

MODELAGEM FORMAL UTILIZANDO REDES DE PETRI COLORIDAS DE UM SISTEMA DE AUTOMAÇÃO PARA ABASTECIMENTO E DILUIÇÃO DE ÁCIDO SULFÚRICO

LEANDRO DIAS DA SILVA*, HEITOR JUDISS SAVINO*, TIAGO FIGUEIREDO VIEIRA*, DAVI BIBIANO BRITO*

**Instituto de Computacao
Universidade Federal de Alagoas
Maceió, Alagoas*

Emails: leandrodias@ic.ufal.br, heitor.savino@ic.ufal.br, tvieira@ic.ufal.br, davi@ic.ufal.br

Abstract— Abstract In this paper we present the formal modeling in Colored Petri Nets (CPN) of an automation system for the supply and dilution of sulfuric acid at 98%. For this type of system, it is necessary to analyze and validate its operation before its implantation to avoid accidents that can cause great financial and even of human lives losses, besides possible environmental damages. Therefore, it is necessary to use models that allow a representation not only of the system to be implemented in the Programmable Logic Controller (PLC) but also of the plant to be controlled and its interaction with the critical automation and control system. The focus of this work is the presentation of the developed model and the formal analysis based on simulations.

Keywords— Coloured Petri Nets, Critical Automation and Control Systems, Formal Methods.

Resumo— Neste artigo a modelagem formal em Redes de Petri Coloridas (RPC) de um sistema de automação para abastecimento e diluição de ácido sulfúrico 98% é apresentada. Para este tipo de sistema, é necessário analisar e validar seu funcionamento antes de sua implantação para evitar acidentes que podem ocasionar grandes perdas financeiras e mesmo de vidas humanas, além de possíveis danos ambientais. Portanto, é necessário o uso de modelos que permitam uma representação não apenas no sistema a ser implementado no Controlador Lógico Programável (CLP) mas também da planta a ser controlada e sua interação com o sistema crítico de automação e controle. O foco deste trabalho é a apresentação do modelo desenvolvido e da análise formal baseada em simulações.

Palavras-chave— Redes de Petri Coloridas, Sistemas Críticos de Automação e Controle, Métodos Formais.

1 Introdução

Sistemas de automação são bastante utilizados hoje em dia em diversos domínios de aplicação como, por exemplo plantas de processos químicos. Neste tipo de sistema, é necessário verificar valores de vários sensores em diversos pontos diferentes da planta e as relações entre eles, os *set points*. Exemplos de variáveis a serem medidas com sensores são níveis máximos e mínimos dos tanques e de elementos de misturas, condutividade, pressão, temperatura, e estado aberto ou fechado de válvulas. De acordo com os valores dos sensores e a lógica de controle, diversos atuadores devem ser controlados como, por exemplo, bombas e válvulas. Para este tipo de sistema, considerados sistemas críticos de automação e controle, é necessário analisar e validar seu funcionamento de forma mais rigorosa antes de sua implantação para evitar acidentes que podem ocasionar grandes perdas financeiras e mesmo de vidas humanas, além de possíveis danos ambientais. Ainda, o teste do sistema não é suficiente visto que erros durante o teste no sistema real em funcionamento também pode levar aos problemas citados acima. Finalmente, testes durante o desenvolvimento do código Ladder para um Controlador Lógico Programável (CLP) não necessariamente refletem adequadamente o comportamento do sistema. Portanto, é necessário o

uso de modelos que permitam uma representação não apenas do sistema a ser implementado no CLP mas também da planta a ser controlada e sua interação com o sistema crítico de automação e controle.

O uso de métodos formais como RPC na modelagem de sistema agrega vários benefícios ao projeto e desenvolvimento de sistemas críticos de automação e controle. Por exemplo, é possível realizar a prova de propriedades no modelo antes de o sistema ser desenvolvido, aumentando a confiança no modelo. Um modelo formal de RPC pode ser utilizado para treinamento de operadores através de simulações e visualizações em 3D. Ainda, um processo de desenvolvimento baseado em modelos formais pode incluir a geração automática de código e de testes. Finalmente, os modelos formais podem ser utilizados em um processo de validação através da técnica *hardware-in-the-loop* (HIL).

