Controle Supervisório Hierárquico de Processos Industriais Comandados por Circuito de Válvulas

Rafael Garlet de Oliveira [*] **Max Hering de Queiroz** [**]
José Eduardo Ribeiro Cury [**]

[*] *Campus Luzerna, Instituto Federal Catarinense, Luzerna - SC, (e-mail: rafael.oliveira@ifc.edu.br)*
[**] *Dep. de Automação e Sistemas, Universidade Federal de Santa Catarina, Florianópolis - SC (e-mail: [max.queiroz, jose.cury]@ufsc.br)*

Abstract:
This paper proposes a multilevel modelling strategy for the supervisory control of industrial processes commanded by circuits of valves subject to failure. The method aims to reduce the complexity of modelling the process and of synthesis of supervisors by exploring the theory of multilevel hierarchical supervisory control of discrete event systems. At each hierarchical level, the valves are successively associated in series or in parallel and abstractions are obtained in intermediate equivalent models with an isomorphic structure to that of a single valve. From the composition of the equivalent valve with the other components of the plant, the method allows the synthesis of a control logic reactive to discrete events, which imposes safety specifications to the process in a minimally restrictive, controllable and non-blocking manner. As a result, a multilevel hierarchical supervisory control implementation architecture is proposed, which is applied to a level control process by the action of a pump and four block valves subject to locking, highlighting the advantages of the proposed strategy to facilitate the modelling of plant and specifications and to reduce the computational complexity of synthesis.

Resumo:
Este artigo propõe uma estratégia de modelagem multinível para o controle supervisório de processos industriais comandados por circuitos de válvulas sujeitas a falhas. O método visa reduzir a complexidade de modelagem do processo e da síntese de supervisores explorando a teoria de controle supervisório hierárquico multinível de sistemas a eventos discretos. A cada nível hierárquico, as válvulas são associadas sucessivamente em série ou em paralelo e são obtidas abstrações em modelos equivalentes intermediários com estrutura isomórfica à de uma única válvula. A partir da composição da válvula equivalente com os demais componentes da planta, o método permite a síntese de uma lógica de controle reativa a eventos discretos, que impõe especificações de segurança ao processo de forma minimamente restritiva, controlável e não-bloqueante. Como resultado é proposta uma arquitetura de implementação do controle supervisório hierárquico multinível, que é aplicada a um processo de controle de nível pela ação de uma bomba e quatro válvulas de bloqueio sujeitas a travamento, evidenciando as vantagens da estratégia proposta para facilitar a modelagem de planta e especificações e para reduzir a complexidade computacional da síntese.

Keywords: Discrete event systems; supervisory control theory; hierarchical supervisory control; industrial processes; industrial valves.

Palavras-chaves: Sistemas a eventos discretos; teoria do controle supervisório; controle supervisório hierárquico; processos industriais; válvulas industriais.

1. INTRODUÇÃO

Em diversos processos industriais as válvulas desempenham papel fundamental. Em muitos casos, esses elementos atuam de maneira associada, em estruturas em série ou paralelo, o que constitui os circuitos de válvulas. Para este tipo de processo, a aplicação de métodos formais é um requisito indispensável, devido aos riscos envolvidos (Bridges e Clark, 2011). Dentre os trabalhos existentes que envolvem o controle supervisório de processos industriais comandados por circuitos de válvulas, um tema ainda a ser explorado é a complexidade de síntese de supervisores. No geral, a composição de válvulas em circuitos causa o crescimento exponencial dos modelos resultantes, o que pode inviabilizar aplicações práticas (Yamalidou e Kantor, 1991; Yeh e Chang, 2012). Além disso, os métodos existentes para controle supervisório de sistemas híbridos são demasiadamente complexos no que diz respeito aos modelos resultantes e procedimentos utilizados (Koutsoukos et al., 2000; Alur et al., 2000).

A teoria de controle supervisório (TCS) se apresenta como um método formal para o projeto de sistemas a even-

tos discretos (SEDs), objetivando o desenvolvimento de sistemas seguros (Ramadge e Wonham, 1989). Algumas técnicas desenvolvidas têm o objetivo de reduzir a complexidade de síntese da TCS, como por exemplo o controle modular de SEDs (Wonham e Ramadge, 1988) e o controle supervisório hierárquico (Zhong e Wonham, 1990). Considerando a modelagem e síntese para circuitos de válvulas aplicados a processos industriais, destacam-se os trabalhos de Yamalidou e Kantor (1991) que abordam a questão utilizando as redes de Petri para projetar controladores para o processo, sem considerar falhas nas válvulas; Yeh e Chang (2012) que obtêm supervisores de resposta a emergências em processos a bateladas, tratando também a questão de falhas e travamento em válvulas e Tittus e Lennartson (1999) que aplicam o controle hierárquico de SEDs, por meio das redes de Petri em processos em batelada, conseguindo uma certa redução da complexidade computacional exigida. O trabalho seminal de Sampath et al. (1996) introduz técnicas baseadas em autômatos com observação parcial para diagnóstico de falhas não observáveis com aplicação em válvulas de controle.

O objetivo deste trabalho consiste em propor uma estratégia de modelagem multinível 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 sujeitas a falhas de travamento, considerando-se as falhas como eventos observáveis. Com o método proposto, o modelo de abstração de válvula equivalente é utilizado como elemento que compõe o processo industrial, o que permite calcular seu controle supervisório. Como abordagem de modelagem do processo industrial, são utilizados os conceitos de abstrações discretas dos sinais contínuos e preempção de eventos por meio dos atuadores, conforme já explorado em um trabalho preliminar em que foi realizado o controle modular de um processo industrial contendo apenas uma válvula e implementação em Foundation Fieldbus (Oliveira et al., 2020). A abordagem utilizada contrasta de métodos já existentes que modificam a TCS de modo a considerar eventos forçados (Sanchez, 1996; Balemi et al., 1993). Como resultado, propõe-se uma arquitetura de implementação do controle supervisório hierárquico multinível, que é aplicada a um processo de controle de nível pela ação de uma bomba hidráulica e de um circuito com quatro válvulas de bloqueio redundantes sujeitas a falhas de travamento observáveis.

