbf{G_2}$ e deve também ser possível de ser vocalizado em alguma transição elegível em $\mathbf{G_1^{op}}$. Dessa forma, se um evento de baixo nível em $\mathbf{G_1^{op}}$ leva a um estado vocalizador, esse não pode ocorrer se o mesmo evento vocalizado por esse estado não estiver elegível em $\mathbf{G_2}$. Por essa razão não faz sentido um evento de T_1 ocorrer em $\mathbf{G_2}$ se não tiver sido vocalizado por $\mathbf{G_1^{op}}$.

Definição 6.2.1. ***Estrutura hierárquica com composição no gerente:*** *Uma estrutura hierárquica com composição no gerente, conforme ilustrado na Figura 73, pode ser definida como uma tupla*

$$(\mathbf{G_1^{op}}, \mathbf{G_2}, C_1^{op}, \mathcal{S}^{ge}), \text{ onde}$$

$\mathbf{G_1^{op}} = (Q_1^{op}, \Sigma_1, f_1, q_{0,1}, Q_{1,m}^{op}, T_1 \cup \{\tau_0\}, \omega_1)$, *com* $\Sigma_1 = \Sigma_{1,c} \cup \Sigma_{1,u}$ *e* $T_1 = T_{1,c} \cup T_{1,u}$*, é uma planta operacional,* $\mathbf{G_2} = (Q_2, T_1 \cup \Sigma_2, f_2, q_{0,2}, Q_{2,m}^{op})$*, com* $\Sigma_2 = \Sigma_{2,c} \cup \Sigma_{2,u}$*, é uma planta,* $C_1^{op} : L(\mathbf{G_1^{op}}) \times 2^{T_{1,c}} \to 2^{\Sigma_{1,c}}$ *é o mapa de desabilitações de* $\mathbf{G_1^{op}}$ *e* $\mathcal{S}^{ge} : L(\mathbf{G_{12}^{ge}}) \to 2^{T_c}$ *é supervisor gerencial. Para o modelo do gerente,* $\mathbf{G_{12}^{ge}} = \mathbf{G_1^{ge}} || \mathbf{G_2}$ *sobre o alfabeto* $T = T_c \cup T_u$*, onde* $T_c = T_{1,c} \cup \Sigma_{2,c}$*,* $T_u = T_{1,u} \cup \Sigma_{2,u}$ *e* $\mathbf{G_1^{ge}}$ *é a abstração de* $\mathbf{G_1^{op}}$*.*

Nessa estrutura, o supervisor gerencial deve ser capaz de realizar desabilitações reais em $\Sigma_{2,c}$, no nível do gerente, enquanto que envia comandos virtuais de desabilitação em $T_{1,c}$ para o nível do operador. Entretanto, nesse tipo de estrutura, o modelo de $\mathbf{G_1^{op}}$ é incompleto no sentido de que algumas de suas cadeias somente podem ocorrer a depender da sincronização de sua abstração (em $\mathbf{G_1^{ge}}$) com o modelo de $\mathbf{G_2}$. O problema nessa dinâmica é que a sincronização de eventos entre $\mathbf{G_1^{ge}}$ e $\mathbf{G_2}$ interfere nas sequências de eventos em $\mathbf{G_1^{op}}$, o que não é possível representar utilizando a operação de composição paralela de linguagens, nem mesmo a composição

de sistemas vocalizados definida em Pu (2000). Os resultados encontrados em Pu (2000) e Seow (2014) não são capazes de resolver essa questão pois ambos autores assumem que os modelos no nível do gerente sejam completamente disjuntos.

6.3 ABORDAGEM FORMAL INTERNÍVEIS

Para ser possível sincronizar a linguagem operacional de $\mathbf{G_1^{op}}$ com a linguagem gerencial de $\mathbf{G_2}$, por meio da vocalização de eventos abstratos compartilhados, é necessário definir uma nova operação, denominada de composição paralela interníveis ($||^I$), que tem como entrada $\mathbf{G_1^{op}}$ e $\mathbf{G_2}$, conforme definição abaixo. Com essa operação, todo evento gerencial de $\mathbf{G_1^{op}}$ é também um evento de $\mathbf{G_2}$. Dessa forma, para que um evento gerencial de $\mathbf{G_1^{op}}$ possa ocorrer, esse deve ser vocalizável em alguma cadeia operacional de $\mathbf{G_1^{op}}$ e, simultaneamente, estar elegível em $\mathbf{G_2}$. Essa operação caracteriza a sincronização de eventos no nível gerencial. Se em $\mathbf{G_1^{op}}$ houver uma cadeia que vocaliza um certo evento gerencial, mas esse evento não estiver elegível em $\mathbf{G_2}$, então $\mathbf{G_1^{op}}$ não pode evoluir por meio dessa cadeia. Esse mesmo tipo de sincronização de eventos gerenciais também ocorre em um processo industrial controlado por um circuito de válvulas, como o apresentado nos capítulos anteriores, ao se levar em conta o modelo da preempção. Esse modelo garante que, por exemplo, um evento de travamento da válvula equivalente, que é um evento abstrato, não ocorra imediatamente após uma mudança de nível do tanque, pois sempre ocorre a ação dos atuadores entre esses dois eventos.

Essa nova operação difere da composição síncrona de sistemas vocalizados encontrada em Pu (2000), pois o autor considera que os modelos envolvidos devem ter os alfabetos disjuntos no nível do operador e também no nível do gerente o que não permite a ocorrência da sincronização de eventos. Também pode ser feito um paralelo com o trabalho de Queiroz e Cury (2005), em que é definido o produto síncrono de autômatos com marcação colorida. Nesse caso, a função de saída relaciona diferentes tipos de marcação (cores) a diferentes classes de tarefas, o que é utilizado para definições de prefixo fechamento e propriedades de vivacidade para sistemas multitarefas, não sendo contextualizada a questão de sincronização de eventos no nível gerencial.

Definição 6.3.1. ***Composição paralela interníveis:*** *A composição paralela interníveis do autômato vocalizador* $\mathbf{G_1^{op}} = (Q_1^{op}, \Sigma_1, f_1, q_{0,1}, Q_{1,m}^{op}, T_1 \cup \{\tau_0\}, \omega_1)$*, onde* $\Sigma_1 = \Sigma_{1,c} \cup \Sigma_{1,u}$*, e do autômato* $\mathbf{G_2} = (Q_2, T_1 \cup \Sigma_2, f_2, q_{0,2}, Q_{2,m})$*, onde* $T_1 = T_{1,c} \cup T_{1,u}$*,* $\Sigma_2 = \Sigma_{2,c} \cup \Sigma_{2,u}$*,* τ_0 *é o evento silencioso, e* $\Sigma_1 \cap \Sigma_2 = \emptyset$*, é definida pelo autômato vocalizador:*

$$\mathbf{G^{op}} = \mathbf{G_1^{op}}||^I\mathbf{G_2} = Ac(Q_1^{op} \times Q_2 \times T_0, \Sigma, f, (q_{0,1}, q_{0,2}, \tau_0), Q_{1,m}^{op} \times Q_{2,m} \times T_0, T_0, \omega),$$

onde $\Sigma = \Sigma_1 \cup \Sigma_2$*,* $T_0 = T \cup \{\tau_0\}$*,* $T = T_1 \cup \Sigma_2$*.*

A função de transição de estados $f : Q^{op} \times \Sigma \to Q^{op}$*, onde* $Q^{op} = Q_1^{op} \times Q_2 \times T_0$*, é definida como:*

$$f((q_1, q_2, \tau'), \sigma) = \begin{cases} (f_1(q_1, \sigma), q_2, \tau_0), \, se \; f_1(q_1, \sigma)! \; e \; \omega_1(f_1(q_1, \sigma)) = \tau_0 \\ (f_1(q_1, \sigma), f_2(q_2, \tau), \tau), \, se \; f_1(q_1, \sigma)!, \, \omega_1(f_1(q_1, \sigma)) = \tau \; e \; f_2(q_2, \tau)! \\ (q_1, f_2(q_2, \sigma), \sigma), \, se \; f_2(q_2, \sigma)! \; e \; \sigma \in \Sigma_2 \\ indefinida, \, senão \end{cases}$$

onde $\tau \neq \tau_0$*.*

Essa função pode ter sua versão estendida para cadeias $\hat{f} : Q^{op} \times \Sigma^* \to Q^{op}$ *definida como:* $\hat{f}(q, \epsilon) = q$ *e*

$$\hat{f}(q, s\sigma) = f(\hat{f}(q, s), \sigma).$$

A linguagem gerada resultante da composição pode ser colocada de maneira genérica como:

$$L(\mathbf{G^{op}}) = \{s \in \Sigma^* : \hat{f}((q_{0,1}, q_{0,2}, \tau_0), s)!\}.$$

A função de saída $\omega : Q^{op} \to T_0$ *é definida como:*

$$\omega((q_1, q_2, \tau)) = \tau.$$

Observa-se que essa operação tem complexidade $\mathcal{O}(|Q_1^{op}|.|Q_2|.|T_0|)$.

O mapa repórter de $\mathbf{G^{op}}$, conforme a definição 2.3.1, é construído com base na função de saída ω do autômato vocalizador $\mathbf{G^{op}}$. Esse mapa é definido de maneira recursiva como a função $\theta : L(\mathbf{G^{op}}) \to T^*$, onde $\theta(\epsilon) = \epsilon$ e

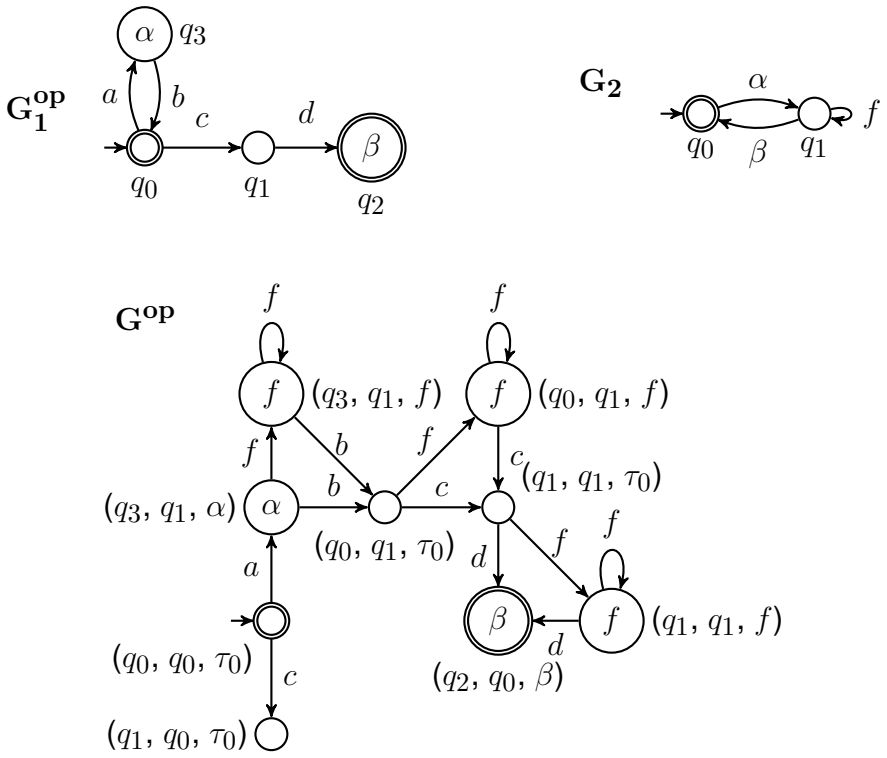
$$\theta(s\sigma) = \begin{cases} \theta(s) & se \; w(f(q_0, s\sigma)) = \tau_0 \quad ou \\ \theta(s)w(f(q_0, s\sigma)) & se \; w(f(q_0, s\sigma)) \neq \tau_0 \end{cases}$$

Exemplo 6.3.1. ***Aplicação da composição paralela interníveis:*** *Neste exemplo os modelos abaixo aplicam-se a uma estrutura hierárquica com composição interníveis conforme definição 6.2.1. Na Figura 74,* $\mathbf{G_1^{op}}$ *é um autômato vocalizador que possui eventos abstratos compartilhados com o autômato* $\mathbf{G_2}$*.*

Para um autômato vocalizador resultante da composição interníveis, pode-se dizer que as cadeias $s \in \Sigma_1^*$ são traduzidas como cadeias de eventos abstratos, enquanto que cada evento $\sigma \in \Sigma_2$ é traduzido como ele próprio para o nível acima. Dessa forma, considerando a definição 6.3.1, o mapa repórter pode ser reescrito como $\theta : L(\mathbf{G^{op}}) \to T^*$, onde $\theta(\epsilon) = \epsilon$ e

$$\theta(s\sigma) = \begin{cases} \theta(s) & se \; \sigma \in \Sigma_1, \, f_1(q_1, \sigma)! \; e \; w_1(f_1(q_1, \sigma)) = \tau_0 \quad ou \\ \theta(s)\tau & se \; \sigma \in \Sigma_1, \, f_1(q_1, \sigma)!, \omega(f_1(q_1, \sigma)) = \tau \neq \tau_0 \; e \; f_2(q_2, \tau)! \quad ou \\ \theta(s)\sigma & se \; \sigma \in \Sigma_2 \; e \; f_2(q_2, \sigma)! \end{cases} \tag{6.2}$$

Figura 74 – Exemplo de aplicação da composição paralela interníveis. $\mathbf{G_1^{op}}$: autômato vocalizador; $\mathbf{G_2}$: autômato no nível do gerente.