Métodos formais tais como autômatos temporizados (Bengtsson and Yi, 2004), Redes de Petri (Murata, 1989) e sua extensão Redes de Petri Coloridas (RPC) (Jensen and Kristensen, 2009), têm sido amplamente utilizados na modelagem e análise formal de sistemas de automação e controle nos mais variados domínios de aplicação (Sobrinho et al., 2017; Lisboa et al., 2009; Zhou and Dicesare, 1993).

Modelagem formal, do Inglês *Formal Mode-*

ling, que se refere a modelagem utilizando modelos formais, que por sua vez se referem a técnicas matemáticas para especificação e verificação de sistemas, no caso deste artigo, RPC. Análise formal se refere ao tipo de análise realizada a partir de modelos formais. Existem diversas técnicas de análise formal, dentre elas verificação de modelos e simulações, o foco deste artigo.

Em (Schild et al., 2017), os autores apresentam um arcabouço para modelagem em redes de Petri de modos de operação para controle de automação de edifícios com foco em eficiência energética. Redes de Petri são utilizadas como modelo matemático para desenvolver, analisar e gerar os algoritmos de controle.

Autômatos temporizados são utilizados para geração automática de testes para programas de CLP desenvolvidos em Ladder (OLIVEIRA et al., 2015). Os autômatos são gerados automaticamente a partir de diagramas ISA 5.2 de especificação do sistema para o formato da ferramenta Uppaal (Bengtsson and Yi, 2004), que pode ser utilizada para validar os modelos. A ferramenta gera os traços de testes para serem executados e comparados com a saída esperada para validar o código Ladder executando no CLP.

Redes de Petri, especificamente IOPT Petri nets, são utilizadas para geração de diagramas Ladder (Feio et al., 2017). A ferramenta desenvolvida lê na entrada modelos IOPT no formato PNML¹ e gera um arquivo com a lista de instruções associadas ao diagrama Ladder. A validação foi feita com exemplos para um CLP específico.

Sistemas de tempo real são analisados através de verificação de modelos de redes de Petri temporizadas em (del Foyo and Silva, 2017). O método proposto permite a análise de propriedades quantitativas e qualitativas de sistemas a eventos discreto enumerando o espaço de estados do modelo temporizado, apesar do problema de explosão do espaço de estados.

Neste trabalho, um modelo formal em RPC para um sistema de diluição de ácido sulfúrico é apresentado. As RPC e a ferramenta de suporte CPN/Tools estão entre as mais consolidadas e maduras para modelagem e análise de sistemas de automação e controle de sistemas a eventos discretos. O sistema será implementado em linguagem Ladder em um CLP. O modelo apresentado será utilizado como base para o desenvolvimento do código e para geração de casos de testes. O foco deste trabalho é a apresentação do modelo desenvolvido e da análise formal baseada em simulações.

O restante deste artigo está organizado da seguinte forma. Na Seção 2 a definição formal e um exemplo ilustrativo de RPC são apresentados. O sistema de diluição de ácido sulfúrico e a modelagem formal do sistema com RPC são descritos na

Seção 3. O artigo é concluído com sugestões de trabalhos futuros na Seção 4.

2 Redes de Petri Coloridas

Uma rede de Petri é um formalismo com uma representação gráfica para modelagem e análise de sistemas concorrentes. O diagrama é um grafo bi-partido com dois tipos de nós: lugares e transições. Os lugares modelam o estado distribuído do sistema e as transições modelam os eventos. Redes de Petri coloridas são uma extensão de redes de Petri de baixo nível (lugar/transição) com extensões de tipos de dados. A definição formal é dada a seguir (Jensen and Kristensen, 2009).

