

UM MODELO DE REFERÊNCIA DE REDES DE PETRI COLORIDAS PARA SISTEMAS DE CONTROLE DE BOMBA DE INFUSÃO DE INSULINA: AUXILIANDO NO PROCESSO DE CERTIFICAÇÃO

Tássio Fernandes Costa¹
Álvaro Sobrinho²
Leonardo Chaves e Silva³
Leandro Dias da Silva⁴
Angelo Perkusich⁵

RESUMO

As bombas de infusão de insulina são sistemas críticos seguros que requerem a avaliação de agências reguladoras do governo (por exemplo, *Food And Drug Administration - FDA*) antes da comercialização. Neste artigo é apresentado um modelo de referência de Redes de Petri Coloridas (*Coloured Petri Nets - CPN*) para sistemas de controle de bomba de infusão de insulina com o objetivo de auxiliar os fabricantes a gerar evidências de segurança e avaliar a qualidade para fins de certificação. Além disso, é realizada a descrição de um estudo de caso sobre o sistema *ACCU-CHEK Spirit* versão 2.XX para avaliar o modelo *CPN*. Portanto, o modelo de referência está disponível e verificado. Além disso, o estudo de caso é útil para demonstrar como os fabricantes podem utilizá-lo durante um processo de certificação. A principal contribuição deste trabalho consiste em um artefato de projeto para diminuir custos e tempo de desenvolvimento de sistemas de controle de bombas de infusão de insulina, além de aumentar a confiança em propriedades de segurança.

Palavras-chave: Modelagem. Simulação. Informática industrial.

ABSTRACT

Insulin infusion pumps are safety-critical systems that require the evaluation of government regulatory agencies (e.g., FDA) before commercialization. This paper presents a Coloured Petri Nets (CPN) reference model of insulin infusion pump control systems to assist manufacturers to generate safety evidence and evaluate quality for certification purposes. It also describes a case study on the ACCU-CHEK Spirit system version 2.XX to evaluate the CPN model. Therefore, the reference model is available and verified. Additionally, the case study is useful to show how manufacturers can reuse it during a certification process. The main contribution of this paper consists on a project artifact to decrease costs and development time of insulin infusion pump control systems, in addition to increase confidence on safety properties.

¹ Bacharel em Tecnologia da Informação pela Universidade Federal Rural do Semi-Árido, tassiof206@gmail.com.

² Bacharel em Análise de Sistemas, Mestre em Modelagem Computacional do Conhecimento e Doutor em Ciência da Computação, docente na Universidade Federal do Agreste de Pernambuco, alvaro.alvares@ufape.edu.br.

³ Bacharel, Mestre e Doutor em Ciência da Computação, docente na Universidade Federal Rural do Semi-Árido, lenardo@ufersa.edu.br.

⁴ Bacharel em Ciência da Computação, Mestre e Doutor em Engenharia Elétrica, docente na Universidade Federal de Alagoas, leandrodias@ic.ufal.br.

⁵ Bacharel, Mestre e Doutor em Engenharia Elétrica, docente na Universidade Federal de Campina Grande, perkusich@dee.ufcg.edu.br.

Key words: Modeling. Simulation. Industrial Informatics.

DOI: 10.1109/IECON.2019.8927111

1 INTRODUÇÃO

Os sistemas médicos embarcados podem ser divididos em três classes: monitoramento (ou seja, adquire e/ou verifica biomarcadores), diagnóstico (ou seja, identifica riscos de doenças) e tratamento (ou seja, atua para realizar uma prescrição médica). Por exemplo, Sharanya, Abhishek e Reddy (2017) apresentam um sistema de monitoramento para doenças cardíacas. O sistema proposto por Muangprathub e Boonjing (2014) realiza o diagnóstico de 50 doenças diferentes. Sjaheim et al. (2014) descreve um sistema médico portátil para tratar e diagnosticar lesões cerebrais traumáticas.

O foco neste artigo está nos sistemas médicos de tratamento. Mais especificamente, o tratamento de diabetes usando sistemas de controle de bomba de infusão de insulina. Este tipo de sistema contém componentes de hardware e software. Por um lado, componentes de hardware compõem a bomba de infusão que simula o comportamento do pâncreas. Por outro lado, um software embarcado controla o sistema para garantir o correto funcionamento, visando prevenir situações de risco (MERTZ, 2018).

Como se trata de um sistema crítico seguro, os fabricantes devem analisar o comportamento dos sistemas de controle da bomba de infusão de insulina para fornecer, pelo menos, a garantia mínima necessária para o correto funcionamento. Nesse contexto, as linguagens de modelagem formal são ferramentas matemáticas úteis para representar requisitos com alto nível de precisão. Redes de Petri coloridas (*Coloured Petri Nets - CPN*) é um exemplo desse tipo de linguagem (JENSEN; KRISTENSEN, 2015).