2. CONTROLE SUPERVISÓRIO HIERÁRQUICO DE SEDS

2.1 Teoria do Controle Supervisório

Na TCS, o comportamento de um SED é modelado por um autômato definido por uma quíntupla $\mathbf{G} = (Q, \Sigma, f, q_0, Q_m)$, onde Q é o conjunto de estados, $\Sigma = \Sigma_c \cup \Sigma_u$ é o alfabeto ou conjunto de símbolos que representam eventos controláveis (Σ_c) e não controláveis (Σ_u), $f : \Sigma \times Q \to Q$ é uma função de transição parcial, $q_0 \in Q$ é o estado inicial e $Q_m \subseteq Q$ é um conjunto de estados marcados. O conjunto de todas as sequências de eventos formadas por elementos de um alfabeto Σ é definida por Σ^*. O comportamento de malha aberta de um SED representado por um autômato $\mathbf{G}$ pode ser descrito pela linguagem $L(\mathbf{G}) \subseteq \Sigma^*$. A linguagem $L_m(\mathbf{G}) \subseteq L(\mathbf{G})$ contém todas as cadeias marcadas, ou seja, cadeias que representam tarefas completas. A operação do produto síncrono, denotada por $\|$, é utilizada para composição de autômatos ou linguagens.

Um supervisor marcador, para uma planta $\mathbf{G}$, é definido por uma função $S : L(\mathbf{G}) \to \Delta$, onde $\Delta = \{\delta \in 2^{\Sigma} : \delta \subseteq \Sigma_c\}$ e uma linguagem marcada $M \subseteq L_m(\mathbf{G})$. O comportamento marcado de um sistema em malha fechada é representado por $L_m(S/\mathbf{G}) = L(S/\mathbf{G}) \cap M$, onde $L(S/\mathbf{G})$ contém as cadeias de $L(\mathbf{G})$ que não são desabilitado por S. Um supervisor é não bloqueante quando $L(S/\mathbf{G}) = \overline{L_m(S/\mathbf{G})}$. A condição necessária e suficiente para a existência de um supervisor não bloqueante S que imponha uma especificação $K \subseteq L_m(\mathbf{G})$ para uma planta $\mathbf{G}$ é a controlabilidade de K. Uma linguagem K é definida controlável em relação a $\mathbf{G}$ se $\overline{K}\Sigma_u \cap L(\mathbf{G}) \subseteq \overline{K}$. A classe das linguagens controláveis contidas na especificação K possui um elemento supremo $SupC(K, \mathbf{G})$, que é o comportamento mais permissivo possível a ser implementado por um supervisor em uma planta $\mathbf{G}$, garantindo uma especificação K. Um supervisor S pode ser representado por um autômato $\mathbf{S}$ e um mapa ϕ, que relaciona seus estados a desabilitações. O número de estados de um supervisor pode ser reduzido pelo método apresentado em Su e Wonham (2004). Um supervisor ótimo é tal que $L_m(\mathbf{S}||\mathbf{G}) = SupC(K, \mathbf{G})$.

2.2 Controle Hierárquico de SEDs

A arquitetura para controle supervisório hierárquico de SEDs, apresentada na Figura 1, é uma alternativa para reduzir a complexidade na síntese de supervisores, pois divide em níveis hierárquicos a estrutura de um sistema. Na figura, os sufixos *op* se referem ao nível operacional, com uma planta $\mathbf{G_{op}}$ e um supervisor S_{op}, e os sufixos *ge*, ao nível gerencial, com planta $\mathbf{G_{ge}}$ e supervisor S_{ge}. O canal de informações Inf_{og} é representado como um mapa repórter $\theta : L(\mathbf{G_{op}}) \to \Sigma_{ge}^*$, definido recursivamente como $\theta(\epsilon) = \epsilon$ e $\theta(s\sigma) = \theta(s)$ ou $\theta(s\sigma) = \theta(s)\tau$, onde ϵ representa a cadeia vazia, $s \in L(\mathbf{G_{op}})$, $\sigma \in \Sigma_{op}$ e $\tau \in \Sigma_{ge}$. O canal de informações Com_{go} é definido como diretrizes de comando do supervisor do gerente, que devem ser traduzidas como sinais de controle para o nível operacional. Na arquitetura de dois níveis apresentada, o modelo de $\mathbf{G_{op}}$ consiste em um autômato de Moore, que é um autômato como o definido como na Seção 2.1, acrescentando-se os elementos T_0 e $\omega : Q \to T_0$, onde Q é o conjunto de estados de $\mathbf{G_{op}}$ e T_0 é seu alfabeto de saída contendo os eventos a serem vocalizados ao nível hierárquico superior (Zhong e Wonham, 1990). Em arquiteturas multinível, considerando as plantas de cada nível, somente a planta gerencial não é modelada como autômato de Moore (Schmidt et al., 2007).

De modo a atender corretamente as especificações e garantir ausência de bloqueio, em uma arquitetura hierárquica os modelos devem apresentar algumas propriedades, que serão mencionadas brevemente a seguir. Os elemen-

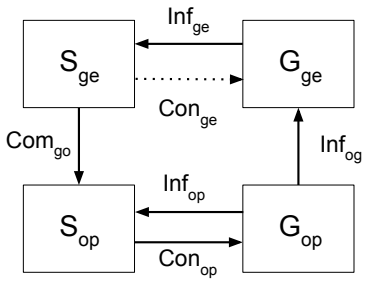

Figura 1. Arquitetura de Controle Hierárquico (Zhong e Wonham, 1990)

tos ($\mathbf{G_{op}}, \theta$) apresentam consistência de controle sempre que é possível determinar sem ambiguidades a controlabilidade dos eventos vocalizados para o nível gerencial. Desta forma, define-se que uma estrutura com consistência de controle e que também não apresenta as denominadas palavras vocais parceiras, como definido em Zhong e Wonham (1990), possui a propriedade de consistência hierárquica. Com essa propriedade, em uma estrutura hierárquica garante-se que toda linguagem implementada no nível gerencial é igual à imagem de um comportamento implementado no nível do operador.