Definição 1. Uma Rede de Petri Colorida é uma 9-tupla $RPC = (P, T, A, \Sigma, V, C, G, E, I)$, onde:

- P é um conjunto finito de Lugares
- T é um conjunto finito de Transições. Temos que $P \cap T = \emptyset$
- A é um conjunto finito de Arcos direcionados. Temos que $A \subseteq P \times T \cup T \times P$
- Σ é um conjunto finito e não vazio de conjuntos de cores (colour sets)
- V é um conjunto finito de Variáveis. Temos que $Tipo[v] \in \Sigma$ para todo $v \in V$
- C é a função de Conjunto de cores $C : P \rightarrow \Sigma$ que associa cada lugar a um conjunto de cores
- G é a função de Guarda $G : T \rightarrow EXP_{R_v}$ que associa cada transição a uma guarda. Temos que $Tipo[G(t)] = Bool$ para todo $t \in T$
- E é a função de Expressão de arco $E : A \rightarrow EXP_{R_v}$ que associa cada arco a uma expressão. Temos que $Tipo[E(a)] = C(p)_{MS}$ para todo $a \in A$, onde p é o lugar conectado ao arco a
- I é a função de inicialização $I : P \rightarrow EXP_{R_0}$ que associa cada lugar a uma marcação inicial. Temos que $Tipo[I(p)] = C(p)_{MS}$ para todo $p \in P$

O funcionamento de RPC, chamado de jogo das fichas (*token game*) é guiado pela ocorrência das transições (*transition occurrence*) que, por sua vez, é formalizado pela regra de disparo das transições. A regra de disparo pode ser resumida da seguinte forma. Para uma transição disparar ela precisa ser habilitada. Para habilitar uma transição em uma RPC as seguintes regras devem ser satisfeitas: i) todos os lugares de entrada de uma transição devem ter fichas em quantidade maior ou igual que o peso do arco que liga o lugar a transição; ii) uma transição habilitada pode ou não ocorrer; iii) a função de guarda deve ser avaliada

¹<http://www.pnml.org/>

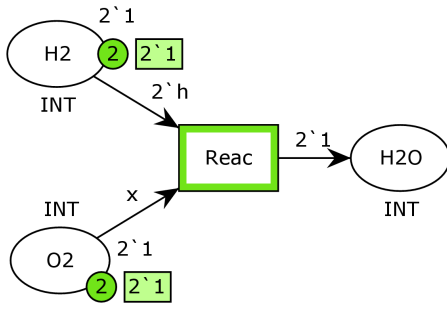


Figura 1: Marcação inicial do modelo de RPC para o exemplo de produção de molécula de água

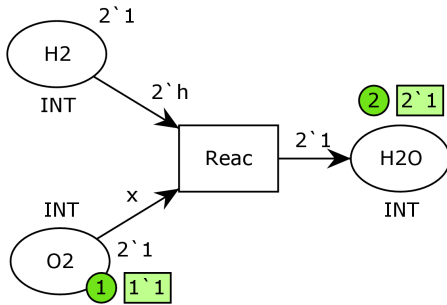


Figura 2: Marcação após o disparo da transição Reac

para verdadeira; iv) o disparo de uma transição habilitada remove fichas dos lugares de entrada e acrescenta nos lugares de saída, de acordo com os pesos dos respectivos arcos.

Na Figura 1 é ilustrado um modelo de RPC para a produção de uma molécula de água, adaptado de (Murata, 1989). Para produzir uma molécula de água são necessárias duas moléculas de hidrogênio e uma de oxigênio. Na figura a marcação (fichas) nos lugares são $M(H2) = 2$, $M(O2) = 2$, e $M(H2O) = 0$. O peso do arco de $O2$ para $Reac$ é 2 e de $H2$ para $Reac$ é 1. Desta forma, a transição está habilitada. Como não existe função de guarda em $Reac$, por definição é assumida como verdadeira. Ao disparar, a transição $Reac$ vai remover duas fichas do lugar $H2$ e uma do lugar $O2$, e depositará duas fichas no lugar $H2O$, como pode ser visto na Figura 2.

Várias técnicas de análise foram definidas para RPC como, por exemplo, simulações, invariantes e verificação de modelos. Neste artigo simulações são utilizadas para validar o comportamento do modelo. Uma vez que o projetista esteja satisfeito com o funcionamento do modelo, o código pode ser desenvolvido com mais segurança, evitando ou diminuindo possíveis erros de projeto.