A linguagem *CPN* permite combinar os conceitos do formalismo tradicional das redes de Petri com a linguagem de programação funcional *CPN/ML*, hierarquia e recursos de temporização. *CPN* (juntamente com o *CPN/Tools*⁶) se enquadra ao propósito deste trabalho considerando que os sistemas de controle da bomba de infusão de insulina requerem características como simultaneidade, comunicação e sincronização.

Portanto, o uso da linguagem de modelagem formal *CPN* é uma alternativa para os fabricantes aumentarem a confiança no correto funcionamento dos sistemas de controle da bomba de infusão de insulina. Porém, para aplicar este tipo de técnica formal é necessário de conhecimento especializado o que aumenta o tempo de desenvolvimento e resulta em custos de projeto. Neste artigo, é argumentado que modelos de referência *CPN* reutilizáveis de sistemas de controle de bomba de infusão de insulina têm o potencial de reduzir o impacto em tempo e custo (SOBRINHO *et al.*, 2017).

Além disso, agências governamentais reguladoras (por exemplo, a *Food And Drug Administration - FDA*) exigem que os fabricantes demonstrem formalmente que os sistemas de controle da bomba de infusão de insulina não colocam os usuários em situações perigosas⁷. Em 2010, a *FDA* lançou a iniciativa de melhoria da bomba de infusão⁸. São destacados problemas como defeitos de software, interface do usuário e falhas mecânicas ou elétricas. Como alguns

⁶ <https://cpntools.org/>

⁷ FDA: Medical device classification procedures. (Abril, 2016).

⁸ FDA: Infusion Pump Improvement Initiative. (Abril, 2010).

resultados da iniciativa de melhoria da bomba de infusão, a *FDA* desenvolveu e lançou alguns artefatos, como a orientação de 2014 para a indústria e equipes da *FDA* durante o desenvolvimento de bombas de infusão de insulina, considerando o ciclo de vida do produto⁹.

No entanto, até o momento, ainda existe um grande número de *recalls* regulatórios relacionados ao mau funcionamento dos sistemas (RATHORE *et al.*, 2018). Para enfrentar este problema, os fabricantes submetem o sistema em desenvolvimento a um processo de certificação conduzido por agências reguladoras com base em padrões prescritivos (por exemplo, ISO 14971 (IMAGAWA; MIZUKAMI; MIYAZAKI, 2018)) e atributos de qualidade (por exemplo, segurança). O uso isolado de especificações informais e semi formais contribui para diminuir a confiança no funcionamento correto dos sistemas de controle da bomba de infusão de insulina.

Neste artigo é apresentado a especificação formal de um modelo de referência *CPN* de sistemas de controle de bomba de infusão de insulina como um artefato de projeto para aumentar a confiança nos comportamentos do sistema, gerar evidências de segurança e avaliar a qualidade para fins de certificação. Também descreve um estudo de caso em um sistema comercial (o *ACCU-CHEK Spirit* versão 2.XX¹⁰) para avaliar o modelo de referência por meio da técnica de verificação de modelos. Embora não apresentada neste trabalho (devido a restrições de espaço), a avaliação também foi realizada por meio de simulações. Além disso, é apresentado como os fabricantes podem reutilizar o modelo de referência durante um processo de certificação. Neste trabalho são ampliadas as contribuições apresentadas por Silva *et al.* (2015). As principais contribuições com este artigo consistem em:

- um modelo de referência modular e parametrizado de sistemas de controle de bomba de infusão de insulina; e
- um estudo de caso para demonstrar como os fabricantes podem gerar evidências para a certificação.

O artigo está estruturado da seguinte forma. Na seção 2 são detalhados os trabalhos relacionados. Na seção 3 é descrita a definição formal de *CPN* usada para especificar o modelo de referência. Na seção 4 é apresentado o modelo de referência *CPN* de sistemas de controle de bomba de infusão de insulina. Na seção 5 é apresentada uma amostra da avaliação do modelo por meio da técnica de verificação de modelos. Na seção 6 são apresentadas a conclusão do trabalho e trabalhos futuros.

2 TRABALHOS RELACIONADOS

Embora neste trabalho seja usado *CPN* como a linguagem de modelagem formal, existem outras linguagens e representações gráficas para o mesmo propósito (por exemplo, autômatos). Um exemplo de uso de autômatos é o trabalho apresentado por Niezen e Eslambolchilar (2016). Os autores aplicaram autômatos híbridos para especificar um modelo de operador humano para interagir com dispositivos médicos.