De forma geral, Wong e Wonham (1996) determinam que para a estrutura hierárquica não possuir bloqueios, além das propriedades já mencionadas, existem duas condições suficientes: que o mapa repórter satisfaça a propriedade de observador e que haja consistência de marcação.

3. O PROCESSO INDUSTRIAL ESTUDADO

O processo industrial estudado é inspirado em uma planta piloto construída por Smar Automação Industrial e localizada no Departamento de Automação e Sistemas na Universidade Federal de Santa Catarina. A planta é equipada com instrumentos inteligentes que se comunicam por meio de uma rede Foundation Fieldbus (FF).

No presente estudo, o processo em questão, ilustrado de forma simplificada na Figura 2, é constituído de um tanque que recebe líquido de uma bomba centrífuga, um circuito de válvulas de bloqueio, que regula o nível de líquido no tanque, uma chave seletora (com sinais de *Start* e *Stop*) e um CLP. Este último é capaz de se comunicar, pela rede FF, com o sensor de nível (LIT) e com as válvulas de bloqueio, além de receber os sinais da chave seletora e comandar o acionamento da bomba. Considera-se que cada uma das válvulas que compõem o circuito seja um instrumento inteligente e dotado de mecanismo de diagnóstico de falhas para detectar a ocorrência de travamentos na posição aberta ou fechada. O presente estudo difere do trabalho preliminar apresentado em Oliveira et al. (2020) onde realizou-se o controle modular de um processo industrial com apenas uma válvula de controle e implementação em rede FF.

O circuito de válvulas é constituído por quatro elementos: duas válvulas em série, associadas em paralelo a outras duas válvulas em série. Nessa configuração, todas as válvulas são categorizadas como de bloqueio, cuja função é impedir ou liberar a passagem de fluido. Desta maneira, explora-se a redundância quanto à ocorrência de travamento nas válvulas, de modo que a vazão resultante no duto possa permanecer sob controle mesmo com o travamento de uma, duas ou até três válvulas, dependendo da configuração das falhas. Considerando algumas hipóteses de modelagem, apresentadas na próxima seção, deseja-se obter um modelo que seja a abstração para uma única válvula equivalente, que represente o comportamento resultante do circuito de válvulas.

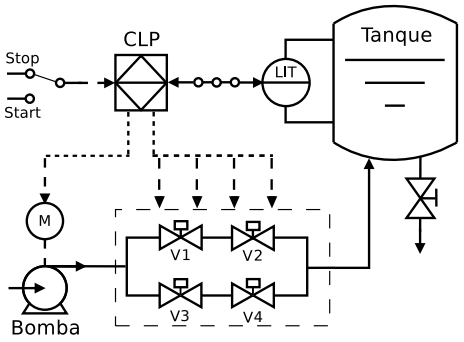

Figura 2. Processo Industrial Estudado

O comportamento desejado para o processo em malha fechada deve considerar especificações de segurança na operação dos dispositivos durante os procedimentos de inicialização, finalização e em regime permanente. No funcionamento do processo deve ser evitado transbordamento do tanque (*overflow*) em qualquer situação. O esvaziamento do tanque (*underflow*) deve ser evitado na inicialização e em regime permanente. Nas situações em que há vazão livre no duto devido ao travamento de válvulas abertas, a bomba deve assumir o controle de nível evitando *underflow* e *overflow*. Já nas situações em que a vazão do duto é bloqueada devido ao travamento de válvulas fechadas, o processo deve ser finalizado.

4. MODELAGEM E CONTROLE SUPERVISÓRIO DO PROCESSO INDUSTRIAL

Nesta seção, apresenta-se o controle supervisório do processo industrial, considerado como nível gerencial na arquitetura hierárquica proposta neste trabalho. Neste nível, portanto, o circuito de válvulas resume-se a uma válvula equivalente, cujo modelo abstrato recebe apenas o controle supervisório virtual no nível gerencial, sendo que seu controle real se dá ao longo dos níveis hierárquicos operacionais da estrutura. Conforme detalhado na Seção 5, a obtenção do modelo abstrato da válvula equivalente se dá por meio de associações em série e paralelo em uma arquitetura hierárquica multinível.

4.1 Modelagem do Processo Industrial

O comportamento em malha aberta do processo industrial é composto por modelos de sete subsistemas que serão apresentados no decorrer desta seção. $\mathbf{G_{Niveis}}$ corresponde ao modelo discreto dos níveis de líquido no tanque (Figura 3 (a)). Como o nível no tanque é uma variável contínua, são definidos sete intervalos de operação, divididos por limiares que correspondem aos eventos de alarme utilizados na rede FF (Fieldbus Foundation, 2002). O transbordamento e esvaziamento do tanque são representados por *overflow* e *underflow* respectivamente. Os eventos *uHiHi* e *dLoLo*

levam a estados críticos, próximos a situações de *overflow* e *underflow* respectivamente. Os eventos *uHi* e *dLo* levam a estados de alerta, quando o nível se afasta da região de *set point*. Os eventos *uSP* e *dSP* indicam que o nível do líquido se aproxima da região de *set point*. Observa-se que todos os eventos de $\mathbf{G_{Niveis}}$ são não controláveis.