3 Modelagem com Redes de Petri Coloridas do Sistema de Automação de Diluição de Ácido Sulfúrico

O sistema é composto das seguintes partes. A entrada do sistema é feita com a descarga de um caminhão no tanque 1 ou no tanque 2 através da bomba 1. A segunda parte é a parte principal do sistema de diluição que consiste em detectar nível baixo no tanque 4 e iniciar a diluição de nova batelada. Para isso, abre-se a válvula do tanque em uso, 1 ou 2, liga-se a bomba, inicia a carga de água potável no tanque 3, do ácido, liga-se o ar-comprimido, torre de resfriação até atingir a temperatura de *set point* ou o nível máximo do tanque. A terceira parte consiste em identificar se a batelada é a de análise ou não. Caso não seja, a mistura é armazenada no tanque 4. Caso seja a batelada de análise, a mistura é analisada através da condutividade e, caso seja aprovada, é liberada e carregada para o tanque 4. Caso não seja aprovada, pode ser rejeitada e armazenada no tanque 5, ou solicitada operação manual para ajustes por parte do operador humano. A quarta parte é manter o tanque 6 sempre cheio. A quinta parte, não modelada neste trabalho, e externa a planta de diluição, é a parte de controle de produção de água desmineralizada. Neste trabalho a ferramenta CPN/Tools² foi utilizada para edição e análise dos modelos de RPC (Ratzer et al., 2003; Jensen et al., 2007).

O modelo desenvolvido neste trabalho foi baseado no descritivo do sistema provido pela empresa que irá operar o mesmo. Por motivos de sigilo o diagrama e o descritivo providos pela empresa não poderão ser publicados aqui. No descritivo do sistema são apresentadas as tabelas com *set points* para cada parte do sistema. Um exemplo de definição de *set point* pode ser visto a seguir:

- Volume Máximo TQAC 01: SP20

Essa definição significa que o nível máximo do tanque 1 é definido no *set point* SP20.

Além das tabelas de *set points*, no descritivo do sistema também são descritas as sequências de operação para cada parte do sistema. Um exemplo de descrição pode ser visto a seguir:

- O Sistema deverá desligar a bomba caso o nível do tanque ultrapasse o Nível SP20.

Na Figura 3 pode ser visto o modelo de RPC para a parte de descarga na entrada do sistema de diluição. O fluxo para essa parte inicial do processo é explicado a seguir. Primeiro o caminhão com 14 toneladas de ácido sulfúrico a 98% chega e uma mangueira é conectada a bomba 1. Em seguida o operador escolhe entre os tanques de