Fonte: Elaborado pelo autor.

onde $q_0 = (q_{0,1}, q_{0,2}, \tau_0)$ e $\hat{f}(q_0, s) = (q_1, q_2, \tau)$.

A θ-imagem inversa é definida como a função $\theta^{-1} : 2^{T^*} \rightarrow 2^{L(\mathbf{G^{op}})}$:

$$\theta^{-1}(L') = \{s \in L(\mathbf{G^{op}}) : \theta(s) \in L'\}, \tag{6.3}$$

onde $L' \subseteq T^*$.

Assim, o modelo abstrato do gerente, $\mathbf{G^{ge}}$ é obtido, a partir do modelo $\mathbf{G^{op}}$, aplicando o mapa repórter θ. O supervisor gerencial $\mathcal{S}^{ge} : L(\mathbf{G^{ge}}) \rightarrow 2^{T_c}$, onde $T_c = T_{1,c} \cup \Sigma_{2,c}$, pode ser calculado seguindo a abordagem Ramadge-Wonham (RAMADGE; WONHAM, 1989). As desabilitações de $T_{1,c}$ agem de forma virtual no modelo de $\mathbf{G^{ge}}$ e são enviadas para execução real ao mapa de desabilitações do operador C_1^{op} : $L(\mathbf{G_1^{op}}) \times 2^{T_{1,c}} \rightarrow 2^{\Sigma_{1,c}}$. As desabilitações em $\Sigma_{2,c}$, agem diretamente em $\mathbf{G_2}$ por meio do supervisor gerencial.

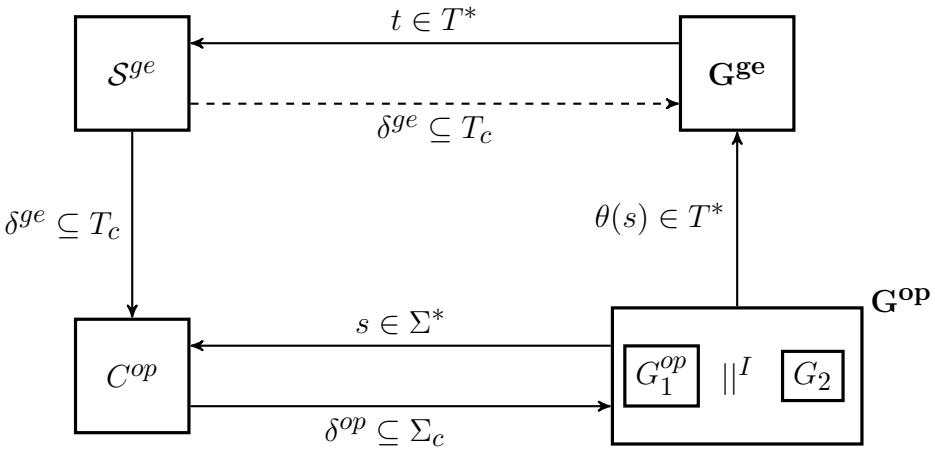
O supervisor induzido é definido como a função $\mathcal{S}^{ge \rightarrow op} : L(\mathbf{G^{op}}) \rightarrow 2^{\Sigma_c}$, que lê elementos de $L(\mathbf{G^{op}}) = L(\mathbf{G_1^{op}} ||^I \mathbf{G_2})$ e leva a desabilitações em 2^{Σ_c}, a estrutura de controle de $\mathbf{G^{op}}$. Destaca-se que esse supervisor não pode se basear somente na linguagem de $\mathbf{G_1^{op}}$, pois as desabilitações para essa planta dependem da sincronização com o modelo de $\mathbf{G_2}$. Portanto o supervisor induzido é definido como:

$$\mathcal{S}^{ge \rightarrow op}(s^{op}) := S_1^{ge \rightarrow op}(s^{op}) \cup S_2^{ge}(s^{op}) \tag{6.4}$$

onde $S_1^{ge \to op}(s^{op}) = C_1^{op}(s_1^{op}, \mathcal{S}^{ge}(\theta(s^{op})) \cap T_1)$ é o supervisor induzido que age sobre $\mathbf{G_1^{op}}$, com $s_1^{op} = P_{\Sigma_1}(s^{op})$, e $S_2^{ge}(s^{op}) = \mathcal{S}^{ge}(\theta(s^{op})) - T_1$ é o supervisor induzido que age sobre $\mathbf{G_2}$ e $s^{op} \in L(\mathbf{G^{op}})$.

Dessa forma, a partir da definição da composição paralela interníveis, a estrutura hierárquica com composição no gerente pode ser representada conforme a estrutura da Figura 75. Com isso, o supervisor do gerente age sobre o modelo de $\mathbf{G^{ge}}$ de forma virtual, e também de forma real, e a composição interníveis soluciona o problema da sincronização de linguagens no nível do gerente.

Figura 75 – Estrutura hierárquica com composição interníveis.



Fonte: Elaborado pelo autor.

A linguagem gerada pela operação de composição paralela interníveis é definida sobre o alfabeto $\Sigma = \Sigma_1 \cup \Sigma_2$. Ou seja, é formada pelos eventos de baixo nível de $\mathbf{G_1^{op}}$ (Σ_1) e pelos eventos gerenciais de $\mathbf{G_2}$ que não são vocalizáveis por $\mathbf{G_1^{op}}$ (Σ_2), já que esses eventos gerenciais de Σ_2 também podem ser considerados operacionais. Como o modelo resultante encontra-se no nível do operador, os eventos abstratos devem ser traduzidos a um nível abaixo por meio da operação da θ-imagem inversa.

Proposição 6.3.1. ***Linguagem gerada na composição interníveis:*** *A linguagem gerada por um modelo* $\mathbf{G^{op}} = \mathbf{G_1^{op}}||^I\mathbf{G_2}$*, é definida como:*

$$L(\mathbf{G^{op}}) = \theta^{-1}(L(\mathbf{G_2}))$$

Demonstração. ($L(\mathbf{G^{op}}) \subseteq \theta^{-1}(L(\mathbf{G_2}))$):

Para todas as cadeias $v \in \Sigma^*$, onde $v \in L(\mathbf{G^{op}})$, será analisado, por indução em $|v|$, que $v \in \theta^{-1}(L(\mathbf{G_2}))$.

i) Seja $|v| = 0$: $v = \epsilon$.

Como $L(\mathbf{G_2}) \neq \emptyset$, então $\theta^{-1}(L(\mathbf{G_2})) \neq \emptyset$ e

$$\epsilon \in \theta^{-1}(L(\mathbf{G_2})).$$

ii) Como hipótese indutiva assume-se que para $v = s \in \Sigma^*$ e $|v| = k$:

$$s \in L(\mathbf{G^{op}}) \rightarrow s \in \theta^{-1}(L(\mathbf{G_2})).$$

Assim,

$$\theta(s) \in L(\mathbf{G_2}).$$

iii) Como passo indutivo demonstra-se que para $v = s\sigma$, onde $\sigma \in \Sigma$, $|v| = k+1$ e $v \in L(\mathbf{G^{op}})$, chega-se a $v \in \theta^{-1}(L(\mathbf{G_2}))$.

Pela definição 6.3.1 existem três possibilidades para $f(\hat{f}(q_0, s), \sigma)!$, onde $\hat{f}(q_0, s) = (q_1, q_2, \tau)$:

a) $\sigma \in \Sigma_1$, $f_1(q_1, \sigma)!$ e $\omega_1(f_1(q_1, \sigma)) = \tau_0$.

Nesse caso, pela equação 6.2:

$$\theta(v) = \theta(s\sigma) = \theta(s) \in L(\mathbf{G_2}).$$

Então:

$$v \in \theta^{-1}(L(\mathbf{G_2})).$$

b) $f_1(q_1, \sigma)!$, $\omega_1(f_1(q_1, \sigma)) = \tau' \neq \tau_0$ e $f_2(q_2, \tau')!$.

Como $\hat{f}(q_0, s) = (q_1, q_2, \tau)$, pela equação 6.2:

$$\theta(v) = \theta(s\sigma) = \theta(s)\tau' \in L(\mathbf{G_2}).$$

Então,

$$v = s\sigma \in \theta^{-1}(L(\mathbf{G_2})).$$

c) $\sigma \in \Sigma_2$ e $f_2(q_2, \sigma)!$.

Pela equação 6.2,

$$\theta(v) = \theta(s\sigma) = \theta(s)\sigma \in L(\mathbf{G_2}).$$

Então

$$v = s\sigma \in \theta^{-1}(L(\mathbf{G_2})).$$

($L(\mathbf{G^{op}}) \supseteq \theta^{-1}(L(\mathbf{G_2}))$):

A partir da equação 6.3, a θ-imagem inversa é definida como a função

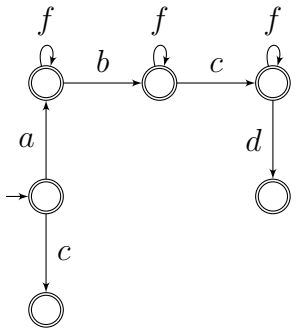
$$\theta^{-1} : 2^{T^*} \rightarrow 2^{L(\mathbf{G^{op}})}.$$

Então, por definição:

$$\theta^{-1}(L(\mathbf{G_2})) \subseteq L(\mathbf{G^{op}}).$$

□

Figura 76 – Linguagem gerada de $\mathbf{G^{op}}$ no exemplo 6.3.1.



Fonte: Elaborado pelo autor.

No exemplo acima, o mapa repórter θ é definido com base na função de saída ω. Para a obtenção da linguagem gerada pelo modelo de $\mathbf{G^{op}}$ do exemplo, primeiramente obtêm-se a linguagem $\theta^{-1}(L(\mathbf{G_2}))$, conforme ilustrado na Figura 76.

Ao analisar a linguagem marcada resultante, percebe-se que sua definição não é similar a da linguagem gerada. Isso porque a operação de θ-imagem inversa não leva em conta as cadeias que não são marcadas em $\mathbf{G_1^{op}}$. Com isso:

$$L_m(\mathbf{G^{op}}) \subseteq \theta^{-1}(L_m(\mathbf{G_2})).$$

Dessa forma, ao analisar a linguagem marcada do modelo resultante da composição interníveis, pode-se inferir a partir dos resultados já apresentados que:

$$L_m(\mathbf{G_1^{op}}||^I\mathbf{G_2}) = P_{\Sigma_1}^{-1}(L_m(\mathbf{G_1^{op}}))||\theta^{-1}(L_m(\mathbf{G_2})) \tag{6.5}$$

Apesar de os modelos $\mathbf{G_1^{op}}$ e $\mathbf{G_2}$ serem independentes, exceto pelo fato de que T_1 faz parte do alfabeto de $\mathbf{G_2}$, o mapa repórter θ é construído sobre o resultado da composição interníveis desses modelos, ou seja, é construído sobre uma estrutura que impõe restrições sobre o comportamento de $\mathbf{G_1^{op}}$ e $\mathbf{G_2}$. Por essa razão, o lema a seguir estabelece qual é a relação entre uma versão de baixo nível da linguagem de $\mathbf{G_2}$ e uma versão acrescida dos eventos de Σ_2 da linguagem de $\mathbf{G_1^{op}}$.

Lema 6.3.1. *Seja uma estrutura hierárquica com composição interníveis conforme a definição 6.2.1. Para uma projeção $P_{\Sigma_1} : \Sigma^* \to \Sigma_1^*$, é sempre verdade que:*

$$\theta^{-1}(L(\mathbf{G_2})) \subseteq P_{\Sigma_1}^{-1}(L(\mathbf{G_1^{op}})).$$

Demonstração. Serão analisadas todas as cadeias pertencentes a $\theta^{-1}(L(\mathbf{G_2}))$ e demonstrado que pertencem também a $P_{\Sigma_1}^{-1}(\mathbf{G_1^{op}})$.

i) Seja $\epsilon \in \theta^{-1}(L(\mathbf{G_2}))$.

Como $L(\mathbf{G_1^{op}}) \neq \emptyset$, então

$$\epsilon \in L(\mathbf{G_1^{op}}) \text{ e } \epsilon \in P_{\Sigma_1}^{-1}(L(\mathbf{G_1^{op}})).$$

ii) Seja $s \in \Sigma^*$, onde $s \in \theta^{-1}(L(\mathbf{G_2}))$ e $s \in P_{\Sigma_1}^{-1}(\mathbf{G_1^{op}})$.

Pode-se dizer que $\hat{f}((q_{0,1}, q_{0,2}, \tau_0), s) = (q_1, q_2, \tau)$, onde $\hat{f}$ é a função de transição de estados estendida de $\mathbf{G_1^{op}}||^I\mathbf{G_2}$.

Tomando $s' = P_{\Sigma_1}(s)$, então

$$s' \in L(\mathbf{G_1^{op}}) \text{ e } \hat{f}_1(q_{0,1}, s') = q_1.$$

iii) Seja $\sigma \in \Sigma$, onde $s\sigma \in \theta^{-1}(L(\mathbf{G_2}))$.