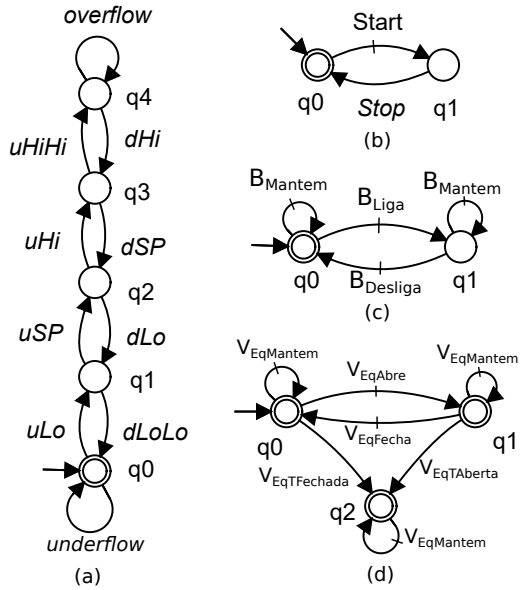

Figura 3. (a) $\mathbf{G_{Niveis}}$: níveis do líquido no tanque; (b) $\mathbf{G_{Chave}}$: chave seletora; (c) $\mathbf{G_{Bomba}}$: bomba centrífuga; (d) $\mathbf{G_{VEquivalente}}$: modelo da abstração da válvula equivalente.

O modelo da chave seletora, $\mathbf{G_{Chave}}$ – Figura 3 (b), conta com dois eventos. Este componente dá ao operador a opção de escolher entre a inicialização e a finalização do processo, o que define os modos de operação. Assume-se que o evento *Start* seja controlável, para que a solicitação de início de operação possa ser desabilitada (desconsiderada) pelo CLP dependendo do estágio em que o processo se encontra. Já o evento *Stop* é não controlável, pois a finalização da operação pode ser solicitada a qualquer tempo. O modelo da bomba centrífuga, $\mathbf{G_{Bomba}}$, é apresentado na Figura 3 (c). Além da possibilidade de ligar e desligar a bomba, esse modelo expressa que é possível também a decisão de manter a bomba no mesmo estado. O modelo $\mathbf{G_{VEquivalente}}$ (Figura 3 (d)) representa o comportamento da abstração da válvula equivalente referente ao circuito de válvulas. Este modelo expressa que a vazão resultante no duto é observada pelo processo em nível gerencial como sendo controlada por uma única válvula equivalente. Os eventos controláveis V_{EqAbre}, $V_{EqFecha}$ e $V_{EqMantem}$ indicam respectivamente a liberação da vazão no duto pelo circuito de válvulas, bloqueio da vazão no duto e a decisão de manter inalterada a abertura ou fechamento resultante do circuito de válvulas. Os eventos não controláveis $V_{EqTAberta}$ e $V_{EqTFechada}$ indicam situações em que um determinado conjunto de válvulas do circuito passa a uma situação de travamento aberto ou fechado respectivamente. Considera-se que após o travamento da válvula, somente o evento $V_{EqMantem}$ seja possível na mesma. A válvula pode apenas travar aberta se estiver na posição aberta, e travar fechada se estiver fechada.

Para garantir a controlabilidade do sistema em malha fechada, é feita uma hipótese de modelagem que assegura que, entre dois eventos da planta, sejam mudanças de nível, comandos da chave seletora ou travamentos da válvula, sempre ocorra uma decisão sobre a ação de cada um dos atuadores, que neste caso são a bomba e a válvula equivalente. Esta hipótese se traduz nos modelos de preempção da válvula equivalente, $\mathbf{G_{PV}}$, e da bomba, $\mathbf{G_{PB}}$. A Figura 4 ilustra o modelo $\mathbf{G_{PV}}$, onde $\Sigma_{planta} = \{uLo, uSp, uHi, uHiHi, overflow, dHi, dSp, dLo. dLoLo, underflow, Start, Stop, V_{EqTAberta}, V_{EqTFechada}\}$.

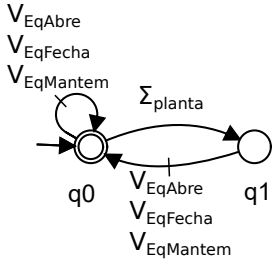

Figura 4. $\mathbf{G_{PV}}$: modelo de preempção da válvula equivalente.

Como último subsistema que compõe o processo industrial, destaca-se o modelo de vazão de líquido no tanque $\mathbf{G_{Vazao}}$, ilustrado na Figura 5, onde $\Sigma_{Lu} = \{uLo, uSp, uHi, uHiHi\}$ são os eventos em que o nível de líquido aumenta e $\Sigma_{Ld} = \{dHi, dSp, dLo.dLoLo\}$, em que o nível de líquido diminui. Esse modelo representa como pode ocorrer a variação de nível no tanque conforme os estados da bomba e da válvula.

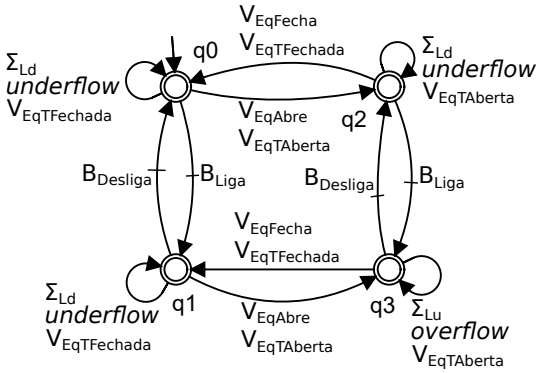

Figura 5. $\mathbf{G_{Vazao}}$: modelo de vazão no tanque.

4.2 Modelagem das Especificações

Para garantir os requisitos do sistema em malha fechada são consideradas três especificações. E_{AV} e E_{AB} determinam a ação reativa da válvula equivalente e da bomba respectivamente. Estas especificações impõem que as ações dos atuadores sejam sempre decididas como resposta aos eventos da planta, sejam mudanças de nível, comando na chave seletora ou travamento da válvula equivalente, conforme ilustrados nas Figuras 6 (a) e (b) que apresentam os autômatos que modelam as linguagens E_{AV} e E_{AB}. O modelo da Figura 6 (c) descreve a especificação de modos de operação, E_M. O estado inicial expressa tanto as condições iniciais do processo, quanto o modo de finalização. Neste estado permite-se que ocorra *underflow*,

mas não é permitido que a válvula equivalente abra, nem a bomba ligue, assim como não é desejável que o nível de líquido do tanque aumente. O estado q_1 expressa a inicialização do processo, bem como o regime permanente. Nesse estado, não deseja-se que ocorra *underflow*. O estado q_3 é atingido quando, depois de inicializado o processo, a válvula equivalente travar aberta. Nesse caso, o processo continua operando, mas com o controle de nível realizado por meio da bomba. O estado q_2 refere-se a uma situação em que o processo é finalizado por apresentar problemas na válvula. O estado não acessível q_4 indica que em nenhum estado acessível é permitida a ocorrência de *overflow*.