Silva *et al.* (2015) descrevem um cenário clínico baseado em um sistema de controle de bomba de infusão de insulina para avaliar uma abordagem para auxiliar na modelagem e validação (por exemplo, propriedades de segurança) de sistemas médicos ciberfísicos. Os diagramas de blocos do *Simulink*¹¹ representam os comportamentos do sistema. Os componentes

⁹<https://www.fda.gov/regulatory-information/search-fda-guidance-documents/infusion-pumps-total-product-life-cycle>

¹⁰<https://www.accu-check.com/download/file/fid/17481>

¹¹<https://www.mathworks.com/products/simulink.html>

básicos de um sistema de controle de bomba de infusão de insulina consistem na agulha para bombear a insulina, controlador, visor, fonte de alimentação, relógio e cartucho de insulina. Exemplos de propriedades de segurança desses sistemas incluem:

- se o nível do cartucho for igual a 0, então o cartucho deve estar vazio e a bomba deve parar; e
- se o nível do cartucho for inferior à dosagem de insulina administrada, a bomba deve parar.

A *FDA* está preocupada com os atributos de qualidade das bombas de infusão. Por um lado, o projeto bomba de infusão de insulina genérica (*Generic Insulin Infusion Pump - GIIP*) é um exemplo de iniciativa para aumentar a confiança nos sistemas de controle de bombas de infusão de insulina. Por exemplo, é realizada a análise de risco por uma especificação arquitetônica genérica (ZHANG, 2010). Ou seja, uma representação de alto nível que não permite a execução de uma instância considerando as restrições de tempo e a verificação formal. Por outro lado, Hatcliff *et al.* (2018) conduziram o projeto aberto de bomba de infusão de analgésico genérica controlada pelo paciente para fornecer artefatos como casos de uso, infraestrutura de teste e simulação, artefatos de gerenciamento de risco e casos de garantia. No entanto, até a presente data, não existe um modelo executável de bomba de infusão de insulina genérico disponível gratuitamente para auxiliar os fabricantes durante o processo de certificação.

Em um trabalho relacionado com *CPN*, Sobrinho et al. (2017) propõem um modelo de referência para auxiliar a certificação de sistemas biomédicos utilizando *CPN*. São especificados componentes de hardware e software e aplica simulações e a técnica de verificação de modelos para avaliar o modelo.

3 REFERENCIAL TEÓRICO

O modelo de referência *CPN* para sistemas de controle da bomba de infusão de insulina é composto por elementos como lugares (elipses), transições (retângulos), tipos de dados e hierarquia. Um Módulo de *CPN* é uma tupla $CPN_M = (P, T, A, \Sigma, V, C, G, E, I, T_{sub}, P_{port}, PT)$:

1. P é um conjunto finito de lugares.
2. T é um conjunto finito de transições tal que $P \cap T = \emptyset$.
3. $A \subseteq P \times T \cup T \times P$ é um conjunto de arcos direcionados.
4. Σ é um conjunto finito não vazio de cores.
5. V é um conjunto finito de variáveis tipadas tal que $Tipo[v] \in \Sigma$ para todas as variáveis $v \in V$.
6. $C : P \rightarrow \Sigma$ é uma função de conjunto de cor que associa uma cor a cada lugar.
7. $G : T \rightarrow EXPR_V$ é uma função de guarda que associa uma guarda a cada transição t tal que $Tipo[G(t)] = Bool$.
8. $E : A \rightarrow EXPR_V$ é uma função de expressão de arco que associa uma expressão de arco a cada arco a tal que $Tipo[E(a)] = C(p)_{MS}^{12}$, onde p é o lugar conectado ao arco a .

¹² MS refere-se a “multiconjunto”.

9. $I : P \rightarrow \text{EXPR}_\theta$ é uma função de inicialização que associa uma expressão de inicialização a cada lugar p tal que $\text{Tipo}[I(p)] = C(p)_{MS}$.
10. $T_{sub} \subseteq T$ é um conjunto de transições de substituição.
11. $P_{port} \subseteq P$ é um conjunto de lugares porta.
12. $PT : P_{port} \rightarrow IN, OUT, I/O$ é uma função de tipo porta que associa tipos de porta a lugares.