²<http://cpntools.org/>

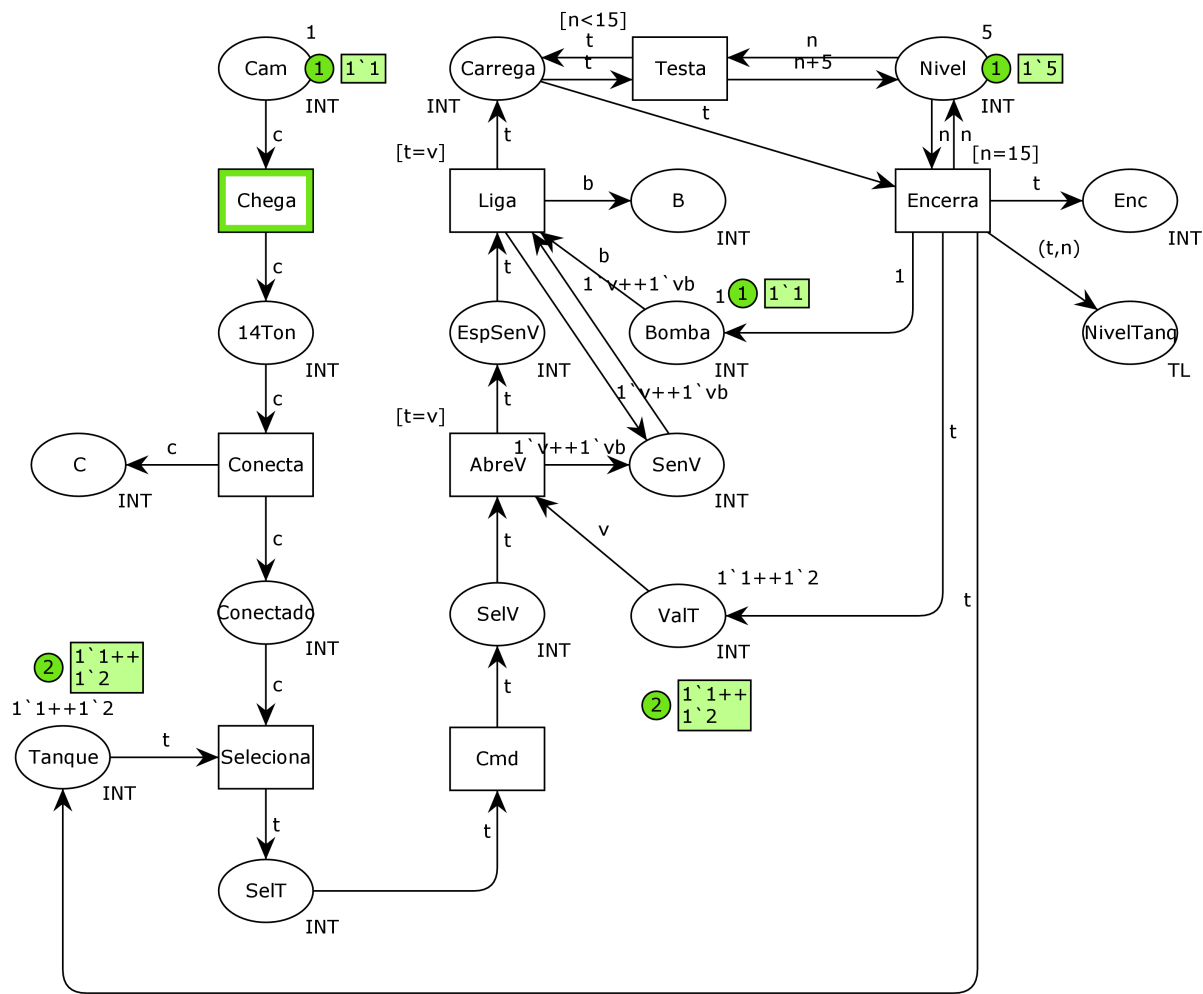


Figura 3: Modelo de RPC para a parte de descarga de ácido sulfúrico na entrada do sistema

entrada 1 ou 2 e liga a bomba. O sistema, deverá abrir a válvula do tanque escolhido, receber o sinal de válvula aberta do tanque e ligar a bomba. O Sistema deverá desligar a bomba caso o nível do tanque ultrapasse o nível máximo estabelecido no *set point*. Após o término do descarregamento, desligar a bomba e fechar as válvulas. Nas Tabelas 1 e 2 são descritos os significados dos lugares e transições do modelo na Figura 3, respectivamente.

Na Figura 4 pode ser visto o modelo de RPC para a parte de diluição de nova batelada. O sistema indicará nível de ácido baixo do tanque 4 e automaticamente iniciará a diluição de nova batelada. O sistema verificará se a condição do tanque 3 está em volume mínimo e iniciará a diluição, abrindo a válvula de entrada de água desmineralizada até nível máximo de água no tanque 3. Após, o sistema abre a válvula de ar comprimido, liga a torre de refrigeração e a bomba centrífuga. Após, o sistema abre a válvula de entrada de ácido e, através de bomba, adicionará ácido sulfúrico 98% no tanque 3 até atingir o nível máximo de ácido. Completado o nível, as válvulas de entrada do tanque 3 e de saída do tanque de ácido escolhido são

Lugar	Descrição
Cam	Caminhão na entrada
14Ton	14 toneladas
C	Caminhão na descarga
Conectado	Cam. conectado
Tanque	Tanques disponíveis
SelT	Tanque selecionado
SelV	Válvula selecionada
ValT	Válvulas de tanques
SenV	Sensor de válvula
EspSenV	Espera sensor de válvula
Bomba	Bombas disponíveis
B	Bomba selecionada
Carrega	Carregando tanque
Nivel	Nível do tanque
Enc	Encerrado
NivelTanq	Nível final do Tanque

Tabela 1: Tabela de descrição dos estados do modelo na Figura 3

fechadas.