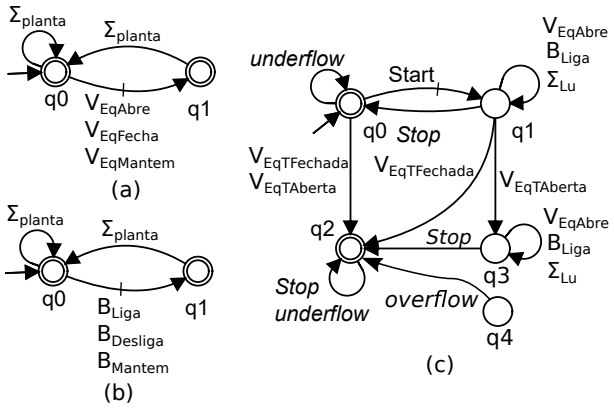

Figura 6. (a) E_{AV}: especificação de ação reativa na válvula; (b) E_{AB}: especificação de ação reativa na bomba; (c) E_M: especificação de modos de operação.

4.3 Síntese do Supervisor

Para a obtenção do supervisor, primeiramente é feito o produto síncrono de todos os subsistemas que compõem a planta: $\mathbf{G} = \mathbf{G_{Niveis}} \,||\, \mathbf{G_{Chave}} \,||\, \mathbf{G_{Bomba}} \,||\, \mathbf{G_{VEquivalente}} \,||\, \mathbf{G_{PV}} \,||\, \mathbf{G_{PB}} \,||\, \mathbf{G_{Vazao}}$, com $\mathbf{G}$ apresentando 320 estados. O supervisor S, representado por um autômato não-bloqueante $\mathbf{S}$, é obtido pela máxima linguagem controlável, tal que $L_m(\mathbf{S}||\mathbf{G}) = SupC(K, \mathbf{G})$, onde $K = E_{AV}||E_{AB}||E_M||L_m(\mathbf{G})$, em que $\mathbf{S}$ contém 290 estados e sua versão reduzida, 68 estados. O supervisor ótimo representa uma lógica de controle reativa aos eventos discretos do processo, que garante todas as especificações de segurança no acionamento da válvula equivalente e da bomba, de forma minimamente restritiva e não-bloqueante. As próximas seções explicam como os eventos gerenciais da válvula equivalente se relacionam com os eventos operacionais das quatro válvulas de bloqueio do circuito.

5. MODELAGEM MULTINÍVEL DO CIRCUITO DE VÁLVULAS

5.1 Arquitetura Multinível

A fim de propor um método para controle supervisório de circuitos de válvulas é empregado o controle supervisório hierárquico de SEDs. A arquitetura multinível proposta para tratar o problema estudado é apresentada na Figura 7, tendo como objetivo reduzir a complexidade de síntese de supervisores. Pretende-se realizar associações sucessivas de pares de válvulas, obtendo, a cada associação, uma abstração equivalente intermediária, resultando ao fim em uma abstração que represente o comportamento de uma única válvula equivalente no duto. O modelo da abstração da válvula equivalente pode então ser utilizado no controle supervisório do processo industrial.

Para o problema estudado neste artigo, a estrutura conta com três níveis hierárquicos, onde o nível operacional inferior corresponde às associações das válvulas em série (V_1 em série com V_2, V_3 em série com V_4, conforme a Figura 2). Nesse nível, 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, como detalhado na próxima subseção. Este 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. Neste 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.

5.2 Modelagem Para Válvulas em Série

O modelo proposto para representar as válvulas de bloqueio são compostos por três estados: fechada, aberta e travada, conforme ilustrado na Figura 8. Neste caso, é considerado que uma válvula somente pode travar aberta se estiver na posição aberta e travar fechada se estiver na posição fechada. Neste 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. Assim, V_1 e V_3 iniciam fechadas, enquanto que V_2 e V_4, abertas.

Nesta abordagem, para cada associação de válvula. em cada nível de abstração, propõe-se obter um supervisor local para garantir requisitos locais. Nas associações em série, a especificação de prioridade E_{12}, cujo modelo é ilustrado na Figura 9, habilita a operação da válvula 2 somente após a válvula 1 travar aberta. Para a planta local $\mathbf{G_1}||\mathbf{G_2}$, essa especificação resulta em um supervisor local S_{12} com 9 estados, reduzido a R_{12} com 2 estados.

Na arquitetura de controle hierárquico, a planta operacional consiste em um autômato de Moore que vocaliza os estados relevantes com eventos para o nível hierárquico acima. 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 $\mathbf{G_{12}^{voc}}$, que associa estados de $\mathbf{G_1^V}||\mathbf{G_2^V}$ a eventos abstratos de Σ_{12}^{eq} conforme a