Portanto, uma CPN hierárquica é definida tupla de quatro elementos $CPN_H = (S, SM, PS, FS)$:

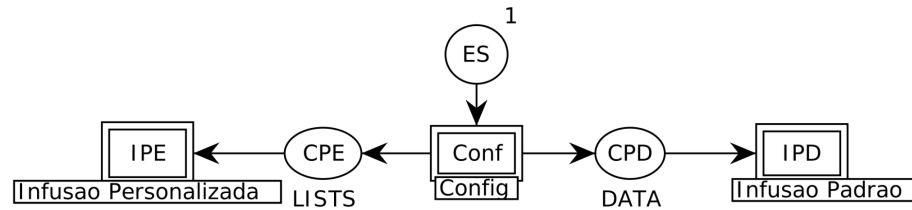
1. S é um conjunto finito de módulos. Cada módulo é um módulo de Rede de Petri $s = ((P^s, T^s, A^s, \Sigma^s, V^s, C^s, G^s, E^s, I^s), T_{sub}^s, P_{port}^s, PT^s)$. É necessário que $(P^{s_i} \cup T^{s_i}) \cap (P^{s_j} \cup T^{s_j}) = \emptyset$ para todo $s_i, s_j \in S$ tal que $i \neq j$.
2. $SM : T_{sub} \rightarrow S$ é uma função de sub-módulo que associa um sub-módulo a cada transição de substituição. É necessário que a hierarquia de módulo seja acíclica.
3. PS é uma função de relação porta-socket que associa uma relação porta-socket $PS(t) \subseteq P_{sock}(t) \times P_{port}^{SM(t)}$ para cada transição de substituição t . É necessário que $PT(p) = PT(p')$, $C(p) = C(p')$, e $I(p) \neq I(p')$ para todo $(p, p') \in PS(t)$ e $t \in T_{sub}$.
4. $FS \subseteq 2^P$ é uma família de conjuntos de fusão (*fusion sets*) não vazios tal que $C(p) = C(p')$ e $I(p) \neq I(p')$ para todo $p, p' \in fs$ e todo $fs \in FS$.

4 MODELO DE REFERÊNCIA

O modelo de referência consiste em um modelo CPN , considerando conjuntos de cores para representar as dosagens de insulina e o cartucho da bomba. O uso de conjuntos de cores inteiras permite aplicar a técnica de verificação de modelos, reduzindo o espaço de estados.

O modelo de referência contém cinco módulos. A composição dos módulos representa todo o sistema de controle da bomba de infusão de insulina. Na Figura 1 é ilustrado o módulo principal (*Bomba de Infusão de Insulina*). Este é o ponto inicial do refinamento modular intermediário (ou decomposição). Cada módulo está relacionado a uma etapa de refinamento modular intermediário. O módulo é dividido em duas partes: configuração da bomba e infusão de insulina. Para habilitar a infusão de insulina é necessário configurar a bomba. Mais especificamente, o módulo *Bomba de Infusão de Insulina* contém as transições de substituição $Conf, IPE$ e $IPD \in T_{sub}$.

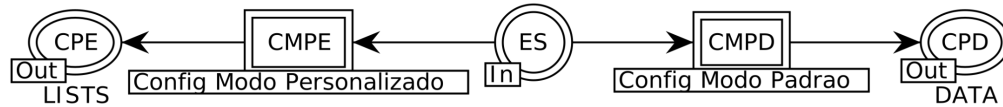
Figura 1 - Módulo *Bomba de Infusão de Insulina* do modelo de referência



Fonte: Autoria própria (2019).

A transição de substituição *Conf* refere-se ao submódulo *Config* (ou seja, $SM(Conf) = Config$). Este submódulo define o perfil que orienta as operações do sistema: padrão ou personalizado. Na Figura 2 é apresentado o submódulo *Config*. A configuração dos valores das dosagens de insulina muda dependendo do perfil do paciente.

Figura 2 - Submódulo *Config* do modelo de referência



Fonte: Autoria própria (2019).

A transição de substituição *CMPD* está relacionada ao submódulo *Config Modo Padrao* (ou seja, $SM(CMPD) = Config Modo Padrao$). Neste caso, as dosagens de insulina basal, bolus e bolus corretivo possuem valores padronizados, implicando na utilização da constante *CONF* para definir a marcação do local *DC* (Figura 3). A capacidade do cartucho também é configurada usando essa constante. Além disso, esses valores devem respeitar os limites superior e inferior. As funções *bolus*, *basal*, *cBolus* e *capCart* verificam esses limites. O sistema é capaz de injetar insulina quando a transição *Todas Config* é disparada.

Usando o modo personalizado, é necessário definir diferentes valores para diferentes dosagens basais diárias. Um arquivo carrega as dosagens de configuração para definir os valores do modo de infusão como estrutura de dados de lista. Esses valores dependem de prescrição médica para um caso específico. O restante da configuração segue a mesma abordagem do modo padrão. No final da configuração, duas listas representam as dosagens basais e bolus (*listBa* e *listDC*). Essas listas são as entradas para a infusão de insulina.