Considerando $f(\hat{f}((q_{0,1}, q_{0,2}, \tau_0), s), \sigma)!$, são possíveis dois casos:

a) $\sigma \in \Sigma_1$:

Pela definição 6.3.1:

$$f_1(q_1, \sigma)! \text{ e assim } s'\sigma \in L(\mathbf{G_1^{op}}).$$

Nesse caso,

$$P_{\Sigma_1}(s\sigma) = s'\sigma.$$

Portanto,

$$s\sigma \in P_{\Sigma_1}^{-1}(L(\mathbf{G_1^{op}})).$$

b) $\sigma \in \Sigma_2$:

Nesse caso,

$$P_{\Sigma_1}(s\sigma) = s'.$$

Como $s' \in L(\mathbf{G_1^{op}})$, então

$$s\sigma \in P_{\Sigma_1}^{-1}(L(\mathbf{G_1^{op}})).$$

□

O mapa repórter θ_1, associado ao modelo da planta operacional $\mathbf{G_1^{op}}$, pode ter uma versão estendida $\hat{\theta}_1 : P_{\Sigma_1}^{-1}(L(\mathbf{G_1^{op}})) \rightarrow T^*$, tendo como domínio a linguagem dessa planta operacional aumentada com os eventos de Σ_2. Define-se de forma recursiva com $\hat{\theta}_1(\epsilon) = \epsilon$ e

$$\hat{\theta}_1(s\sigma) = \begin{cases} \hat{\theta}_1(s) & se\ \sigma \in \Sigma_1\ e\ \theta_1(s'\sigma) = \theta_1(s') \quad ou \\ \hat{\theta}_1(s)\tau & se\ \sigma \in \Sigma_1\ e\ \theta_1(s'\sigma) = \theta_1(s')\tau \quad ou \\ \hat{\theta}_1(s)\sigma & se\ \sigma \in \Sigma_2 \end{cases} \tag{6.6}$$

onde $s' = P_{\Sigma_1}(s)$.

Utilizando as relações acima pode-se chegar a

$$\theta(L(\mathbf{G^{op}})) = \hat{\theta}_1(L(\mathbf{G^{op}})) = \hat{\theta}_1(\theta^{-1}(L(\mathbf{G_2}))). \tag{6.7}$$

A partir do teorema abaixo, constata-se que a estrutura hierárquica com composição no gerente, a partir da abordagem interníveis, é equivalente a uma estrutura hierárquica clássica com um modelo $\mathbf{G^{op}}$ e um modelo $\mathbf{G^{ge}}$. Este teorema afirma que, na estrutura proposta, o modelo $\mathbf{G_{12}^{ge}} = \mathbf{G_1^{ge}}||\mathbf{G_2}$ sempre é equivalente ao modelo da abstração de $\mathbf{G^{op}}$, ou seja $\mathbf{G_{12}^{ge}} \equiv \mathbf{G^{ge}}$. Esse resultado afirma que a composição interníveis representa corretamente a dinâmica de interação entre os modelos de $\mathbf{G_2}$ e $\mathbf{G_1^{op}}$. Tomando como exemplo o processo industrial comandado pela abstração de duas válvulas em série, o comportamento do processo ($\mathbf{G_2}$) controlado pela válvula resultante ($\mathbf{G_1^{ge}}$) é equivalente à abstração da composição interníveis entre o modelo operacional das válvulas ($\mathbf{G_1^{op}}$) e o processo ($\mathbf{G_2}$).

Teorema 6.3.1. *Para uma estrutura hierárquica com composição no gerente conforme a definição 6.2.1 é sempre verdade que*

$$\theta(L(\mathbf{G_1^{op}}||^I\mathbf{G_2})) = L(\mathbf{G_1^{ge}}||\mathbf{G_2}) \text{ e}$$
$$\theta(L_m(\mathbf{G_1^{op}}||^I\mathbf{G_2})) = L_m(\mathbf{G_1^{ge}}||\mathbf{G_2}).$$

Demonstração. Seja $\mathbf{G^{op}} = \mathbf{G_1^{op}}||^I\mathbf{G_2}$, conforme definição 6.3.1, e $\mathbf{G_{12}^{ge}} = \mathbf{G_1^{ge}}||\mathbf{G_2}$, deseja-se demonstrar que

$$\theta(L(\mathbf{G^{op}})) = L(\mathbf{G_{12}^{ge}}).$$

I) ($\theta(L(\mathbf{G^{op}})) \subseteq L(\mathbf{G_{12}^{ge}})$):
A partir da proposição 6.3.1, $L(\mathbf{G^{op}}) = \theta^{-1}(L(\mathbf{G_2}))$.
A partir do lema 6.3.1, $\theta^{-1}(L(\mathbf{G_2})) \subseteq P_{\Sigma_1}^{-1}(L(\mathbf{G_1^{op}}))$.
Então, é verdade que:

$$L(\mathbf{G^{op}}) = \theta^{-1}(L(\mathbf{G_2})) = P_{\Sigma_1}^{-1}(L(\mathbf{G_1^{op}})) \cap \theta^{-1}(L(\mathbf{G_2})).$$

Aplicando o operador θ:

$$\theta(L(\mathbf{G^{op}})) = \hat{\theta}_1(L(\mathbf{G^{op}})) = \hat{\theta}_1(P_{\Sigma_1}^{-1}(L(\mathbf{G_1^{op}})) \cap \theta^{-1}(L(\mathbf{G_2}))).$$

Pode-se afirmar que:

$$\theta(L(\mathbf{G^{op}})) \subseteq \hat{\theta}_1(P_{\Sigma_1}^{-1}(L(\mathbf{G_1^{op}}))) \cap \hat{\theta}_1(\theta^{-1}(L(\mathbf{G_2}))).$$

Como o mapa repórter θ, nessa estrutura, sinaliza cada evento de Σ_2 como o mesmo evento ao nível acima, a parcela $\hat{\theta}_1(P_{\Sigma_1}^{-1}(L(\mathbf{G_1^{op}})))$ pode ser escrita como $P_{T_1}^{-1}(\theta_1(L(\mathbf{G_1^{op}})))$. Assim:

$$\theta(L(\mathbf{G^{op}})) \subseteq P_{T_1}^{-1}(\theta_1(L(\mathbf{G_1^{op}}))) \cap \hat{\theta}_1(\theta^{-1}(L(\mathbf{G_2})))$$
$$\theta(L(\mathbf{G^{op}})) \subseteq P_{T_1}^{-1}(L(\mathbf{G_1^{ge}})) \cap \hat{\theta}_1(\theta^{-1}(L(\mathbf{G_2})))$$

Por outro lado, ao se aplicar o operador $\hat{\theta}_1$ sobre a θ-imagem inversa de $L(\mathbf{G_2})$, pode ocorrer perda de informações. Logo, $\hat{\theta}_1(\theta^{-1}(L(\mathbf{G_2}))) = \theta(\theta^{-1}(L(\mathbf{G_2}))) \subseteq L(\mathbf{G_2})$. De onde se segue que:

$$\theta(L(\mathbf{G^{op}})) \subseteq P_{T_1}^{-1}(L(\mathbf{G_1^{ge}})) \cap L(\mathbf{G_2}).$$

Como T_1 está contido no alfabeto de $\mathbf{G_2}$, a expressão acima é o mesmo que

$$\theta(L(\mathbf{G^{op}})) \subseteq L(\mathbf{G_1^{ge}})||L(\mathbf{G_2})$$
$$\theta(L(\mathbf{G^{op}})) \subseteq L(\mathbf{G^{ge}})$$

II) ($\theta(L(\mathbf{G^{op}})) \supseteq L(\mathbf{G_{12}^{ge}})$):

Seja $t \in L(\mathbf{G_1^{ge}}||\mathbf{G_2})$.

Pela definição de composição paralela de autômatos e considerando que T_1 faz parte do alfabeto de $\mathbf{G_2}$:

$$t \in L(\mathbf{G_2}) \text{ e } t \in P_{T_1}^{-1}(\mathbf{G_1^{ge}}).$$

Ou seja, a cadeia t pertence a $L(\mathbf{G_2})$ considerando ainda as restrições impostas na composição com $\mathbf{G_1^{ge}}$.

Assim, existe $s \in \theta^{-1}(L(\mathbf{G_2}))$, tal que $\theta(s) = t$.

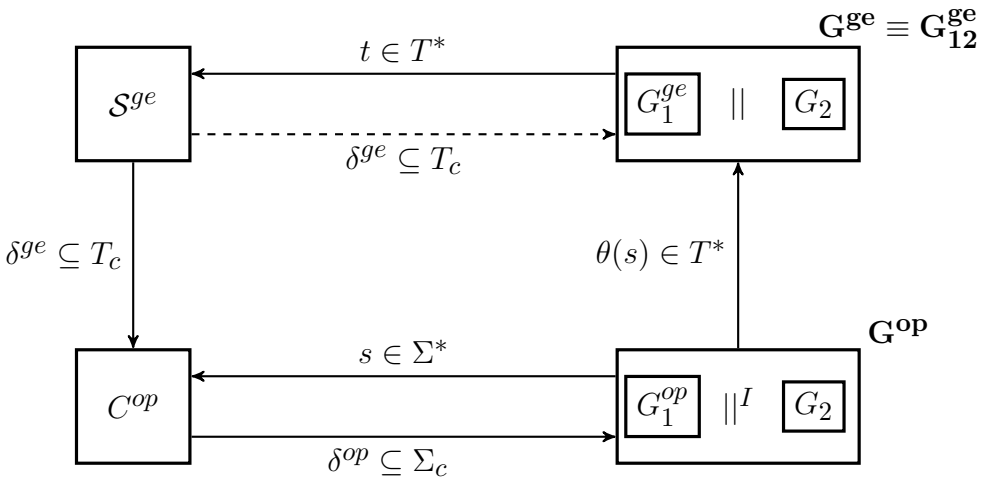
Então:

$$t \in \theta(\theta^{-1}(L(\mathbf{G_2}))) = L(\mathbf{G_1^{op}}||^I\mathbf{G_2}).$$

□

A partir do teorema acima, chega-se à conclusão de que a estrutura hierárquica com composição no gerente é equivalente à estrutura hierárquica clássica quando aplicada a composição interníveis, como ilustrado na Figura 77.

Figura 77 – Estrutura hierárquica com composição no gerente: equivalência entre modelo composto do gerente e abstração da composição interníveis.



Fonte: Elaborado pelo autor.

Assim, com os resultados acima, estabelecidas as devidas condições, é possível aplicar o teorema 5.3.1 para obter um supervisor ótimo e não bloqueante para a estrutura hierárquica com composição no gerente.

Corolário 6.3.1. *Seja uma estrutura hierárquica com composição no gerente conforme a definição 6.2.1,* $T_{conf} \subseteq T$ *o conjunto dos eventos confiáveis e.r.a.* θ *e* $\mathbf{G^{op}} = \mathbf{G_1^{op}}||^I\mathbf{G_2}$*. Para uma especificação gerencial* $E^{ge} \subseteq L_m(\mathbf{G^{ge}})$ *não vazia e controlável e.r.a.* $\mathbf{G^{ge}}$ *e um supervisor não bloqueante* $\mathcal{S}^{ge}$*, tal que* $L_m(\mathcal{S}^{ge}/\mathbf{G^{ge}}) = E^{ge}$*, se o par (*$\mathbf{G^{op}}, \theta$*) possuir consistência de controle estrita, se existir consistência de marcação entre* $\mathbf{G^{op}}$ *e* $\mathbf{G^{ge}}$ *e se o alfabeto* T_{conf} *for suficiente para prefixo fechamento de* E^{ge}*, pode-se garantir que:*

i) $\theta(L_m(\mathcal{S}^{ge\rightarrow op}/\mathbf{G^{op}})) = E^{ge}$ ***e***

ii) O supervisor $\mathcal{S}^{ge\rightarrow op}$ *será não bloqueante para* $\mathbf{G^{op}}$*.*

Demonstração. Com os resultados do teorema 6.3.1 chega-se à conclusão de que a estrutura hierárquica com composição no gerente com uma planta do operador $\mathbf{G_1^{op}}$ e uma planta $\mathbf{G_2}$, a partir da composição interníveis, é equivalente à estrutura hierárquica clássica com $\mathbf{G^{op}} = \mathbf{G_1^{op}}||^I\mathbf{G_2}$ e $\mathbf{G^{ge}} = \mathbf{G_1^{ge}}||\mathbf{G_2}$.

Dessa forma, com as condições acima podem-se aplicar os mesmos resultados obtidos no teorema 5.3.1.

□

Destaca-se que para ser atingida a consistência de controle estrita pelo par ($\mathbf{G^{op}}$, θ), é necessário que $\mathbf{G_1^{op}}$ e seu mapa repórter associado possuam consistência de controle persistente conforme Definição 6.1.1. Do contrário, pela definição da composição interníveis, é possível que o modelo resultante não atinja nem mesmo consistência de controle o que implicaria na não existência de consistência hierárquica de baixo nível para a estrutura.

Lema 6.3.2. *Seja uma estrutura hierárquica com composição no gerente conforme a definição 6.2.1 e* $\mathbf{G^{op}} = \mathbf{G_1^{op}}||^I\mathbf{G_2}$*. Se o par* $(\mathbf{G_1^{op}}, \theta_1)$ *possuir consistência de controle persistente, então o par* $(\mathbf{G^{op}}, \theta)$ *possui consistência de controle estrita.*

Demonstração. De acordo com a definição 6.3.1 e a equação 6.2, para $s\sigma \in L(\mathbf{G^{op}})$ e $\theta(s\sigma) = \theta(s)\tau$, com $\tau \neq \epsilon$, existem duas possibilidades:

I) $\tau \in T_1$;

Nesse caso, por definição, $\sigma \in \Sigma_1$. Assim, como $(\mathbf{G_1^{op}}, \theta_1)$ possui consistência de controle persistente, de acordo com a definição 6.1.1, se $\tau \in T_c$, então $\sigma \in \Sigma_{1,c}$.

II) $\tau \in \Sigma_2$;

Nesse caso, por definição, $\sigma \in \Sigma_2$ e $\theta(s\sigma) = \theta(s)\sigma$.