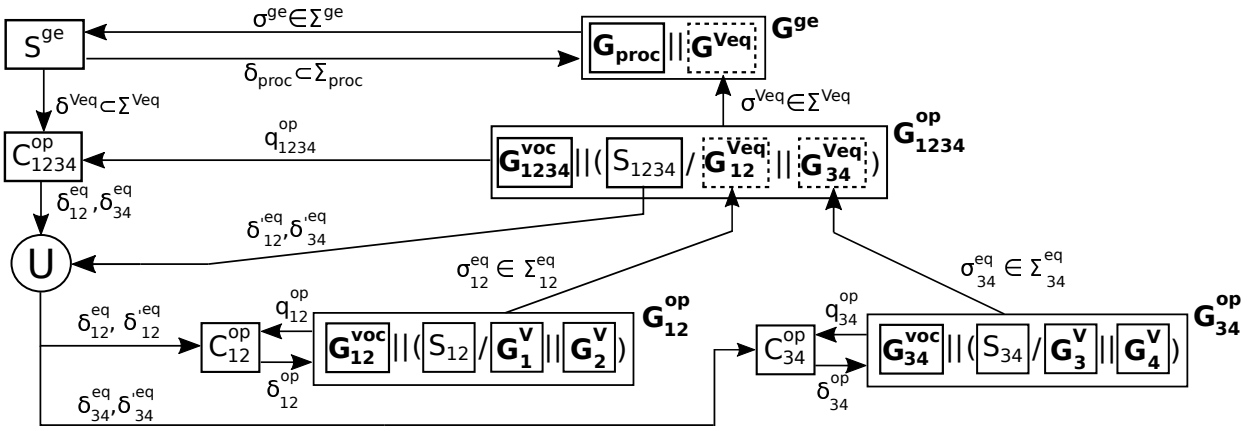

Figura 7. Arquitetura multinível para circuito de válvulas, onde $\mathbf{G_{12}^{op}}$ e $\mathbf{G_{34}^{op}}$ são as plantas do operador associando as válvulas em série, $\mathbf{G_{1234}^{op}}$ representa a associação em paralelo, $\mathbf{G^{Veq}}$ é a abstração do circuito numa válvula equivalente e $\mathbf{G_{proc}}$ modela os demais componentes do processo industrial.

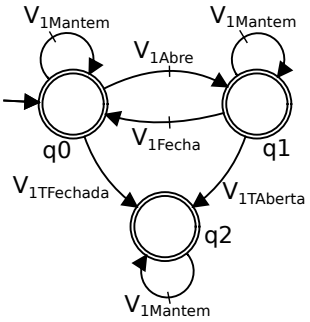

Figura 8. $\mathbf{G_1^V}$: modelo para válvulas de bloqueio.

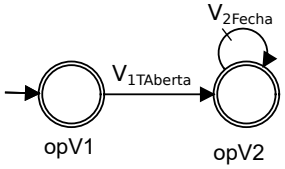

Figura 9. E_{12}: especificação local para válvulas em série.

combinação dos estados das válvulas altera a configuração do circuito em série. Por exemplo, no estado inicial, com V_1 fechada e V_2 aberta, se ocorrer V_{1Abre}, $\mathbf{G_{12}^{voc}}$ vocaliza V_{12Abre}; ocorrendo $V_{1TFechada}$, é vocalizado $V_{12TFechada}$; mas, ocorrendo $V_{2TAberta}$, nenhum evento é vocalizado. 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 (Figura 10). 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 hierárquico acima, para sinais de controle para as válvulas. 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 e Wonham (1990), como o último evento contro-

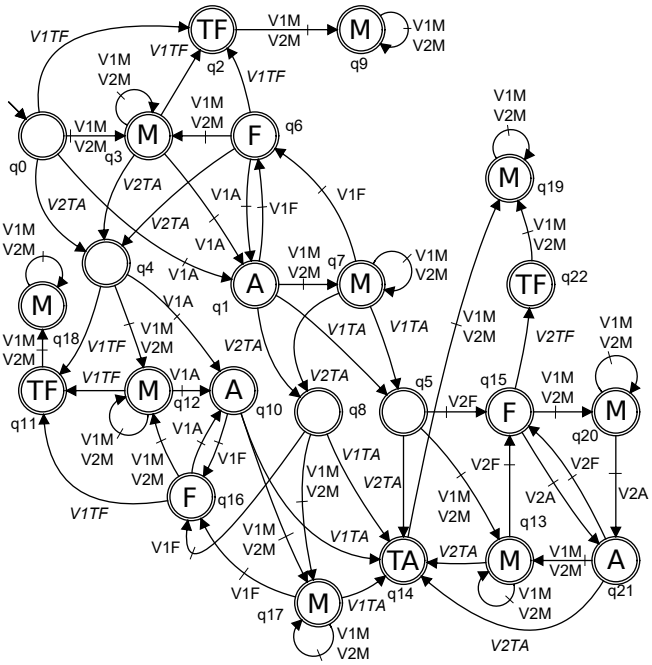

Figura 10. $\mathbf{G_{12}^{op}}$: planta operacional para duas válvulas em série, onde V1A, V1F, V1M, V1TA, V1TF correspondem aos eventos da válvula 1 V_{1Abre}, V_{1Fecha}, $V_{1Mantem}$, $V_{1TAberta}$ e $V_{1TFechada}$, análogo também para a válvula 2; e A, F, M, TA, TF correspondem aos eventos a serem vocalizados V_{12Abre}, $V_{12Fecha}$, $V_{12Mantem}$, $V_{12TAberta}$ e $V_{12TFechada}$.

lável existente antes de atingir um estado vocal, conforme apresentado na Tabela 1. Na primeira coluna constam os estados de $\mathbf{G_{12}^{op}}$, nas demais constam 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.

Partindo do modelo da planta operacional $\mathbf{G_{12}^{op}}$, o modelo para a abstração da válvula equivalente intermediária $\mathbf{G_{12}^{Veq}}$, ilustrado na Figura 11, é obtido por meio do mapa repórter, onde $L(\mathbf{G_{12}^{Veq}}) = \theta(L(\mathbf{G_{12}^{op}}))$ e $L_m(\mathbf{G_{12}^{Veq}}) = \theta(L_m(\mathbf{G_{12}^{op}}))$. Observa-se que o modelo $\mathbf{G_{12}^{Veq}}$ tem a mesma

Tabela 1. 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 $\mathbf{G_{12}^{op}}$, $\Sigma_{12,c}^{eq}$ são os eventos controláveis de $\mathbf{G_{12}^{Veq}}$, Δ_{12} são as desabilitações em $\mathbf{G_{12}^{op}}$.