A segunda parte da modelagem do sistema de controle da bomba de infusão de insulina é a infusão de insulina. Esta parte da modelagem contém as especificações para os modos padrão e personalizado. Na Figura 4 é apresentado o submódulo para a infusão padrão. A primeira etapa é registrar os dados de configuração. O sistema notifica que a bomba está funcionando e que o cartucho está carregado. Posteriormente, é possível selecionar um modo específico disparando uma das transições *Adm Basal*, *Adm CBolus* e *Adm Bolus*. O usuário pode escolher um ou mais tipos de insulina durante a execução do sistema. Se a soma de todas as dosagens não ultrapassar um limite de segurança, o sistema aplica uma dosagem única composta por todos os tipos de insulina selecionados. Caso contrário, aplica-se apenas a quantidade máxima permitida. A transição *Aplicar Insulina* representa o evento que inicia a infusão de insulina. Quatro tuplas com 2 elementos cada representam a insulina basal, a insulina bolus corretiva, a insulina bolus e a capacidade do cartucho.

Considerando ambas as situações ($cap^{13} = 0$ ou abaixo da dosagem mínima necessária), a bomba transita do estado parcial de execução (removendo uma ficha sem cor do local E) para o estado parcial de parada (marcando o local S com uma ficha sem cor). Quando o usuário recarrega a bomba, o sistema retorna ao estado parcial de execução.

O modo de infusão de insulina personalizado se comporta de maneira semelhante ao modo padrão. Porém, ao invés de utilizar valores constantes de dosagens, permite ao usuário personalizar as dosagens desejadas a partir de um arquivo. Inicialmente, são utilizadas estruturas de dados de lista para representar as dosagens de insulina, que são convertidas para o formato original de tupla com dois elementos. Posteriormente, a primeira dosagem basal é removida de uma lista chamada *listaBa* (dosagens basais diárias de insulina) e inserida na cabeça da lista chamada *listaDC* (doses bolus, bolus corretivo e capacidade total do cartucho). Um lugar específico é responsável pelo registro das demais dosagens basais. Quando necessário, o sistema aplica essas dosagens basais. A representação da bomba de infusão permanece quase igual ao modo padrão. A mudança mais significativa diz respeito ao uso das doses basais restantes. O sistema repete a infusão até que existam fichas de dosagens basais representando o restante da insulina. Finalmente, a especificação do processo de recarga do cartucho também é quase igual ao modo padrão. Nesse caso, o modo personalizado contém novos lugares e transições para controlar as seguintes situações:

- o sistema aplicou a dosagem basal atual, sendo necessário aplicar as demais dosagens em um futuro próximo;
- é necessário aplicar a dosagem basal atual, sendo que as demais dosagens são registradas; e
- não há dosagem basal atual e nenhuma para o futuro.

Na Tabela 1 são apresentados os parâmetros de entrada do modelo de referência junto com descrições e exemplos de valores. Os valores são utilizados para ilustrar como um fabricante de bomba de infusão de insulina pode definir o modelo de referência para representar um produto específico. Os parâmetros *BASAL*, *BOLUS*, *CBOLUS*, *CAPCART*, *LIMITEDOSEINFERIOR*, *LIMITEDOSESUPERIOR*, *LIMITECAPCART* e *LIMITEINFUSAO* estão relacionados com valores inteiros para configurar a bomba, enquanto que o parâmetro *ARQUIVO* está relacionado com uma *string* que representa o nome de um arquivo contendo os valores de dosagem basal de insulina. Este refinamento de modelo é composto por tipos de dados inteiros para reduzir o problema de explosão de espaço de estados e simplificar a execução da técnica de verificação de modelos.

Tabela 1 - Parâmetros de entrada do modelo de referência

Parâmetro	Descrição	Valor Hipotético
BASAL	A dose de insulina basal	3
BOLUS	A dose de insulina bolus	3
CBOLUS	A dose de insulina bolus corretivo	3
CAPCART	A capacidade do cartucho	9

¹³ Variável *CPN* que representa a capacidade do cartucho.

LIMITEDOSEINFERIOR	O limite inferior de qualquer tipo de insulina	3
LIMITEDOSESUPERIOR	O limite superior de qualquer tipo de insulina	1
LIMITECAPCART	O limite da capacidade do cartucho	9
LIMITEINFUSAO	O limite de infusão de insulina	6
ARQUIVO	O nome do arquivo com valores de doses basal personalizadas	“BasalV1MR.txt”

Fonte: Autoria própria (2019).

5 AVALIAÇÃO DO MODELO DE REFERÊNCIA

Nesta seção é descrito um estudo de caso sobre o sistema de bomba de infusão comercial denominado *ACCU-CHEK Spirit* versão 2.XX. O estudo de caso estende o modelo de referência para avaliá-lo por meio da técnica de verificação de modelos. Além disso, é útil demonstrar como os fabricantes podem reutilizar o modelo durante o processo de projeto e certificação de sistemas de controle de bomba de infusão de insulina. Portanto, a configuração dos parâmetros do modelo de referência segue os requisitos técnicos do *ACCU-CHEK Spirit* versão 2.XX.