O sistema aguarda até que a temperatura da solução atinja o valor de *set point*, desliga a torre

Transição	Descrição
Chega	Chagada de Caminhão
Conecta	Conecta caminhão
Seleciona	Seleciona tanque
Cmd	Comando para abrir válvula
AbreV	Abre válvula
Liga	Liga bomba
Testa	Testa nível do tanque
Encerra	Encerra carga

Tabela 2: Tabela de descrição das transições do modelo na Figura 3

de refrigeração, bomba centrífuga e ar comprimido. São medidos os valores de condutividade e volume da solução e comparados com os valores dos respectivos *set points*.

O sistema deverá verificar a quantidade de preparações e comparar com o *set point*, e caso todos os valores estejam corretos, o sistema bombeará automaticamente para o tanque de armazenagem, abrindo as válvulas de saída do tanque 3, de entrada do tanque 4 e da bomba. Caso contrário, o sistema ficará em espera com alarme, aguardando atuação do operador que deverá retirar amostra para análise e após a checagem, o mesmo acionará a continuação do processo decidindo aprovar, ajustar ou reprovar a solução. Em caso de aprovação, bombear o ácido para o tanque de armazenagem abrindo as válvulas indicadas anteriormente. Em caso de ajustar, liberar o sistema em modo manual para que o operador possa realizar as adições necessárias. Em caso de reprovação, bombear o ácido para o tanque 5, de ácido reprovado, abrindo as válvulas de saída do tanque 3, de entrada do tanque 5 e da bomba.

Com os modelos de RPC várias técnicas de análise podem ser aplicadas como, por exemplo, simulação e verificação de modelos simulação. Na Figura5 é ilustrado um relatório de simulação gerado automaticamente pelo CPN/Tools. No cabeçalho do relatório é possível verificar informações gerais do modelo como arquivo utilizado, data e hora. A seguir temos enumerados os passos ocorridos, que são disparos de transições. Os passos contém informação de qual transição foi disparada e qual o valor das fichas, através dos valores das variáveis nos arcos. Por exemplo, o primeiro passo 1 temos: 1 0 Chega @ (1:Descarga), com $c = 1$. Isso significa que no passo 1 a transição *Chega*, na página descarga disparou com $c = 1$. Neste modelo, c é a variável que identifica o caminhão. A transição *conecta* significa que a mangueira foi conectada ao caminhão e a bomba. No passo 3 a transição *Seleciona* foi disparada com $t = 2$. Isso significa que o tanque 2 foi selecionado. No próximo passo, o disparo de *Cmd* modela o comando para abertura da válvula do tanque 2. No passo 5, o disparo de *AbreV* com $v = 2$ significa que a

válvula do tanque 2 foi aberta, e a bomba 1 pode ser ligada, como ilustrado no passo 6 como o disparo de *Liga* com $b = 1$. A transição *testa* modela o teste do nível do tanque enquanto a bomba 1 bombeia o ácido do caminhão para o tanque escolhido, no caso o 2. Quando o nível atingir o *set point*, neste caso 15, o processo é encerrado, a bomba é desligada, e o nível do tanque é armazenado no lugar *NivelTanq*, para ser acompanhando por outras partes do processo (veja a Figura3).

O mesmo raciocínio vale para o relatório que ilustra o modelo da parte de diluição ilustrado na Figura 6. Com o nível do tanque 4 baixo, a nova batelada é iniciada. O tanque 3 inicialmente é enchido com água desmineralizada até o limite de água através da abertura da válvula 8. Após, o ar comprimido é aberto através da válvula 11 e a torre de refrigeração e a bomba 2 são ligadas. Após isso o tanque de uso é escolhido e a bomba através da válvula 10 é ligada para carregar o ácido do tanque de uso para o tanque 3. Quando atingir o limite de ácido do tanque 3 as válvulas são fechadas, as bombas e a torre de refrigeração são desligadas.

4 Conclusões

Neste trabalho, um modelo formal em RPC para um sistema de diluição de ácido sulfúrico é apresentado. O modelo é importante para a validação do projeto antes do desenvolvimento do código Ladder, aumentando a confiança no funcionamento do sistema. Além disso, o modelo foi validado através de simulações.

O modelo desenvolvido, validado e apresentado neste trabalho será utilizado como base para o desenvolvimento do código Ladder para o CLP que controlará o sistema. Além disso, o modelo também será utilizado para geração de casos de testes que poderão ser utilizados tanto para validação do código em desenvolvimento como para guiar o teste de comissionamento para implantação utilizando técnicas de hardware-in-the-loop (HIL) através de comunicação via sockets entre o modelo e o servidor OPC do CLP. Finalmente, um outro trabalho futuro é a verificação de propriedades do modelo utilizando a técnica de verificação de modelos.