Então, obviamente, se $\tau \in T_c$, então $\sigma \in \Sigma_{2,c}$.

Dessa forma, se $\tau \in T_c$, então $\sigma \in \Sigma_{1,c} \cup \Sigma_{2,c} = \Sigma_c$.

Conclui-se então que $s\sigma \in \Sigma^* \Sigma_c$, o que implica na consistência de controle persistente para o par $(\mathbf{G^{op}}, \theta)$. Assim, de acordo com a proposição 6.1.1, $(\mathbf{G^{op}}, \theta)$ possui consistência de controle estrita. □

Com as condições impostas no corolário 6.3.1, a partir da composição interníveis em uma estrutura hierárquica com composição no gerente, é possível garantir um supervisor ótimo e não bloqueante para determinadas especificações gerenciais para plantas que não possuam mapa repórter observador e para modelos que sincronizam eventos em uma composição no nível do gerente.

Esse resultado difere de Pu (2000), que exige que o mapa repórter da planta do operador seja observador e que não haja sincronização de eventos entre os modelos compostos. Difere também de Seow (2014) que impõe a restrição de que a linguagem do modelo abstrato não sofra interferência da composição e supervisão no nível gerencial. Sob a óptica da abordagem interníveis, pode-se dizer que os resultados desses autores são casos particulares da aplicação dessa abordagem.

Contudo, uma limitação ainda encontrada nessa metodologia é relacionada a complexidade para realizar a composição interníveis e a possível explosão no número de estados. De toda forma, ao analisar o problema de controle hierárquico em um circuito de válvulas, chega-se a algumas condições que garantem os requisitos do corolário 6.3.1 mesmo sem a necessidade de calcular o modelo de $\mathbf{G^{op}}$ para determinados tipos de sistemas. Com determinadas condições para a marcação dos modelos, garantindo consistência de controle persistente e ainda a confiabilidade de alguns eventos, é possível obter os mesmos resultados do corolário de uma forma mais direta. Essas condições são estabelecidas por meio do Lema 6.3.2 e dos dois lemas a seguir para se chegar ao teorema principal deste capítulo.

Lema 6.3.3. *Seja uma estrutura hierárquica com composição no gerente conforme a definição 6.2.1 e* $\mathbf{G^{op}} = \mathbf{G_1^{op}} ||^I \mathbf{G_2}$*. Se todos os estados de* $\mathbf{G_1^{op}}$ *forem marcados, então existe consistência de marcação entre* $\mathbf{G^{op}}$ *e* $\mathbf{G^{ge}}$*.*

Demonstração. Expressa-se por $\theta^{-1}(L_m(\mathbf{G^{ge}})) = L_m(\mathbf{G^{op}})$ a consistência de marcação entre $\mathbf{G^{op}}$ e $\mathbf{G^{ge}}$.

Supõe-se por contradição que, para algum $t \in L_m(\mathbf{G^{ge}})$, $\exists s \in L(\mathbf{G^{op}}) \backslash L_m(\mathbf{G^{op}})$ tal que $\theta(s) = t$.

Para essa condição, a única possibilidade seria uma cadeia particionada em $s = s'\sigma$, onde σ é silencioso, ou seja, $\theta(s'\sigma) = \theta(s') = \theta(s) = t$.

Nesse caso, pela definição 6.3.1, $f(q_0, s') = (q_1, q_2, \tau')$ e $f((q_1, q_2, \tau'), \sigma) = (f_1(q_1, \sigma), q_2, \tau_0)$.

Como $s \in L(\mathbf{G^{op}}) \setminus L_m(\mathbf{G^{op}})$, então o estado $f_1(q_1, \sigma)$ seria desmarcado, o que, pela suposição inicial é uma contradição.

Dessa forma, $\nexists$ tal cadeia s, o que implica na consistênica de marcação entre $\mathbf{G^{op}}$ e $\mathbf{G^{ge}}$. □

Lema 6.3.4. *Seja uma estrutura hierárquica com composição no gerente conforme a Definição 6.2.1, uma planta do operador $\mathbf{G^{op}} = \mathbf{G_1^{op}}||^I\mathbf{G_2}$, com mapa repórter associado θ tal que, para uma planta do gerente $\mathbf{G^{ge}}$, $L(\mathbf{G^{ge}}) = \theta(L(\mathbf{G^{op}}))$. Se um evento $\tau \in T_1$ for confiável e.r.a θ_1, então τ será confiável e.r.a. θ.*

Demonstração. Seja $s \in L(\mathbf{G^{op}})$ tal que $\theta(s)\tau \in L(\mathbf{G^{ge}})$.

Segundo o Lema 6.3.1, $s \in P^{-1}_{\Sigma_1}(L(\mathbf{G_1^{op}}))$, isto é,

$$s_1 = P_{\Sigma_1}(s) \in L(\mathbf{G_1^{op}}).$$

Conforme o Teorema 6.3.1, $\theta(s)\tau \in L(\mathbf{G_1^{ge}}||\mathbf{G_2})$, ou seja, τ é elegível depois de $\theta(s)$, então $\theta_1(s_1)\tau \in L(\mathbf{G_1^{ge}})$.

Assumindo que τ é confiável e.r.a. θ_1, então

$$(\exists u_1 \in \Sigma_1^+) : s_1u_1 \in L(\mathbf{G_1^{op}}) \,\&\, \theta_1(s_1u_1) = \theta_1(s_1)\tau.$$

Sabendo que $\Sigma_1 \subset \Sigma$, então $u_1 \in \Sigma^+$.

Como $s_1u_1 \in L(\mathbf{G_1^{op}})$, $\theta_1(s_1u_1) = \theta_1(s_1)\tau$ e $s_1 = P_{\Sigma_1}(s)$, então, pela Definição 6.3.1, $su_1 \in L(\mathbf{G^{op}})$.

Com isso, $\theta(su_1) = \theta(s)\tau$.

Dessa forma,

$$(\forall s \in L(\mathbf{G^{op}}))\theta(s)\tau \in L(\mathbf{G^{ge}}) \rightarrow (\exists u_1 \in \Sigma^+)\text{: } su_1 \in L(\mathbf{G^{op}}) \;\&\; \theta(su_1) = \theta(s)\tau,$$

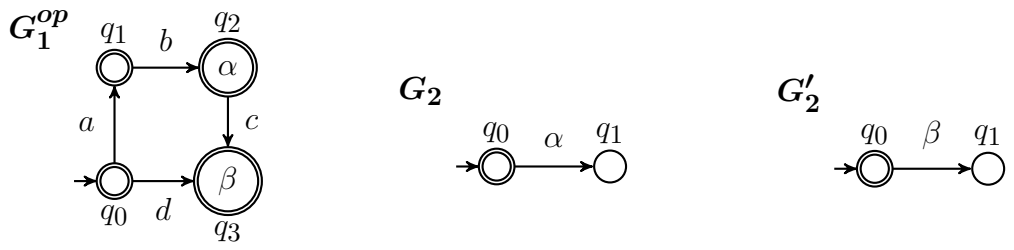
o que indica que τ é confiável e.r.a. θ.

□

Exemplo 6.3.2. ***Evento confiável na composição interníveis:*** *Neste exemplo é ilustrada a afirmação do Lema 6.3.4 a respeito da confiabilidade dos eventos na composição interníveis. Na Figura 78 é apresentado o modelo de $\mathbf{G_1^{op}}$ e seu mapa repórter θ_1, um modelo $\mathbf{G_2}$ e um modelo $\mathbf{G_2'}$ que será utilizado como contraponto. Nota-se que o evento abstrato α é confiável em relação a θ_1 e o evento abstrato β é não confiável em relação a θ_1.*

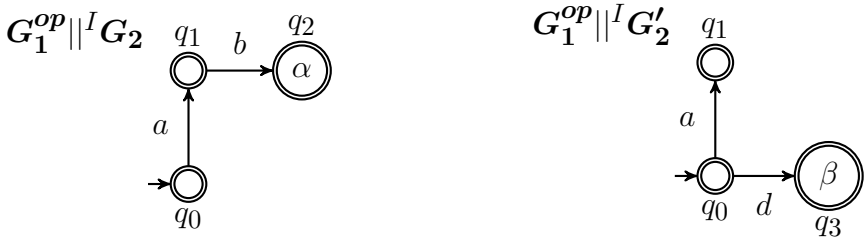
Submetendo-se $\mathbf{G_1^{op}}$ a uma composição interníveis com $\mathbf{G_2}$, o evento α permanece sendo confiável em relação a θ. Do mesmo modo, submetendo-se $\mathbf{G_1^{op}}$ a uma composição interníveis com $\mathbf{G_2'}$, o evento β permanece sendo como não confiável, agora em relação a θ.

Figura 78 – Em relação a θ_1, o evento α é confiável, mas β é não confiável.



Fonte: Elaborado pelo autor.

Figura 79 – Em relação a θ a confiabilidade dos eventos é mantida, ou seja, o evento α é confiável, mas β é não confiável.



Fonte: Elaborado pelo autor.

Com base nos três lemas anteriores, chega-se ao teorema principal, com condições suficientes que atendem o corolário 6.3.1, garantindo um supervisor ótimo e não bloqueante, sem a necessidade da obtenção do modelo de $\mathbf{G^{op}}$, apenas observando o modelo de $\mathbf{G_1^{op}}$ e seu mapa repórter associado.

Teorema 6.3.2. *Seja uma estrutura hierárquica com composição no gerente conforme a definição 6.2.1, $T_{conf} \subseteq T$ o conjunto dos eventos confiáveis e.r.a. θ e $\mathbf{G^{op}} = \mathbf{G_1^{op}}||^I\mathbf{G_2}$. Para uma especificação gerencial $E^{ge} \subseteq L_m(\mathbf{G^{ge}})$ não vazia e controlável e.r.a $\mathbf{G^{ge}}$ e um supervisor não bloqueante $\mathcal{S}^{ge}$, tal que $L_m(\mathcal{S}^{ge}/\mathbf{G^{ge}}) = E^{ge}$, se o par ($\mathbf{G_1^{op}}, \theta_1$) possuir consistência de controle persistente, se todos os estados de $\mathbf{G_1^{op}}$ forem marcados e se o alfabeto $T_{1,conf} \cup \Sigma_2$ for suficiente para prefixo fechamento de E^{ge}, pode-se garantir que:*

i) $\theta(L_m(\mathcal{S}^{ge\rightarrow op}/\mathbf{G^{op}})) = E^{ge}$ *e*

ii) O supervisor $\mathcal{S}^{ge\rightarrow op}$ será não bloqueante para $\mathbf{G^{op}}$.

Demonstração. De acordo com o lema 6.3.2, como ($\mathbf{G_1^{op}}, \theta_1$) possui consistência de controle persistente, então ($\mathbf{G^{op}}, \theta$) possui consistência de controle estrita.

De acordo com o lema 6.3.3, como todos os estados de $\mathbf{G_1^{op}}$ são marcados, então há consistência de marcação entre $\mathbf{G^{op}}$ e $\mathbf{G^{ge}}$.

Por outro lado, de acordo com o lema 6.3.4, os eventos de $T_{1,conf}$, por serem

confiáveis em relação a θ_1, são confiáveis em relação a θ. E como cada evento de Σ_2 é vocalizado como o próprio evento na composição interníveis, então são também confiáveis em relação a θ. Assim, $T_{1,conf} \cup \Sigma_2$ é um alfabeto de eventos confiáveis de $\mathbf{G^{ge}} = \mathbf{G_1^{ge}}||\mathbf{G_2}$ em relação a θ.

Dessa forma chega-se às mesmas condições estabelecidas no corolário 6.3.1 para garantir os resultados do teorema.

□

Com base no Teorema 6.3.2, a partir de condições estabelecidas na planta do operador $\mathbf{G_1^{op}}$ pode-se chegar a garantias para controle ótimo e não bloqueante em uma estrutura hierárquica com composição no gerente. Esse resultado é relevante ao se analisar a complexidade computacional do modelo do operador em uma composição interníveis, o que pode ser evitado ao garantir as condições na planta de $\mathbf{G_1^{op}}$. A estrutura hierárquica com composição no gerente com sincronização de eventos no gerente pode ser empregada em diversos tipos de sistemas, como em processos industriais comandados por circuitos de válvulas. Nas próximas seções serão analisados exemplos de aplicação dos resultados obtidos com esse teorema.

6.4 EXEMPLO DE APLICAÇÃO EM UM PROCESSO INDUSTRIAL SIMPLIFICADO

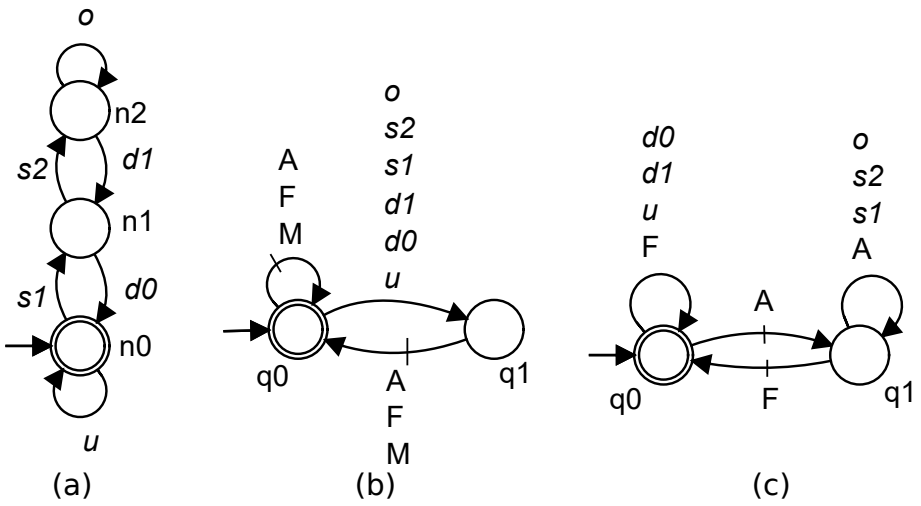
Nesta seção será apresentado um exemplo com um processo industrial simplificado, a fim de ilustrar a aplicação dos conceitos abordados anteriormente nesse capítulo. O exemplo em questão se assemelha em alguns pontos com o processo industrial comandado por um circuito de válvulas, enquadrando-se como uma estrutura hierárquica com composição no gerente, conforme definição 6.2.1. Neste exemplo, o processo é formado por um tanque, uma válvula que pode apresentar falha e uma bomba que sempre permanece ligada. O nível do tanque é comandado por eventos abstratos da válvula, contando que essa apresenta eventos operacionais que não aparecem no controle do processo industrial.