A verificação do modelo de referência está relacionada com a configuração dos parâmetros para aplicação da técnica de verificação do modelo. Considerando as propriedades do sistema, a configuração do modelo está de acordo com os requisitos técnicos do *ACCU-CHEK Spirit*. Na Tabela 2 é apresentada a configuração definida para a atividade de verificação (marcação inicial do modelo). O arquivo denominado *BasalV1AC.txt* contém 24 valores hipotéticos de dosagens basais para o modo personalizado.

Tabela 2 - Parâmetros de entrada do modelo de referência para o *ACCU-CHEK SPIRIT VERSION 2.XX*

Nome do Parâmetro	Valor Inteiro/String
BASAL	10
BOLUS	8
CBOLUS	6
CAPCART	315
LIMITEDOSEINFERIOR	25
LIMITEDOSESUPERIOR	1
LIMITECAPCART	315
LIMITEINFUSAO	25
ARQUIVO	“BasalV1AC.txt”

Fonte: Autoria própria (2019).

Esta atividade consiste na verificação das duas propriedades de segurança dos sistemas de controle da bomba de infusão de insulina mostradas na Tabela 3. A especificação do *ACCU-CHEK Spirit 2.XX* considera essas propriedades. Dado que a técnica de verificação de modelos utilizando *CPN* é baseada na lógica de árvore de computação (*Computation Tree Logic - CTL*), as funções disponíveis na biblioteca *ASK/CTL* do *CPN/Tools* representam as especificidades destas propriedades. O *ASK/CTL* é uma extensão baseada em *CPN* da lógica modal temporal *CTL*.

Tabela 3 - Amostra de propriedades de segurança de sistemas de controle de bomba de infusão de insulina

ID	Propriedade	Fórmula <i>ASK-CTL</i>
1	Se o nível do cartucho for igual a 0, então o estado do cartucho deve tornar-se “VAZIO” e o estado da bomba deve ser “PARADO”.	$OR(NOT(EV(NF("a_", p), Vazio))), EV(AND(NF("c_", bombaEmStop), NF("d_", cartVazio))))$
2	Se o nível do cartucho for menor do que a dosagem de insulina administrada, então o estado da bomba deve ser “PARADO”.	$OR(NOT(EV(NF("a_", nivelCartBaixo))), EV(NF("c_", bombaEmStop)))$

Fonte: Autoria própria (2019).

A descrição de ambas as propriedades sugere o uso de uma fórmula composta usando o conectivo de implicação. Considerando que *ASK/CTL* não fornece este conectivo, a fórmula representa a seguinte equivalência lógica: $\varphi \rightarrow \psi \equiv \neg\varphi \vee \psi$, onde $\rightarrow$, $\neg$ e $\vee$ são símbolos que representam os conectivos lógicos de implicação, negação e disjunção, respectivamente.

5.1 Verificação de Modelo da Propriedade 1

A primeira propriedade (Tabela 3, ID 1) define que quando o nível do cartucho é zero (ou seja, a bomba está vazia), o sistema deve ser parado. Portanto, a fórmula contém as seguintes proposições lógicas:

- φ = o nível do cartucho é 0;
- ψ_1 = o estado do cartucho é “VAZIO”; e
- ψ_2 = o estado da bomba é “PARADO”.

Portanto, isso implica na fórmula $\varphi \rightarrow (\psi_1 \wedge \psi_2)$ ao aplicar a equivalência lógica $\neg\varphi \vee \psi$. A fórmula *ASK/CTL* simplesmente traduz essa equivalência lógica. Posteriormente, o verificador de modelos analisou se o modelo está em conformidade com essa propriedade (Figura 5). As funções *cartZero*, *cartVazio* e *bombaEmStop* representam as proposições φ , ψ_1 e ψ_2 , respectivamente. Eles usam as instâncias locais chamadas *Aplicacao_de_insulina_padrao'Dados_Config*, *Aplicacao_de_insulina_padrao'STOP* e *Aplicacao_de_insulina_padrao'CARTUCHO_VAZIO* para verificar a primeira propriedade considerando o modo padrão de infusão de insulina. Para o modo personalizado, a única diferença é o nome de cada instância de local. É possível observar que o modelo de

referência está de acordo com a primeira propriedade usual dos sistemas de controle da bomba de infusão de insulina para os modos padrão e personalizado.