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

estrutura de uma válvula simples. Para a associação em série das válvulas V_3 e V_4, o modelo da válvula equivalente $\mathbf{G_{34}^{Veq}}$ é obtido empregando-se o mesmo procedimento.

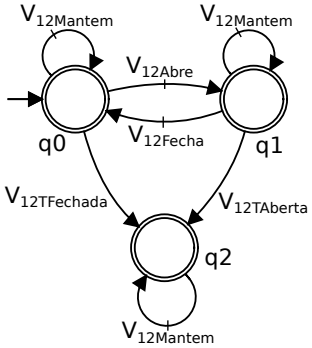

Figura 11. $\mathbf{G_{12}^{Veq}}$: abstração de duas válvulas em série.

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 hierárquica a partir de $\mathbf{G_{12}^{op}}$. Para este modelo, verifica-se que são atingidas as propriedades de consistência hierárquica, mapa repórter observador e consistência de marcação. Essa última é atingida pois consideram-se todos os estados como marcados, o que garante a propriedade. Assim, para este nível hierárquico a estrutura não está sujeita a bloqueios e o comportamento da válvula equivalente intermediária da estrutura em série é igual à imagem do comportamento em malha fechada do operador.

5.3 Modelagem Para Válvulas em Paralelo

Considerando o exemplo estudado neste artigo, a associação de válvulas em paralelo é feita utilizando-se os modelos abstratos de $\mathbf{G_{12}^{Veq}}$ e $\mathbf{G_{34}^{Veq}}$ no nível intermediário da arquitetura hierárquica apresentada na Figura 7. Para a associação de válvulas em paralelo, considera-se que as duas iniciam fechadas. Para a obtenção do supervisor local, utiliza-se a especificação E_{1234} apresentada na Figura 12. Esta especificação prioriza a operação para V_{12}^{eq}, somente permitindo a operação de V_{34}^{eq} quando da ocorrência de travamento fechada de V_{12}^{eq}. Assim, obtém-se o supervisor local S_{1234} com 9 estados e R_{1234} reduzido de 2 estados.

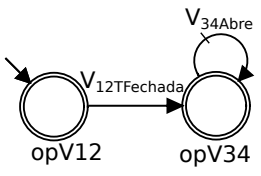

Figura 12. E_{1234}: especificação para válvulas em paralelo.

Com o objetivo de encontrar o modelo da planta do operador para a associação em paralelo, que corresponde ao nível intermediário na arquitetura hierárquica, é construído o modelo de vocalizações $\mathbf{G_{1234}^{voc}}$, de forma análoga ao que foi explicado para o caso da associação em série. A partir desses modelos obtém-se a planta do operador $\mathbf{G}_{1234}^{op}$, contendo 23 estados, sendo todos eles marcados, bem como seu mapa de desabilitações para o operador C_{1234}^{op}.

Desta forma, através do mapa repórter obtém-se o modelo de abstração da válvula equivalente $\mathbf{G^{Veq}}$ como o apresentado na Figura 3 (d), isomórfico ao modelo de uma única válvula de bloqueio. Assim, o procedimento de abstração pode ser generalizado para todos os níveis intermediários de quaisquer circuitos de associações em série e paralelo. Por fim, analisa-se que o modelo de $\mathbf{G_{1234}^{op}}$ apresenta as propriedades de consistência hierárquica, mapa repórter observador e consistência de marcação. Essa última é atingida pois consideram-se todos os estados como marcados. Assim, garante-se que a síntese de controle supervisório, modelando-se todo o circuito de válvulas de bloqueio por uma única válvula equivalente $\mathbf{G^{Veq}}$, como na Seção 4, seja minimamente restritiva e não bloqueante.

5.4 Controle Hierárquico do Processo Industrial

A abstração do circuito de válvulas numa válvula equivalente $\mathbf{G^{Veq}}$ simplifica a modelagem de especificações gerenciais e reduz a complexidade computacional da síntese de supervisor. Porém, a arquitetura hierárquica multinível pressupõe a implementação de 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 ações operacionais sobre as válvulas. A Figura 7 apresenta essa estrutura para o processo industrial da Seção 3. Neste caso, onde 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 S^{ge} representa o supervisor gerencial do processo (supervisor S na Seção 4). Enquanto os eventos de $\Sigma_{proc,c}$ desabilitados por S^{ge} estão diretamente relacionados com os eventos do processo, as desabilitações de Σ_c^{Veq} são traduzidas por C_{1234}^{op} em desabilitações sobre os modelos intermediários $\mathbf{G_{12}^{Veq}}$ e $\mathbf{G_{34}^{Veq}}$, que por sua vez são traduzidas por C_{12}^{op} e C_{34}^{op} em desabilitações para cada uma da válvulas operacionais V_1, V_2, V_3 e V_4. Ao analisar a arquitetura multinível sob a óptica de Pu (2000), que trata sobre a agregação de novos componentes nos níveis abstratos, observa-se que a consistência é preservada, pois as desabilitações referentes às ações de controle nas plantas operacionais, traduzidas pelos mapas C^{op}, se dão sempre na última transição antes de atingir um estado vocal.

6. RESULTADOS

Ao aplicar a estratégia proposta ao processo industrial, foram obtidos supervisores para os três níveis hierárquicos. Nos níveis operacionais, para cada uma das associações em série ou paralelo do circuito de válvulas, são projetados: um supervisor local reduzido de 2 estados, uma planta operacional vocalizadora com 23 estados e um mapa com as desabilitações em cada um desses estados. No nível gerencial, calcula-se um supervisor reduzido de 68 estados, como apresentado na Tabela 2. Nota-se que, pela estratégia

multinível, a complexidade da síntese no nível gerencial e em cada nível intermediário independe do número de associações em série ou paralelo do circuito de válvulas.

Tabela 2. Número de estados na síntese de supervisores na arquitetura multinível.