A partir deste exemplo será possível obter algumas conclusões sobre a estrutura do processo industrial e como podem ser analisados processos mais complexos que possuem as mesmas características.

O processo industrial utilizado neste exemplo consiste em um tanque com três níveis: baixo, médio e alto, que serão identificados com os índices 0, 1 e 2 respectivamente. O tanque inicia no nível baixo, indicando que está vazio. O modelo $\mathbf{G_N}$ (Figura 80 - a) representa as mudanças de nível no tanque, onde todos os eventos são não controláveis. Os eventos u e o indicam *underflow* e *overflow* respectivamente. Os eventos $s1$ e $s2$ indicam subida de nível para os índices 1 e 2 respectivamente. Os eventos $d1$ e $d0$ indicam descida do nível para os índices 1 e 0 respectivamente. O modelo $\mathbf{G_P}$ representa a preempção da válvula (Figura 80 - b), indica que sempre ocorre um co-

mando da válvula entre duas mudanças de nível. O modelo que representa a vazão no tanque, $\mathbf{G_{VAZ}}$ (Figura 80 - c), indica as mudanças de nível de acordo com a abertura da válvula. Nesse processo não é considerado um modelo de bomba, considera-se que a bomba sempre permanece ligada.

Figura 80 – (a) $\mathbf{G_N}$: Modelo do tanque simplificado com três divisões de nível. (b) $\mathbf{G_P}$: Modelo de preempção da válvula. (c) $\mathbf{G_{VAZ}}$: Modelo de vazão do tanque.



Fonte: Elaborado pelo autor.

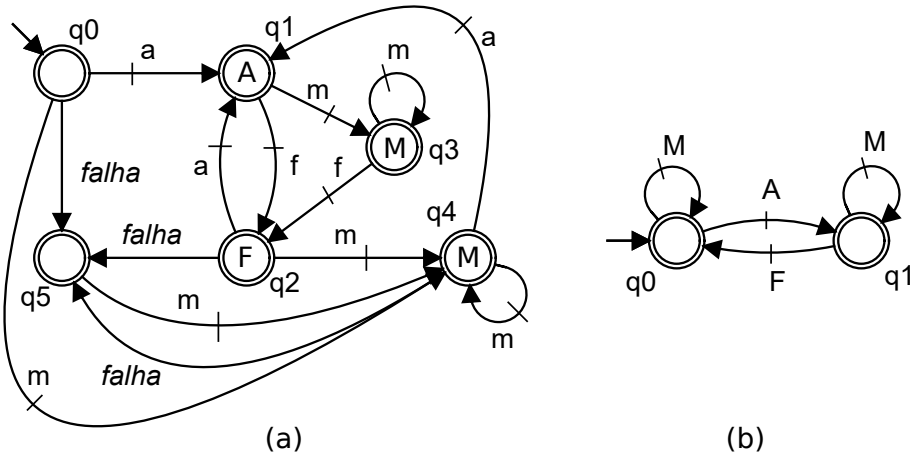
Para comando do processo considera-se uma única válvula de bloqueio que apresenta uma falha intermitente em sua abertura. Essa falha não é controlável e somente aparece no nível operacional, sua característica é de não permitir a abertura da válvula no momento de um comando do operador, o que não é perceptível no nível abstrato. Essa característica torna o evento abstrato de abertura da válvula como não confiável. Depois da ocorrência da falha, a válvula ainda pode se manter na posição fechada e, após esse comando, existe a possibilidade da abertura da válvula com sucesso ou ainda uma nova falha de abertura.

O modelo que representa o comportamento operacional da válvula é chamado de $\mathbf{G_1^{op}}$ (Figura 81 - a) e seu modelo abstrato, $\mathbf{G_1^{ge}}$, é representado na Figura 81 - b.

Os eventos controláveis a, f e m representam respectivamente os comandos do operador para *abrir*, *fechar* ou *manter* a posição da válvula. Os eventos abstratos controláveis A, F e M formam o modelo abstrato da válvula, indicam respectivamente as respostas da válvula para abrir, fechar ou manter. Observa-se no modelo $\mathbf{G_1^{op}}$ que o evento A é não confiável, pois o evento a, que leva a vocalização de A em q_1 não está habilitado no estado q_5 e, como esse é um estado silencioso, a impossibilidade de ocorrência de A não é perceptível no nível do gerente.

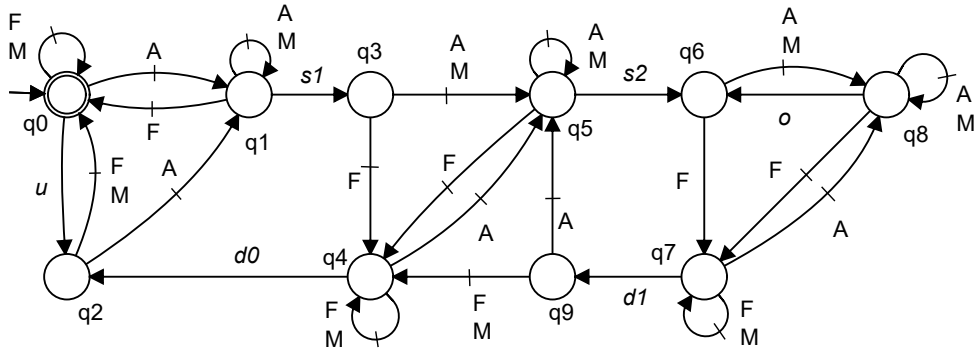
O processo utilizado neste exemplo se enquadra em uma estrutura hierárquica com composição no gerente (definição 6.2.1), em que a composição dos modelos $\mathbf{G_N}$, $\mathbf{G_P}$ e $\mathbf{G_{VAZ}}$ forma um modelo $\mathbf{G_2}$ (Figura 82) que, por sua vez, sincroniza eventos com o modelo abstrato da válvula (Figura 81 - b).

Figura 81 – (a) $\mathbf{G_1^{op}}$: Modelo operacional de uma válvula de bloqueio com falha simplificada. (b) $\mathbf{G_1^{ge}}$: Modelo abstrato de uma válvula de bloqueio com falha simplificada.



Fonte: Elaborado pelo autor.

Figura 82 – $\mathbf{G_2 = G_N || G_P || G_{VAZ}}$: Composição paralela entre os modelos do processo.



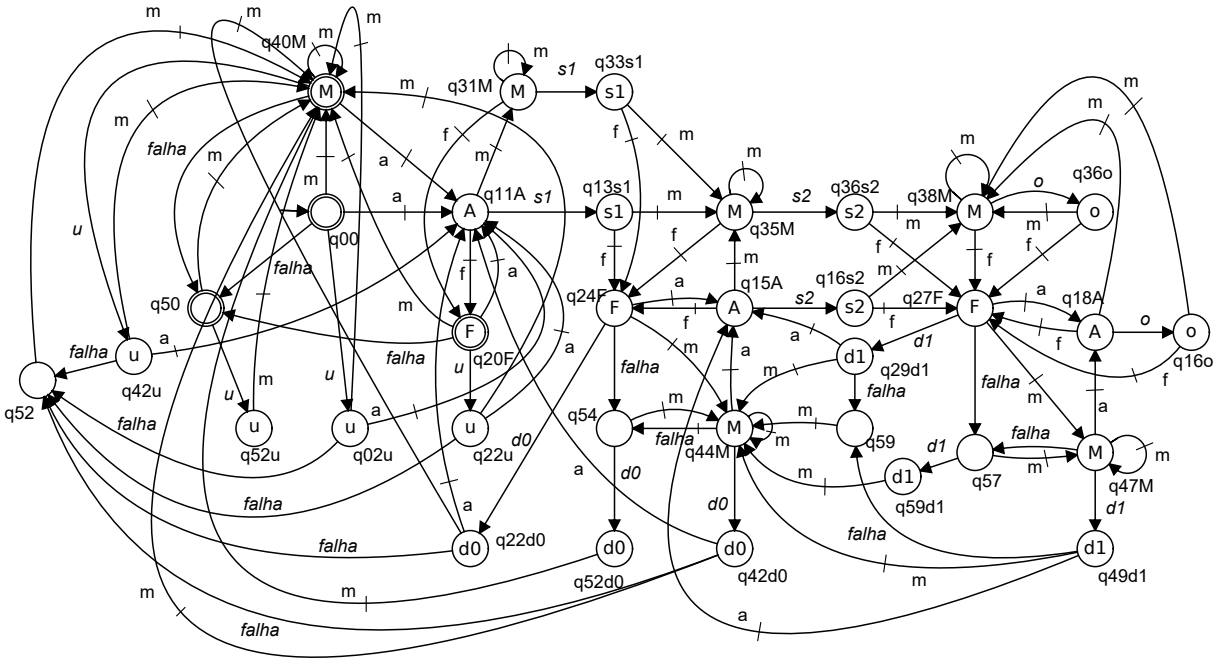
Fonte: Elaborado pelo autor.

Como $\mathbf{G_2}$ sincroniza eventos com $\mathbf{G_1^{ge}}$ que, por sua vez, são gerados por vocalizações em $\mathbf{G_1^{op}}$, é necessário empregar a composição interníveis. Para analisar as propriedades de consistência da estrutura é obtido o modelo de $\mathbf{G^{op}}$ na Figura 83, por meio de $\mathbf{G_1^{op}} ||^I \mathbf{G_2}$. Conforme a nomenclatura da definição 6.3.1 (composição interníveis), os alfabetos envolvidos nesse modelo são:

$$\Sigma_1 = \{a, f, m, falha\};$$
$$T_1 = \{A, F, M\};$$
$$\Sigma_2 = \{u, s_1, s_2, o, d_1, d_0\};$$
$$T = T_1 \cup \Sigma_2; T_0 = T \cup \{\tau_0\}.$$

Os nomes dos estados de $\mathbf{G^{op}}$ são padronizados como $q_{nmv} \in Q_1^{op} \times Q_2 \times T_0$, onde n se refere ao estado correspondente em $\mathbf{G_1^{op}}$, m se refere ao estado correspondente em $\mathbf{G_2}$ e v se refere ao evento vocalizado pelo estado.

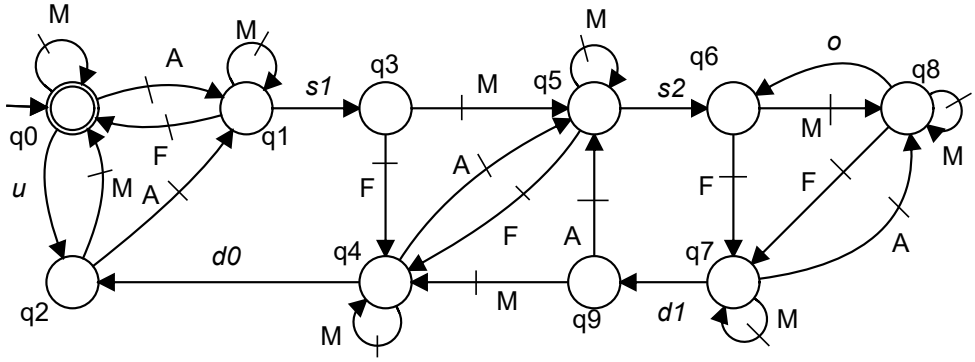
Figura 83 – $\mathbf{G^{op}} = \mathbf{G_1^{op}}||^I\mathbf{G_2}$: Composição interníveis entre o modelo operacional da válvula simplificada e o processo.



Fonte: Elaborado pelo autor.

Na Figura 84 apresenta-se o modelo composto do gerente, que pode ser obtido de duas formas diferentes. Em primeiro lugar, esse modelo pode ser considerado como a composição paralela de $\mathbf{G_1^{ge}}$ com $\mathbf{G_2}$, ou seja $\mathbf{G^{ge}} = \mathbf{G_1^{ge}}||\mathbf{G_2}$. Por outro lado, conforme o teorema 6.3.1, esse modelo também pode ser obtido por meio da abstração de $\mathbf{G^{op}}$ com seu mapa repórter θ. Segundo esse teorema, os modelos obtidos por esses dois caminhos são equivalentes.

Figura 84 – $\mathbf{G^{ge}} = \mathbf{G_1^{ge}}||\mathbf{G_2}$: composição paralela da abstração da válvula simplificada com o processo. Esse modelo também é obtido como a abstração de $\mathbf{G^{op}}$.