Figura 5 - Verificação de modelo da propriedade 1 para os modos padrão e personalizado

(a) Propriedade 1 para o modo de aplicação padrão

```
val cartZerado = fn : Node -> bool
val bombaEmStop = fn : Node -> bool
val cartVazio = fn : Node -> bool
val myASKCTLformula =
  OR
  (NOT (FORALL_UNTIL (TT,NF ("a_",fn))),
   FORALL_UNTIL (TT,NOT (OR (NOT (NF ("c_",fn)),NOT (NF ("d_",fn)))))) : A
val it = true : bool

fun cartZerado b = Mark.Aplicacao_de_insulina_padrao'Dados_Config 1 b = 1` (1,3)++1` (2,3)++1` (3,3)++1` (4,0);
fun bombaEmStop r = Mark.Aplicacao_de_insulina_padrao'STOP 1 r = 1` ();
fun cartVazio s = Mark.Aplicacao_de_insulina_padrao'CARTUCHO_VAZIO 1 s = 1` ();

val myASKCTLformula = OR(
  NOT(
    EV(NF("a_",cartZerado))),
    EV( AND( NF("c_",bombaEmStop), NF("d_",cartVazio) ) )
);

eval_node myASKCTLformula InitNode;
```

(b) Propriedade 1 para o modo de aplicação personalizado

```
val cartZerado = fn : Node -> bool
val bombaEmStop = fn : Node -> bool
val cartVazio = fn : Node -> bool
val myASKCTLformula =
  OR
  (NOT (FORALL_UNTIL (TT,NF ("a_",fn))),
   FORALL_UNTIL (TT,NOT (OR (NOT (NF ("c_",fn)),NOT (NF ("d_",fn)))))) : A
val it = true : bool

fun cartZerado b = Mark.Aplicacao_de_insulina_personalizado'Dados_Config 1 b = 1` (4,0);
fun bombaEmStop r = Mark.Aplicacao_de_insulina_personalizado'STOP 1 r = 1` ();
fun cartVazio s = Mark.Aplicacao_de_insulina_personalizado'CARTUCHO_VAZIO 1 s = 1` ();

val myASKCTLformula = OR(
  NOT(EV(NF("a_",cartZerado))),
  EV(AND(NF("c_",bombaEmStop),NF("d_",cartVazio)))
);

eval_node myASKCTLformula InitNode;
```

Fonte: Autoria própria (2019).

O formato da fórmula *ASK-CTL* difere da equivalência lógica $\neg\phi \vee (\psi_1 \wedge \psi_2)$ devido aos operadores *EV* e *NF*. O primeiro visa especificar que a fórmula considera todos os caminhos do espaço de estados no futuro, enquanto o segundo especifica que se trata de uma fórmula de nó. A função *eval_node* de *ASK-CTL* executa o algoritmo de verificação de modelos. O valor booleano *true* significa que o algoritmo confirma esta propriedade para o modelo.

5.1 Verificação de Modelo da Propriedade 2

A segunda propriedade (Tabela 3, ID 2) define que a bomba não pode funcionar quando a dosagem de insulina é maior que o nível do cartucho. A formalização desta propriedade seguiu a mesma abordagem da primeira propriedade. Inicialmente, considera algumas proposições:

- ϕ = o nível do cartucho é menor do que a dosagem de insulina administrada;
- ψ = o estado da bomba é “PARADO”.

Resultou na fórmula $\phi \rightarrow \psi$, mais uma vez, ao aplicar a equivalência lógica: $\neg\phi \vee \psi$. Posteriormente, essa fórmula foi simplesmente traduzida para sua respectiva fórmula *ASK-CTL*. Na Figura 6 são apresentados os resultados da verificação do modelo. As proposições ϕ e ψ são equivalentes às funções `nivelCartBaixo` e `bombaEmStop`, respectivamente. Estas funções estão relacionadas com as instâncias de lugar `Aplicacao_de_insulina_padrao'Atualizando_estado_da_bomba1` e `Aplicacao_de_insulina_padrao'STOP` para executar o algoritmo de verificação de modelos considerando o modo padrão. Para o modo personalizado, a única diferença é o nome de cada instância dos lugares.