	G	E	$E\|\|L_m(\mathbf{G})$	**S**	**R**
Nível Gerente	320	16	327	290	68
Associações em Paralelo	9	2	9	9	2
Associações em Série	9	2	9	9	2

Para efeito de comparação, foi desenvolvido o controle supervisório monolítico, utilizando-se os mesmos requisitos, para o mesmo processo industrial com diferentes configurações do circuito de válvulas, conforme apresentado na Tabela 3. Para o processo controlado somente por uma válvula, as dimensões dos modelos são as mesmas que para o nível gerencial da arquitetura multinível. Para o processo controlado por duas válvulas em paralelo nota-se que há um aumento representativo nas dimensões. Por fim analisam-se os modelos para o processo controlado por três válvulas, sendo uma delas paralela a uma associação de duas válvulas em série. Observa-se que no circuito com apenas três válvulas a especificação E já apresenta 56 estados e 848 transições, com grande propensão a erros de modelagem manual. O modelo da vazão no tanque $\mathbf{G_{Vazao}}$ de 16 estados também cresce com o número de válvulas no circuito pela abordagem monolítica. Esses modelos se tornam complexos demais para serem definidos manualmente para o processo com quatro válvulas da Seção 3. Portanto, além de proporcionar a redução na complexidade computacional exigida para a síntese dos supervisores, o método proposto favorece a distribuição da complexidade de modelagem ao longo dos níveis hierárquicos.

Tabela 3. Número de estados na síntese monolítica para diferentes circuitos de válvulas.

	G	E	$E\|\|L_m(\mathbf{G})$	**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

Comparando com a abordagem do controle modular, sem empregar níveis de abstração, não foram obtidas vantagens em relação à complexidade de síntese e de modelagem, devido ao forte acoplamento entre os modelos da planta.

7. CONCLUSÃO

Este trabalho propõe uma estratégia sistemática de modelagem de circuitos de válvulas de bloqueio sujeitas a falhas observáveis por sucessivas abstrações de associações em série ou paralelo em um modelo simplificado de válvula equivalente, que facilita a modelagem de especificações gerenciais e reduz a complexidade de síntese de supervisores do processo industrial. A arquitetura hierárquica multinível especifica como são gerados os eventos abstratos da válvula equivalente e como as desabilitações do supervisor gerencial são traduzidas em ações sobre as válvulas operacionais. As propriedades de consistência hierárquica e de marcação asseguram que a solução do problema de controle supervisório no nível gerencial seja minimamente restritiva e não bloqueante sobre todo o circuito.

REFERÊNCIAS

Alur, R., Henzinger, T.A., Lafferriere, G., e Pappas, G.J. (2000). Discrete abstractions of hybrid systems. *Proc. of the IEEE*, 88(7), 971–984.

Balemi, S., Hoffmann, G.J., Gyugyi, P., Wong-Toi, H., e Franklin, G. (1993). Supervisory control of a rapid thermal multiprocessor. *IEEE Transactions on Automatic Control*, 38, 1040–1059.

Bridges, W. e Clark, T. (2011). How to efficiently perform the hazard evaluation (PHA) required for non-routine modes of oper. (startup, shutdown, online maintenance). In *7th Global Congress in Process Safety*. Chicago.

Fieldbus Foundation (2002). *Function Block Capabilities in Hybrid/Batch Applications*. Fieldbus Foundation. Application Guide.

Koutsoukos, X.D., Antsaklis, P.J., Stiver, J.A., e Lemmon, M.D. (2000). Supervisory control of hybrid systems. *Proceedings of the IEEE*, 88(7), 1026 – 1048.

Oliveira, R.G., Queiroz, M.H., e Cury, J.E.R. (2020). Synthesis of supervisors for a PID-controlled industrial process and implementation on foundation fieldbus. In *Workshop of Discrete Event Systems 2020*. RJ.

Pu, K.Q. (2000). *Modeling and control of discrete-event systems with hierarchical abstraction*. Master's thesis, University of Toronto, Canadá.

Ramadge, P.J. e Wonham, W.M. (1989). The control of discrete event systems. *Proceedings of IEEE: Special Issue on Discrete Event Dynamic Systems*, 77, 81–98.

Sampath, M., Sengupta, R., Lafortune, S., Sinnamohideen, K., e Teneketzis, D. (1996). Failure diagnosis using discrete-event models. *IEEE Transactions on Control Systems Technology*, 4(2), 105–124.

Sanchez, A. (1996). *Formal Specification and Synthesis of Procedural Controllers for Process Systems*. Lecture Notes on Control and Information Sciences, Vol 212. Springer, London.

Schmidt, K., Queiroz, M.H., e Cury, J.E.R. (2007). Hierarchical and decentralized multitasking control of discrete event systems. In *2007 46th IEEE Conference on Decision and Control*, 5936–5941.

Su, R. e Wonham, W.M. (2004). On supervisor reduction in DES. *Disc.-Event Dynamic Systems*, 14, 31–53.

Tittus, M. e Lennartson, B. (1999). Hierarchical supervisory control for batch processes. *IEEE Transactions on Control Systems Technology*, 7(5), 542 – 554.

Wong, K.C. e Wonham, W.M. (1996). Hierarchical control of discrete-event systems. *Discrete Event Dynamic Systems*, 6(3), 241–273.

Wonham, W.M. e Ramadge, P.J. (1988). Modular supervisory control of DES. *Math. of Control of DES*, 1, 13–30.

Yamalidou, E. e Kantor, J. (1991). Modeling and optimal control of discrete-event chemical processes using petri nets. *Computers & Chemical Eng.*, 15(7), 503 – 519.

Yeh, M.L. e Chang, C.T. (2012). An automata based method for online synthesis of emergency response procedures in batch processes. *Computers & Chemical Engineering*, 38, 151 – 170.

Zhong, H. e Wonham, W.M. (1990). On the consistency of hierarchical supervision in discrete-event systems. *IEEE Transactions on Automatic Control*, 35(10), 1125–1134.