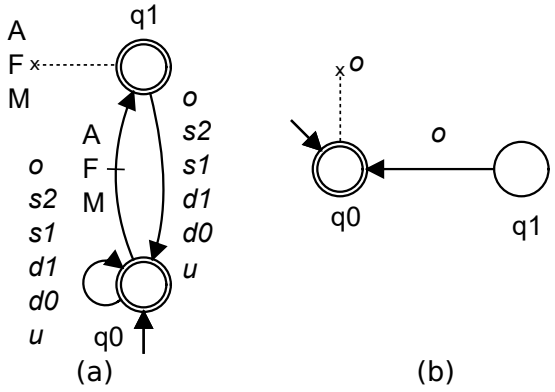


Fonte: Elaborado pelo autor.

Como requisitos para o sistema em malha fechada no nível gerencial deseja-se que o comportamento da válvula seja reativo às mudanças de nível, o que é imposto pela especificação E_A (Figura 85 - a), e que nunca ocorra *overflow*, o que é imposto pela especificação E_L (Figura 85 - b). A especificação E_A age sobre eventos abstratos

da válvula, ação que deverá ser realizada por meio do supervisor induzido sobre a planta operacional. Já a especificação E_L estabelece que o evento de *overflow* não deve ocorrer, ação que será traduzida como comandos para a válvula operacional, também por meio do supervisor induzido.

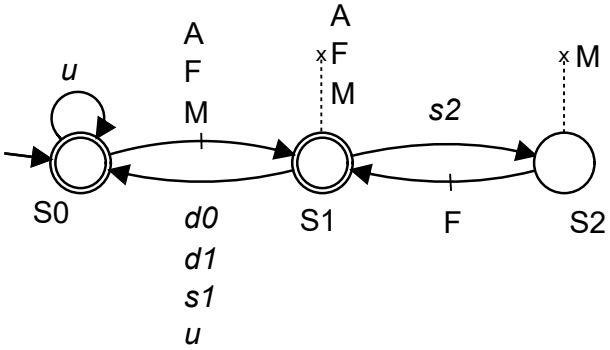
Figura 85 – (a) E_A: Modelo que representa especificação de ação da válvula. (b) E_L: Modelo que representa especificação de limite de operação do tanque.



Fonte: Elaborado pelo autor.

De modo a atender as especificações é obtido um supervisor no nível gerencial $\mathcal{S}^{ge}$, cuja versão reduzida ($\mathcal{R}^{ge}$) é apresentada na Figura 86, tal que $L_m(\mathcal{R}^{ge}/\mathbf{G^{ge}}) = L_m(\mathcal{S}^{ge}/\mathbf{G^{ge}}) = E^{ge}$, onde E^{ge} é uma linguagem controlável e.r.a. $\mathbf{G^{ge}}$ que atende as especificações $E_A||E_L$. Analisando o supervisor reduzido, o estado inicial é totalmente permissivo, ou seja não desabilita nenhuma ação da válvula. Assim que a vávula age, estado $S1$, os seus eventos são desabilitados para aguardar uma alteração no nível do tanque, o que caracteriza a ação reativa do controle supervisório. Na ocorrência do evento $s2$, $\mathcal{R}^{ge}$ dirige-se ao estado $S2$, o que significa que o tanque já atingiu o seu nível máximo e um *overflow* deve ser evitado, o que é feito proibindo a válvula de manter-se na posição aberta.

Figura 86 – $\mathcal{R}^{ge}$: Supervisor reduzido para o processo industrial simplificado.

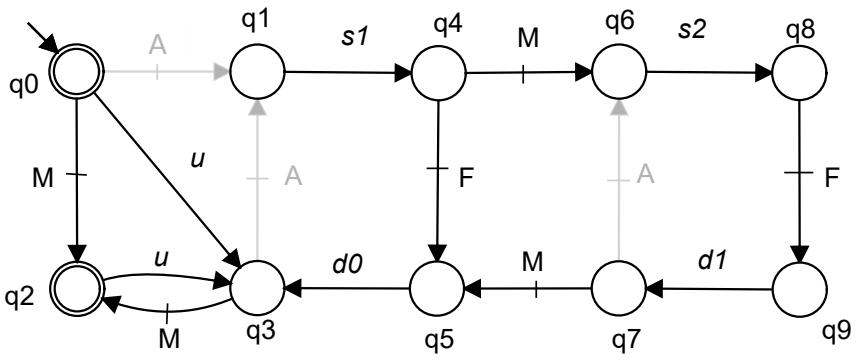


Fonte: Elaborado pelo autor.

A análise da linguagem do gerente em malha fechada é feita com o supervisor gerencial $\mathcal{S}^{ge}$ apresentado na Figura 87, sabendo que $L_m(\mathcal{S}^{ge}/\mathbf{G^{ge}}) = E^{ge}$. Nessa figura, o evento abstrato A é destacado na cor cinza, por ser um evento não confiável.

Nesse modelo pode-se constatar que a partir de qualquer estado é possível atingir um estado marcado por meio de cadeias formadas por eventos confiáveis. Em outras palavras, mesmo excluindo o evento não confiável A, o modelo de $\mathcal{S}^{ge}$ permanece coacessível, o que indica que o alfabeto dos eventos confiáveis é suficiente para prefixo fechamento de E^{ge}.

Figura 87 – $\mathcal{S}^{ge}$: Supervisor gerencial para o processo industrial simplificado. As transições com o evento não confiável A são distinguidas pela cor cinza.



Fonte: Elaborado pelo autor.

Analisando o corolário 6.3.1, nota-se que suas três condições são satisfeitas pelos modelos do exemplo em questão. Em outras palavras, como o modelo $\mathbf{G^{op}}$ (Figura 83) e seu mapa repórter associado possuem consistência de controle estrita, como existe consistência de marcação entre $\mathbf{G^{op}}$ e $\mathbf{G^{ge}}$ e como o alfabeto dos eventos confiáveis é suficiente para prefixo fechamento de E^{ge}, então o supervisor induzido $\mathcal{S}^{ge \to op}$ é não bloqueante para $\mathbf{G^{op}}$ e $\theta(L_m(\mathcal{S}^{ge \to op}/\mathbf{G^{op}})) = E^{ge}$.

No entanto, a obtenção do modelo de $\mathbf{G^{op}}$ pode ter um custo computacional demasiadamente alto dependendo dos modelos envolvidos. Por outro lado, ao observar os modelos acima pode-se perceber que as condições do teorema 6.3.2 são também satisfeitas. Dessa forma podem-se garantir os mesmos resultados para o supervisor induzido sem a necessidade de obtenção do modelo de $\mathbf{G^{op}}$, o que traz uma grande vantagem na análise no que se refere à complexidade envolvida. Abaixo segue uma breve descrição dessas três condições no contexto do exemplo em questão.

Ao analisar o modelo de $\mathbf{G_1^{op}}$, constata-se que para cada evento de alto nível controlável, os caminhos silenciosos correspondentes possuem um evento controlável ao final da cadeia, o que caracteriza a consistência de controle persistente para ($\mathbf{G_1^{op}}$, θ_1). Assim, de acordo com o lema 6.3.2, o par ($\mathbf{G^{op}}$, θ) possui consistência de controle estrita.

Analisando o modelo operacional da válvula, $\mathbf{G_1^{op}}$, observa-se que todos os seus estados são marcados, implicando em $L_m(\mathbf{G_1^{op}}) = L(\mathbf{G_1^{op}})$ e na existência da consistência de marcação entre $\mathbf{G_1^{op}}$ e $\mathbf{G_1^{ge}}$ conforme o lema 6.3.3. Pela construção da composição interníveis, todo trecho silencioso que corresponde a algum $\tau \in \Sigma_2$ é formado somente por um único evento. Os trechos silenciosos de $\mathbf{G^{op}}$ formados

por cadeias de comprimento maior que um correspondem a eventos de $\tau \in T_1$, que são os eventos abstratos de $\mathbf{G_1^{op}}$. Como todas as cadeias de $\mathbf{G_1^{op}}$ são marcadas, se um trecho silencioso de $\mathbf{G^{op}}$ não é marcado, então a palavra vocal que o antecede também não é marcada, pois essa desmarcação sempre ocorre devido às cadeias não marcadas de $\mathbf{G_2}$. Se uma palavra vocal de $\mathbf{G^{op}}$ é marcada, então o trecho silencioso que o segue permanece também marcado. Essa correspondência entre as linguagens marcadas, conforme definição 2.3.11, caracteriza a consistência de marcação entre $\mathbf{G^{op}}$ e $\mathbf{G^{ge}}$.

Como terceira característica a ser analisada, o evento abstrato A, único evento não confiável de $\mathbf{G_1^{op}}$, permanece sendo como o único evento não confiável de $\mathbf{G^{op}}$, característica que não é modificada pela composição interníveis, conforme afirmação do lema 6.3.4.

A partir da análise dessas três características dos modelos, verifica-se que atingem-se as condições dos lemas 6.3.2, 6.3.3, e 6.3.4. Esse resultado leva ao teorema 6.3.2, que afirma que é possível chegar a uma estrutura hierárquica com composição no gerente não bloqueante analisando somente o modelo de $\mathbf{G^{ge}} = \mathbf{G_1^{ge}}||\mathbf{G_2}$ e a especificação E^{ge} sem a necessidade de obtenção do modelo $\mathbf{G^{op}}$.

6.5 EXEMPLO DE APLICAÇÃO: PROCESSO INDUSTRIAL COMANDADO POR UM CIRCUITO DE VÁLVULAS

Para a aplicação do método proposto em um processo real, retoma-se o exemplo apresentado nas seções 4.4 e 4.5, onde é obtido o modelo abstrato da associação de uma válvula de controle em série com uma válvula de bloqueio para o controle supervisório de um processo industrial. Nesse exemplo foi evidenciada a impossibilidade de solução desse problema a partir dos métodos conhecidos devido a dois fatores principais. Em primeiro lugar destaca-se a não existência da propriedade de observador pelo mapa repórter envolvido o que impossibilita, com os métodos existentes, a obtenção de um controle supervisório não bloqueante. O primeiro fator foi solucionado no capítulo 5, a partir da definição de eventos confiáveis e alfabeto suficiente para prefixo fechamento de uma linguagem, o que tornou possível resolver o mesmo problema utilizando uma nova abordagem. O segundo fator envolvido diz respeito à sincronização de eventos pelos modelos do nível gerencial, o que também é uma restrição imposta pelas técnicas conhecidas. Conforme apresentado na Seção 4.5, a utilização do modelo abstrato de uma válvula equivalente para o comando do processo industrial apresenta essa característica, o que impossibilita a resolução do problema utilizando os métodos conhecidos. Por outro lado, a partir da nova abordagem apresentada no presente capítulo, torna-se possível projetar um controle supervisório hierárquico ótimo e não bloqueante para o problema apresentado, mesmo levando em conta essas condições apresentadas.

Ao analisar os modelos do exemplo apresentado, observa-se que se enquadram em uma estrutura hierárquica com composição no gerente conforme definição 6.2.1. Utiliza-se a estratégia de modelagem multinível por abstrações sucessivas apresentada na Seção 4.2 para obter o modelo abstrato para a associação em série de uma válvula de controle com uma válvula de bloqueio. O autômato da Figura 64 (planta operacional para uma válvula de controle em série com uma válvula de bloqueio, com 30 estados) é utilizado como modelo $\mathbf{G_1^{op}}$ na estrutura com composição no gerente. Sua abstração, o autômato da válvula equivalente com 4 estados apresentado na Figura 65, enquadra-se como modelo $\mathbf{G_1^{ge}}$ na estrutura.

O diagrama do processo industrial a ser controlado é apresentado na Figura 66, composto pelo tanque de nível, circuito de válvulas, bomba centrífuga, controlador lógico programável, chave seletora, rede Foundation Fieldbus, e demais sensores. O modelo do processo industrial ($\mathbf{G_{proc}}$) é obtido como a composição dos modelos apresentados na Seção 4.5 ($\mathbf{G_{Niveis}} \,||\, \mathbf{G_{Chave}} \,||\, \mathbf{G_{Bomba}} \,||\, \mathbf{G_{PB}} \,||\, \mathbf{G_{PV}} \,||\, \mathbf{G_{Vazao}}$), contendo 240 estados. Na estrutura com composição no gerente, essa planta enquadra-se como modelo $\mathbf{G_2}$.

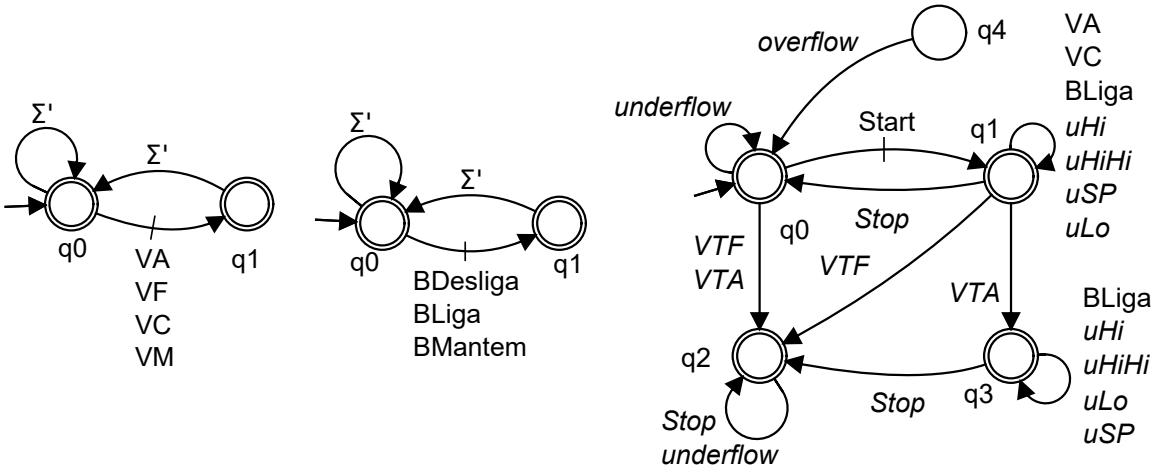
Neste exemplo, utilizando a abordagem interníveis pode ser obtido o modelo de $\mathbf{G^{op}} = \mathbf{G_1^{op}}||^I\mathbf{G_2}$, por meio da composição interníveis. O número máximo de estados dessa composição é relativo ao número de estados de $\mathbf{G_1^{op}}$, que nesse exemplo é 30, o número de elementos em T_0, que nesse caso é 6, e o número de estados em $\mathbf{G_2}$, 240 nessa aplicação, resultando em um modelo que totaliza um máximo de 43200 estados. Nesse modelo de $\mathbf{G^{op}}$ devem ser verificadas as propriedades de consistência, de acordo com as condições impostas, para projetar o controle supervisório hierárquico ótimo e não bloqueante.