Referências

- Bengtsson, J. and Yi, W. (2004). *Timed Automata: Semantics, Algorithms and Tools*, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 87–124.
- del Foyo, P. M. G. and Silva, J. R. (2017). Improving the verification of real-time systems using time petri nets, *Journal of Control, Au-*

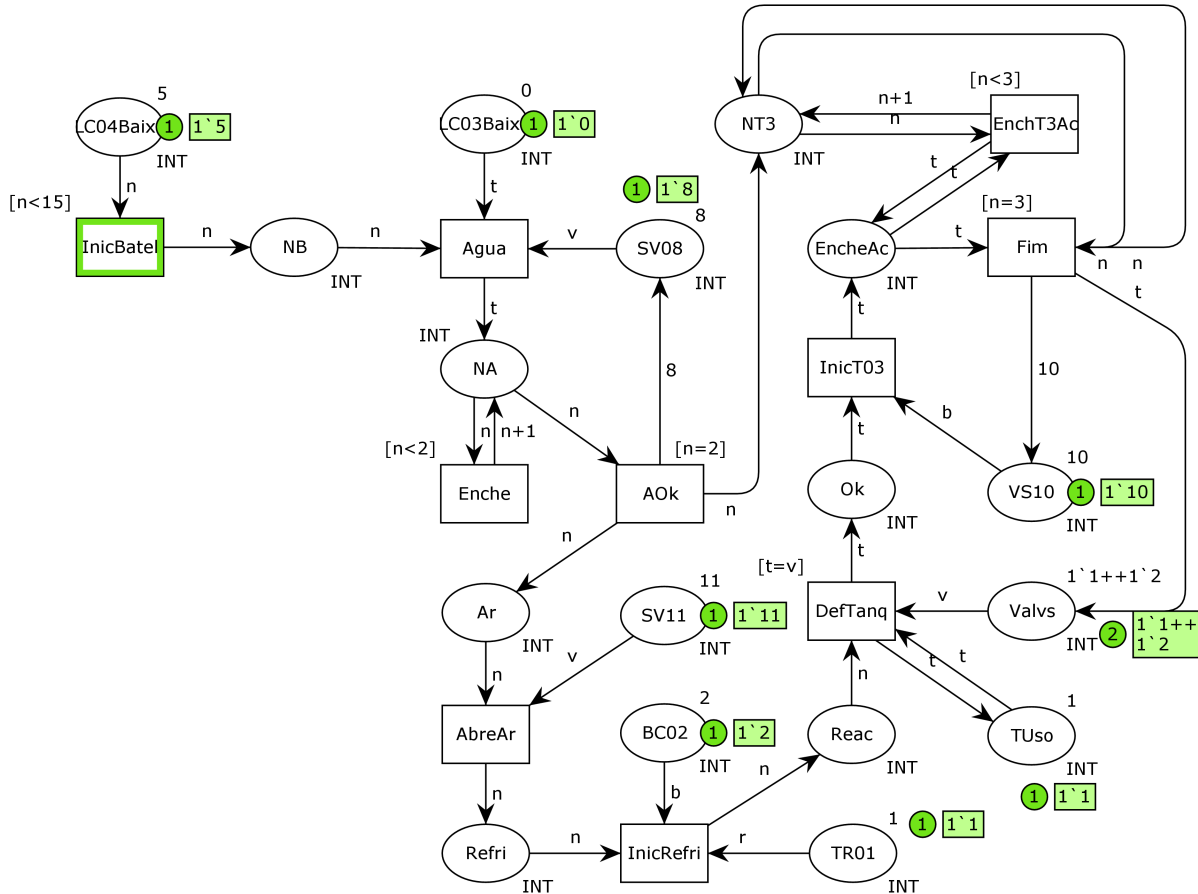


Figura 4: Modelo de RPC para a diluição de nova batelada

CPN Tools simulation report for:
PlantaAcidoSulfurico.cpn
Report generated: Fri Apr 13 11:49:53 2018

```

1    0    Chega @ (1:Descarga)
- c = 1
2    0    Conecta @ (1:Descarga)
- c = 1
3    0    Selecciona @ (1:Descarga)
- t = 2
- c = 1
4    0    Cmd @ (1:Descarga)
- t = 2
5    0    AbreV @ (1:Descarga)
- t = 2
- v = 2
6    0    Liga @ (1:Descarga)
- b = 1
- t = 2
- v = 2
7    0    Testa @ (1:Descarga)
- t = 2
- n = 5
8    0    Testa @ (1:Descarga)
- t = 2
- n = 10
9    0    Encerra @ (1:Descarga)
- n = 15
- t = 2

```

Figura 5: Relatório de simulação da página de descarga do modelo de RPC

Automation and Electrical Systems **28**(6): 774–784.

Feio, R., Rosas, J. and Gomes, L. (2017). Translating iopt petri net models into plc ladder diagrams, *2017 IEEE International Conference on Industrial Technology (ICIT)*, pp. 1211–1216.

Jensen, K. and Kristensen, L. M. (2009). *Coloured Petri Nets: Modelling and Validation of Concurrent Systems*, Springer.

Jensen, K., Kristensen, L. M. and Wells, L. (2007). Coloured petri nets and cpn tools for modelling and validation of concurrent systems, *International Journal on Software Tools for Technology Transfer* **9**(3): 213–254.

Lisboa, L. A. C., Lima, A. M. N. and Silva, L. D. (2009). Using hierarchical coloured petri net to support substation restoration, *2009 IEEE Bucharest PowerTech*, pp. 1–8.

Murata, T. (1989). Petri nets: Properties, analysis and applications, *Proceedings of the IEEE* **77**(4): 541–580.

OLIVEIRA, K. V., OLIVEIRA, A. B., SILVA, L. D., PERKUSICH, A. and GORGONIO,