Por outro lado, ao analisar os autômatos do problema apresentado, observa-se que o par ($\mathbf{G_1^{op}}$, θ_1) (Figura 64) possui consistência de controle persistente, o que implica, segundo o lema 6.3.2, que ($\mathbf{G^{op}}$, θ) possui consistência de controle estrita. Observa-se ainda que $\mathbf{G_1^{op}}$ possui todos os estados marcados, o que implica, conforme o lema 6.3.3, que existe consistência de marcação entre $\mathbf{G^{op}}$ e $\mathbf{G^{ge}}$. A partir desses dois pontos, constata-se que é possível garantir condições do teorema 6.3.2 sem a necessidade de obter o modelo de $\mathbf{G^{op}}$.

Para o processo industrial comandado pela válvula equivalente, são projetadas três especificações gerenciais conforme apresentado na figura abaixo. As especificações E_{AV} (Figura 88 – a) e E_{AB} (Figura 88 – b) dizem respeito à ação reativa do controle supervisório, ou seja, sua ação deve ocorrer como reação aos eventos da planta, onde $\Sigma' = \{start,\, stop,\, dHi,\, dSP,\, dLo,\, dLoLo,\, overflow,\, uHiHi,\, uHi,\, uSP,\, uLo,\, underflow,\, VTA,\, VTF\}$. A especificação E_M (Figura 88 – c) diz respeito aos modos de operação do sistema, onde $q0$ representa o modo de inicialização e de finalização, em que somente é permitido o fechamento da válvula; $q1$ é o modo de

operação normal, onde todos os eventos da válvula são permitidos; $q3$ representa um modo especial de operação onde a válvula trava aberta e a bomba assume o comando; o estado $q2$ representa o modo do operação de encerramento da operação, quando a válvula trava fechada ou quando a válvula trava aberta e a chave de seleção vai para a posição *stop*; o estado $q4$ indica que em nenhuma hipótese deve ocorrer *overflow* no nível do tanque.

Figura 88 – (a) E_{AV}: Especificação de ação reativa da válvula. (b) E_{AB}: Especificação de ação reativa da bomba. (c) E_M Especificação de modos de atuação.



Fonte: Elaborado pelo autor.

Para obtenção do supervisor gerencial, obtém-se primeiramente o modelo de $\mathbf{G^{ge}} = \mathbf{G_1^{ge}}||\mathbf{G_2}$ com 400 estados. A linguagem alvo $K_{Mono} = E_{AV} \mid\mid E_{AB} \mid\mid E_M \mid\mid L_m(\mathbf{G^{ge}})$, nesse caso não controlável em relação a $\mathbf{G^{ge}}$, possui 403 estados. Para análise de não bloqueio da estrutura hierárquica de acordo com o método proposto, calcula-se a máxima linguagem controlável no nível gerencial como $E^{ge} = Sup\mathcal{C}(K_{Mono})$ com 353 estados.

De acordo com o Lema 6.3.4, o único evento gerencial não confiável permanece sendo VC, o evento não confiável da válvula equivalente de controle. Dessa forma, aplicando também os lemas 6.3.2 e 6.3.3, como exposto acima, pode-se utilizar o Teorema 6.3.2 para analisar a estrutura hierárquica diretamente a partir do nível gerencial. Segundo esse teorema, além das condições verificadas para os lemas citados neste parágrafo, deve-se verificar se o alfabeto $T_{1,conf} \cup \Sigma_2$ é suficiente para prefixo fechamento de E^{ge}, o que foi feito neste exemplo utilizando a ferramenta computacional Supremica (MALIK *et al.*, 2017). Em outras palavras, verifica-se que E^{ge} permanece coacessível mesmo apagando o evento VC, cumprindo todas as condições do Teorema 6.3.2, o que garante um controle supervisório hierárquico não bloqueante para o sistema.

6.6 CONCLUSÃO DO CAPÍTULO

Neste capítulo, em adição a uma estrutura de controle supervisório hierárquico clássica, é definida a estrutura com composição no gerente. De modo a solucionar a sincronização de eventos no nível gerencial, o que exige a sincronização de eventos abstratos com eventos reais, é proposta a abordagem interníveis. Mostra-se que, utilizando a abordagem interníveis, existe equivalência entre a estrutura de controle supervisório hierárquica clássica e a estrutura com composição no gerente, o que permite utilizar os resultados dos capítulos anteriores para garantir o não bloqueio.

São definidas condições que permitem, utilizando a abordagem interníveis, a análise da estrutura hierárquica com composição no gerente sem a necessidade do custo computacional de obter o modelo do operador, ou seja, analisando somente a planta do gerente.

É apresentado um exemplo ilustrativo para mostrar a utilidade da abordagem proposta e, por fim, apresentada uma aplicação real com o circuito de válvulas que permite realizar o controle supervisório hierárquico utilizando uma válvula equivalente para comando de um processo industrial.

7 CONCLUSÕES E PERSPECTIVAS

Nesta tese são desenvolvidas estratégias de modelagem e implementação, bem como proposta uma nova abordagem para contribuir com a aplicação da teoria de controle supervisório em sistemas reais, mais especificamente processos industriais comandados por um circuito de componentes.

Visando garantir requisitos de segurança para um processo industrial de regulagem de nível, primeiramente é desenvolvida uma estratégia de modelagem que aborda a preempção de eventos não controláveis por meio dos atuadores, a interação entre o controle supervisório e o controlador PID, bem como a saturação dos atuadores. Para permitir a controlabilidade do modelo do processo industrial, que contém intrinsecamente eventos não controláveis referentes a leitura de sensores por exemplo, utilizou-se o conceito de preempção desses eventos por meio dos atuadores. A aplicação da metodologia proposta mostrou-se eficaz em um sistema de controle de nível em uma planta piloto construída sob a tecnologia Foundation Fieldbus. Por meio da síntese dos supervisores, foram projetados procedimentos seguros de inicialização e finalização do processo e os resultados mostraram a ação antecipatória, reativa e minimamente restritiva dos supervisores.

Ao abordar o controle supervisório de processos industriais comandados por um circuito de componentes, como válvulas e bombas, a problemática que surge diz respeito à complexidade computacional e de modelagem de um circuito de componentes. Foi apresentado que, mesmo para circuitos com poucas válvulas, o número de estados nos modelos cresce exponencialmente, além da dificuldade inerente na elaboração desses modelos devido a sua dimensão. A abordagem proposta para solucionar essa questão é a estratégia de modelagem por abstrações sucessivas, empregando o controle supervisório hierárquico de sistemas a eventos discretos. Como ideia geral foi proposta a utilização de níveis hierárquicos para realizar a associação de componentes aos pares e, sucessivamente, obter um modelo equivalente para ser utilizado no comando do processo industrial. Essa estratégia se mostra eficaz no sentido de evitar o crescimento exponencial no número de estados dos modelos, ao passo que, a cada nível hierárquico, o número de estados cresce de maneira polinomial. Em contrapartida, a implementação do supervisor hierárquico pressupõe uma estrutura de controle mais complexa, que envolve tanto a vocalização de eventos para os níveis superiores quanto a tradução das desabilitações de eventos abstratos em desabilitações operacionais para os níveis inferiores.

Por outro lado, observou-se que para a correta aplicação do controle supervisório hierárquico no estudo de caso inicial, algumas consistências exigidas pelos métodos existentes se mostraram demasiadamente conservadoras. Mais especificamente, constatou-se que a propriedade de observador do mapa repórter associado é

um requisito apenas suficiente para garantir um controle hierárquico não bloqueante, mas que para alguns tipos de estruturas não é uma propriedade necessária. Com isso, para a estrutura hierárquica de dois níveis a propriedade de observador foi particularizada individualmente para cada evento gerencial, sendo esses classificados em confiáveis e não confiáveis. Dessa forma, foi formalizada uma nova propriedade que se baseia na análise da co-acessibilidade da linguagem marcada de malha fechada no nível gerencial, levando em conta apenas os eventos confiáveis. Com isso foi possível elaborar novas condições para garantir o controle supervisório hierárquico ótimo e não bloqueante mesmo em estruturas em que o mapa repórter associado não é observador. Com base nesse resultado, foram criados ainda mais dois requisitos relativos aos eventos abstratos não controláveis que, juntamente com as demais condições, garantem o controle ótimo e não bloqueante para qualquer especificação gerencial controlável.

Para permitir o controle supervisório de processos industriais comandados por um modelo abstrato de válvula equivalente (obtido pela aplicação do método de associações sucessivas), foi definida a estrutura hierárquica com composição no gerente. De modo a tratar sobre a sincronização de eventos no nível gerencial nesse tipo de estrutura, ou seja, sincronização de eventos abstratos com eventos reais, foi proposta, como resultado principal da tese, a abordagem interníveis. Mostrou-se que, empregando essa abordagem, existe equivalência entre a estrutura de controle supervisório hierárquica clássica e a estrutura com composição no gerente, o que permite utilizar os resultados acima para garantir o não bloqueio. Com base nesse resultado, utilizando a abordagem interníveis, foram definidas ainda algumas condições adicionais que garantem a síntese do controle supervisório hierárquico ótimo e não bloqueante examinando apenas o nível gerencial, sem a necessidade do custo computacional de obter o modelo do operador.

De maneira ilustrativa, é apresentado um exemplo simplificado para mostrar a utilidade da abordagem proposta, detalhando suas vantagens. Por fim, é destacado um exemplo de síntese de controle supervisório hierárquico para um processo industrial comandado por um circuito de válvulas, mostrando a aplicabilidade dos métodos propostos. Com os resultados obtidos foi possível solucionar o problema de controle supervisório hierárquico de um processo industrial comandado por um circuito de componentes.

Como limitação da abordagem, pode-se mencionar que a formalização foi realizada para dois níveis hierárquicos e, para a aplicabilidade em circuitos de componentes com mais níveis é necessário um desenvolvimento adicional. Nessa linha propõe-se a definição de uma composição paralela de autômatos vocalizadores, visando completar a estrutura hierárquica proposta para a estratégia de modelagem por abstrações sucessivas. Como perspectivas para trabalhos futuros sugere-se a definição de uma arquitetura de implementação do controle supervisório hierárquico em controladores

reais.

A produção bibliográfica referente aos resultados desta tese é exposta a seguir. No *Workshop em Sistemas a Eventos Discretos - WODES 2020*, a estratégia de modelagem e implementação em um processo industrial tratada no Capítulo 3, foi apresentada com o título *Synthesis of Supervisors for a PID-Controlled Industrial Process and Implementation on Foundation Fieldbus* (OLIVEIRA *et al.*, 2020). Pretende-se ainda expandir esse tema para publicação em revista científica. A estratégia de modelagem multinível proposta no Capítulo 4 foi apresentada no *Simpósio Brasileiro de Automação Inteligente - SBAI* sob o título *Controle Supervisório Hierárquico de Processos Industriais Comandados por Circuitos de Válvulas* (OLIVEIRA *et al.*, 2021), e submetida ao Congresso Brasileiro de Automática, sob o título Controle Hierárquico de Circuitos de Componentes de Processos Industriais Modelados por Abstrações Sucessivas de Sistemas a Eventos Discretos no mês de Maio de 2024 (OLIVEIRA *et al.*, submetido[a]). Pretende-se ainda aprofundar esse tema para publicação em revista científica. O desenvolvimento formal das novas condições para flexibilizar a propriedade de observador, tratado no Capítulo 5, foi submetido ao *Journal of Discrete Event Dynamic Systems* sob o título *Hierarchical Supervision Control Of Discrete Event Systems Based On Reliable Events* no mês de Abril de 2024, onde também é trazida a proposta de padronização de notação a respeito do controle hierárquico de SEDs apresentada no Capítulo 2 (OLIVEIRA *et al.*, submetido[b]). A abordagem formal interníveis trazida no Capítulo 6, pelo seu caráter inovador, é tema de escrita de artigo científico em preparação, para revista científica conceituada (OLIVEIRA *et al.*, em preparação).

REFERÊNCIAS

ALUR, R.; COURCOUBETIS, C.; HALBWACHS, N.; HENZINGER, T.A.; HO, P.-H.; NICOLLIN, X.; OLIVERO, A.; SIFAKIS, J.; YOVINE, S. The algorithmic analysis of hybrid systems. **Theoretical Computer Science**, v. 138, n. 1, p. 3–34, 1995.

ALUR, R.; HENZINGER, T. A.; LAFFERRIERE, G.; PAPPAS, G. J. Discrete Abstractions of Hybrid Systems. **Proc. of the IEEE**, v. 88, n. 7, p. 971–984, 2000.

BALEMI, S.; HOFFMANN, G. J.; GYUGYI, P.; WONG-TOI, H.; FRANKLIN, G.F. Supervisory Control of a Rapid Thermal Multiprocessor. **IEEE Transactions on Automatic Control**, v. 38, p. 1040–1059, 1993.

BOUTIN, Olivier; KOMENDA, Jan; MASOPUST, Tomáš; SCHMIDT, Klaus; SCHUPPEN, Jan H. van. Hierarchical control with partial observations: Sufficient conditions. *In*: 2011 50th IEEE Conference on Decision and Control and European Control Conference. [*S.l.*: *s.n.*], 2011. P. 1817–1822.

BRIDGES, W.; CLARK, T. How to efficiently perform the hazard evaluation (PHA) required for non-routine modes of operation (startup, shutdown, online maintenance). *In*: 7TH Global Congress in Process Safety. Chicago: [*s.n.*], 2011.

CASSANDRAS, Christos G.; LAFORTUNE, Stephane. **Introduction to Discrete Event Systems**. 2nd. [*S.l.*]: Springer Publishing Company, Incorporated, 2008.

CHUTINAN, A.; KROGH, B. H. Computational techniques for hybrid system verification. **IEEE Transactions on Automatic Control**, v. 48, n. 1, p. 64–75, 2003.

CUNHA, A. E. C. da; CURY, J. E. R. Hierarchical Supervisory Control Based on Discrete Event Systems With Flexible Marking. **IEEE Transactions on Automatic Control**, v. 52, n. 12, p. 2242–2253, 2007.

CURY, J. E. R.; KROGH, B. H.; NIINOMI, T. Synthesis of supervisory controllers for hybrid systems based on approximating automata. **IEEE Transactions on Automatic Control**, v. 43, n. 4, p. 564–568, 1998.

FIELDBUS FOUNDATION. **Function Block Capabilities in Hybrid/Batch Applications**. [*S.l.*], 2002. Application Guide.

GONZÁLEZ, José M. E.; CUNHA, Antonio E. C. da; CURY, José E. R.; KROGH, Bruce H. Supervision of Event-Driven Hybrid Systems: Modeling and Synthesis. *In*: PROCEEDINGS of the 4th International Workshop on Hybrid Systems: Computation and Control. Berlin, Heidelberg: Springer-Verlag, 2001. (HSCC '01), p. 247–260.

GU, Tianlong; BAHRI, Parisa A. A survey of Petri Net Applications in Batch Processes. **Computers in Industry**, v. 47, n. 1, p. 99–111, 2002.

HILL, R. C.; CURY, J. E. R.; QUEIROZ, M. H.; TILBURY, D. M.; LAFORTUNE, S. Multi-Level Hierarchical Interface-Based Supervisory Control. **Automatica**, Pergamon Press, Inc., USA, v. 46, n. 7, p. 1152–1164, jul. 2010.

HOPCROFT, John E.; ULLMAN, Jeffrey D. **Introduction to Automata Theory, Languages and Computation**. 1st. [*S.l.*]: Addison-Wesley Publishing Company, 1979.

IEC 61508-1. **INTERNAT. STANDARD - Functional safety of electrical / electronic / programmable electronic safety-related systems**. [*S.l.*], 2010.

KOMENDA, Jan; MASOPUST, Tomáš; SCHUPPEN, Jan H. van. Multilevel coordination control of partially observed modular DES. *In*: 2015 American Control Conference (ACC). [*S.l.*: *s.n.*], 2015. P. 384–389.

KOUTSOUKOS, Xenofon D.; ANTSAKLIS, Panos J.; STIVER, James A.; LEMMON, Michael D. Supervisory Control of Hybrid Systems. **Proceedings of the IEEE**, v. 88, n. 7, p. 1026–1048, 2000.

LEDUC, Ryan J.; BRANDIN, Bertil A.; LAWFORD, Mark; WONHAM, W. M. Hierarchical interface-based supervisory control - Part I: Serial case. **IEEE Transactions on Automatic Control**, v. 50, n. 9, p. 1322–1335, 2005.

LEDUC, Ryan J.; LAWFORD, Mark; WONHAM, W. M. Hierarchical interface-based supervisory control - Part II: Parallel case. **IEEE Transactions on Automatic Control**, v. 50, n. 9, p. 1336–1348, 2005.

MALIK, Robi; ÅKESSON, Knut; FLORDAL, Hugo; FABIAN, Martin. Supremica–An Efficient Tool for Large-Scale Discrete Event Systems. **IFAC-PapersOnLine**, v. 50, n. 1, p. 5794–5799, 2017. 20th IFAC World Congress. ISSN 2405-8963.

MOOR, T.; RAISCH, J.; O'YOUNG, S.D. Discrete supervisory control of hybrid systems based on l-complete approximations. **Discrete Event Dynamic Systems: Theory and applications**, v. 12, p. 83–107, 2002.

MOORE, Edward F. Gedanken-Experiments on Sequential Machines. *In*: **Automata Studies**. Edição: Claude Shannon e John McCarthy. Princeton, NJ: Princeton University Press, 1956. v. 1 cap. 5, p. 129–153.

MULER, O. P. **Síntese e Implementação de Controle Supervisório de Processos Industriais com Malha de Válvulas**. 2018. Diss. (Mestrado) – Universidade Federal de Santa Catarina, Brasil.

MULER, O. P.; QUEIROZ, M. H.; CURY, J. E. R. Síntese e Implementação de Controle Supervisório em Rede Foundation Fieldbus. *In*:
AUTOMÁTICA, Congresso Brasileiro de (Ed.). **Anais do XXII Congresso Brasileiro de Automática**. João Pessoa: [*s.n.*], 2018.

NILSSON, J.W.; RIEDEL, S.A. **Circuitos Elétricos**. [*S.l.*]: PRENTICE HALL BRASIL, 2015.

NOVA SMAR S/A. **PD3-302 - Planta Didática FOUNDATION™ Fieldbus**. [*S.l.*: *s.n.*], 2023. `https://www.smar.com/pt/produto/pd3-302-planta-didatica-foundation-fieldbus`. Acessado em: 27/09/2023.

OLIVEIRA, R. G.; QUEIROZ, M. H.; CURY, J. E. R. Controle Hierárquico de Circuitos de Componentes de Processos Industriais Modelados por Abstrações Sucessivas de Sistemas a Eventos Discretos. *In*: CONGRESSO Brasileiro de Automática 2024. Rio de Janeiro - RJ: [*s.n.*], submetido.

OLIVEIRA, R. G.; QUEIROZ, M. H.; CURY, J. E. R. Controle Supervisório Hierárquico de Processos Industriais Comandados por Circuitos de Válvulas. *In*: SIMPÓSIO Brasileiro de Automação Inteligente 2021. Rio Grande - RS: [*s.n.*], 2021.

OLIVEIRA, R. G.; QUEIROZ, M. H.; CURY, J. E. R. Hierarchical Supervisory Control of Discrete Event Systems Based On Reliable Events. **Journal of Discrete Event Dynamic Systems**, submetido.

OLIVEIRA, R. G.; QUEIROZ, M. H.; CURY, J. E. R. Inter-Level Approach for Hierarchical Supervisory Control of Discrete Event Systems, em preparação.

OLIVEIRA, R. G.; QUEIROZ, M. H.; CURY, J. E. R. Synthesis of Supervisors for a PID-Controlled Industrial Process and Implementation on Foundation Fieldbus. *In*: WORKSHOP of Discrete Event Systems 2020. Rio de Janeiro: [*s.n.*], 2020.

PETTERSSON, Stefan; LENNARTSON, Bengt. Stability of Hybrid Systems Using LMIs — A Gear-Box Application. *In*: LYNCH, Nancy; KROGH, Bruce H. (Ed.). **Hybrid Systems: Computation and Control**. Berlin, Heidelberg: Springer Berlin Heidelberg, 2000. P. 381–395.

PU, K. G. **Modeling and Control of Discrete-Event Systems with Hierarchical Abstraction**. 2000. Diss. (Mestrado) – Systems Control Group, Department of Electrical & Computer Engineering, University of Toronto, Canadá.

QUEIROZ, M. H.; CURY, J. E. R. Modular Control of Composed Systems. *In*: PROCEEDINGS of the American Control Conference. Chicago: [*s.n.*], 2000.

QUEIROZ, M. H.; CURY, J. E. R. Modular Multitasking Supervisory Control of Composite Discrete-Event Systems. *In*: 16TH IFAC World Congress. Prague: [*s.n.*], 2005.

QUEIROZ, M. H.; CURY, J. E. R.; WONHAM, W. M. Multitasking Supervisory Control of Discrete-Event Systems. **Discrete Event Dynamic Systems**, v. 15, p. 375–395, 2005.

RAISCH, J.; O'YOUNG, S. D. Discrete approximation and supervisory control of continuous systems. **IEEE Transactions on Automatic Control**, v. 43, n. 4, p. 569–573, 1998.

RAMADGE, P. J.; WONHAM, W. M. The Control of Discrete Event Systems. **Proceedings of IEEE: Special Issue on Discrete Event Dynamic Systems**, v. 77, p. 81–98, 1989.

SANCHEZ, A. **Formal Specification and Synthesis of Procedural Controllers for Process Systems**. London: Lecture Notes on Control e Information Sciences, Vol 212. Springer, 1996.

SCHMIDT, K.; BREINDL, Christian. Maximally Permissive Hierarchical Control of Decentralized Discrete Event Systems. **IEEE Transactions on Automatic Control**, v. 56, n. 4, p. 723–737, 2011.

SCHMIDT, K.; BREINDL, Christian. On maximal permissiveness of hierarchical and modular supervisory control approaches for discrete event systems. *In*: 2008 9th International Workshop on Discrete Event Systems. [*S.l.*: *s.n.*], 2008. P. 462–467.

SCHMIDT, K.; MOOR, T.; PERK, S. Nonblocking Hierarchical Control of Decentralized Discrete Event Systems. **IEEE Transactions on Automatic Control**, v. 53, n. 10, 2008.

SEOW, Kiam Tian. Organizational Control of Discrete-Event Systems: A Hierarchical Multiworld Supervisor Design. **IEEE Transactions on Control Systems Technology**, v. 22, n. 1, p. 23–33, 2014.

SIMON, Herbert A. The Architecture of Complexity. **Proceedings of the American Philosophical Society**, American Philosophical Society, v. 106, n. 6, p. 467–482, 1962. ISSN 0003049X.

SKOUSEN, Philip L. **Valve Handbook**. 3rd ed. New York: McGraw-Hill, 2011.

SU, R.; WONHAM, W. M. On Supervisor Reduction in DES. **Disc.-Event Dynamic Systems**, v. 14, p. 31–53, 2004.

TITTUS, Michael; ÅKESSON, Knut. Modular Supervisors for Deadlock Avoidance in Batch Processes. *In*: 764–769 vol.1.

TORRICO, César R.C.; CURY, J. E. R. HIERARCHICAL SUPERVISORY CONTROL OF DISCRETE EVENT SYSTEMS BASED ON STATE AGGREGATION. **IFAC Proceedings Volumes**, v. 35, n. 1, p. 169–174, 2002. 15th IFAC World Congress. ISSN 1474-6670.

VIEIRA, A. D.; SANTOS, E. A. P.; QUEIROZ, M. H. de; LEAL, A. B.; PAULA NETO, A. D. de; CURY, J. E. R. A Method for PLC Implementation of Supervisory Control of Discrete Event Systems. **IEEE Transactions on Control Systems Technology**, v. 25, p. 175–191, 2017.

WONG, K. C.; WONHAM, W. M. Hierarchical Control of Discrete-Event Systems. **Discrete Event Dynamic Systems**, v. 6, n. 3, p. 241–273, 1996.

WONG, K. C.; WONHAM, W. M. Modular Control and Coordination of Discrete-Event Systems. **Discrete Event Dynamic Systems**, v. 8, n. 3, p. 247–297, 1998.

WONHAM, W. M.; CAI, K. **Supervisory Control of Discrete-Event Systems**. [*S.l.*]: Springer International Publishing, 2019.

WONHAM, W. M.; CAI, K.; RUDIE, K. Supervisory Control of Discrete-Event Systems: A Brief History. **Annual Reviews in Control**, v. 45, p. 250–256, 2018.

WONHAM, W. M.; RAMADGE, P. J. Modular Supervisory Control of DES. **Math. of Control of DES**, v. 1, p. 13–30, 1988.

YAMALIDOU, E.C.; KANTOR, J.C. Modeling and Optimal Control of Discrete-Event Chemical Processes Using Petri Nets. **Computers & Chemical Engineering**, v. 15, n. 7, p. 503–519, 1991.

YEH, Ming-Li; CHANG, Chuei-Tin. An Automata Based Method for Online Synthesis of Emergency Response Procedures in Batch Processes. **Computers & Chemical Engineering**, v. 38, p. 151–170, 2012.

ZAMANI FEKRI, Mohsen; HASHTRUDI-ZAD, Shahin. Hierarchical supervisory control of discrete-event systems under partial observation. *In*: PROCEEDINGS of the 48h IEEE Conference on Decision and Control (CDC) held jointly with 2009 28th Chinese Control Conference. [*S.l.*: *s.n.*], 2009. P. 181–186.

ZHONG, H. **Hierarchical control of discrete-event systems**. 1992. Tese (Doutorado) – Department of Electrical Engineering, University of Toronto.

ZHONG, H.; WONHAM, W. M. On the Consistency of Hierarchical Supervision in Discrete-Event Systems. **IEEE Transactions on Automatic Control**, v. 35, n. 10, p. 1125–1134, 1990.