CPN Tools simulation report for:
 PlantaAcidoSulfurico.cpn
 Report generated: Fri Apr 13 11:50:30 2018

```

1      0      InicBatel @ (1:Diluicao)
- n = 5
2      0      Agua @ (1:Diluicao)
- n = 5
- v = 8
- t = 0
3      0      Enche @ (1:Diluicao)
- n = 0
4      0      Enche @ (1:Diluicao)
- n = 1
5      0      AOok @ (1:Diluicao)
- n = 2
6      0      AbreAr @ (1:Diluicao)
- v = 11
- n = 2
7      0      InicRefri @ (1:Diluicao)
- r = 1
- b = 2
- n = 2
8      0      DefTanq @ (1:Diluicao)
- n = 2
- t = 1
- v = 1
9      0      InicT03 @ (1:Diluicao)
- b = 10
- t = 1
10     0      EnchT3Ac @ (1:Diluicao)
- t = 1
- n = 2
11     0      Fim @ (1:Diluicao)
- n = 3
- t = 1

```

Figura 6: Relatório de simulação da página de diluição do modelo de RPC

for certification, *Software & Systems Modeling*.

Zhou, M. and Dicesare, F. (1993). *Petri Net Synthesis for Discrete Event Control of Manufacturing Systems*, Springer.

- K. (2015). Geração e execução automática de testes para programas de controladores lógicos programáveis para sistemas instrumentados de segurança, *Anais do XII Simpósio Brasileiro de Automação Inteligente, 2015*, pp. 1156–1161.
- Ratzer, A. V., Wells, L., Lassen, H. M., Laursen, M., Qvortrup, J. F., Stissing, M. S., Westergaard, M., Christensen, S. and Jensen, K. (2003). Cpn tools for editing, simulating, and analysing coloured petri nets, in W. M. P. van der Aalst and E. Best (eds), *Applications and Theory of Petri Nets 2003*, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 450–462.
- Schild, T., Fütterer, J. and Müller, D. (2017). A mode-based implementation framework for advanced control methods in building automation systems with petri-nets, *2017 IEEE International Conference on Advanced Intelligent Mechatronics (AIM)*, pp. 213–218.
- Sobrinho, A., da Silva, L. D., Perkusich, A., Cunha, P., Cordeiro, T. and Lima, A. M. N. (2017). Formal modeling of biomedical signal acquisition systems: source of evidence