Figura 6 - Verificação de modelo da propriedade 2 para os modos padrão e personalizado

(a) Propriedade 1 para o modo de aplicação personalizado

```
val nivelCartBaixo = fn : Node -> bool
val bombaEmStop = fn : Node -> bool
val myASKCTLformula =
  OR (NOT (FORALL_UNTIL (TT,NF ("a_",fn))),FORALL_UNTIL (TT,NF ("c_",fn))) : A
val it = true : bool

fun nivelCartBaixo i = Mark.Aplicacao_de_insulina_padrao'Atualizando_Estado_da_Bomba1 i <> [];
fun bombaEmStop r = Mark.Aplicacao_de_insulina_padrao'STOP 1 r = 1` ();

val myASKCTLformula = OR(
  NOT(EV(NF("a_",nivelCartBaixo))),
  EV(NF("c_",bombaEmStop))
);
eval_node myASKCTLformula InitNode;
```

(b) Propriedade 2 para o modo de aplicação personalizado

```
val nivelCartBaixo = fn : Node -> bool
val bombaEmStop = fn : Node -> bool
val myASKCTLformula =
  OR (NOT (FORALL_UNTIL (TT,NF ("a_",fn))),FORALL_UNTIL (TT,NF ("c_",fn))) : A
val it = true : bool

fun nivelCartBaixo i = Mark.Aplicacao_de_insulina_personalizado'Atualizando_Estado_da_Bomba1 i <> [];
fun bombaEmStop r = Mark.Aplicacao_de_insulina_personalizado'STOP 1 r = 1` ();

val myASKCTLformula = OR(
  NOT(EV(NF("a_",nivelCartBaixo))),
  EV(NF("c_",bombaEmStop))
);
eval_node myASKCTLformula InitNode;
```

Fonte: Autoria própria (2019).

Da mesma forma que a primeira propriedade, ela contém os operadores *EV* e *NF* de *ASK-CTL*. Isso permitiu a especificação da fórmula, enquanto a execução do algoritmo de verificação do modelos foi possível utilizando a função *eval_node* de *ASK-CTL*. Mais uma vez, o algoritmo apresentou o valor booleano *true*, significando que o modelo está de acordo com a segunda propriedade de sistemas de controle de bomba de infusão de insulina.

6 CONCLUSÕES E TRABALHOS FUTUROS

Neste trabalho foi apresentado a especificação formal de um modelo de referência de sistemas de controle de bombas de infusão de insulina com o objetivo de auxiliar no processo de certificação. Além disso, foi apresentado um estudo de caso sobre o sistema comercial de controle de bomba de infusão de insulina denominado *ACCU-CHEK Spirit 2.XX*. Um modelo de referência é relevante no contexto da certificação porque esses sistemas críticos seguros são manipulados para tratar pacientes com diabetes.

O modelo de referência foi especificado usando a linguagem de modelagem *CPN* (juntamente com o software *CPN/Tools*) e inclui os recursos essenciais que garantem o funcionamento correto de um sistema de controle de bomba de infusão de insulina. A linguagem *CPN* permitiu a especificação considerando parâmetros, módulos, simulação e verificação.

O modelo apresentado neste artigo é relevante porque possui características não totalmente consideradas pelas soluções existentes. Isso inclui, por exemplo, parâmetros (modelo instanciado para diferentes sistemas), módulos (gerenciamento da complexidade da especificação) e execução (simulação de comportamentos reais).

O estudo de caso foi útil para estender o modelo de referência conduzindo verificações. Foi considerada a verificação de duas propriedades de segurança do sistema para o controle da infusão de insulina. Além disso, o estudo de caso demonstra que os fabricantes podem reaproveitar o modelo durante o processo de certificação de sistemas de controle de bombas de infusão de insulina.

O modelo *CPN* é um artefato de projeto usado para realizar atividades de verificação com o objetivo de aumentar a confiança nos sistemas de controle da bomba de infusão de insulina. Além disso, é útil realizar avaliações de qualidade das propriedades do sistema, como segurança, durante um processo de certificação. Por exemplo, uma vez que uma agência reguladora emite um *recall* de um sistema, o modelo de referência pode ajudar os fabricantes a avaliar a especificação atual, comparando a solução física com a especificação formal (solução simulada). Isso pode diminuir o custo e o tempo de desenvolvimento, permitindo a correção imediata dos defeitos/falhas com base no modelo do sistema em avaliação. Portanto, a principal contribuição com este trabalho é o modelo de referência de sistemas de controle de bombas de infusão de insulina de forma que os fabricantes podem reutilizar durante um processo de certificação (junto com o estudo de caso).

Um exemplo de trabalho futuro é a extensão do modelo de referência de sistemas de controle de bomba de infusão de insulina para representar recursos de tempo e uma bomba de infusão de insulina de circuito fechado. A versão de circuito fechado incluirá a detecção de glicose e monitoramento e tratamento de pacientes com diabetes. Além disso, pretende-se definir um modelo mais genérico para representar qualquer tipo de sistema de bomba de infusão, como sistemas de bomba de infusão de analgésicos.

REFERÊNCIAS

- HATCLIFF, J.; LARSON, B.; CARPENTER, T.; JONES, P.; ZHANG, Y.; JORGENS, J. The open pca pump project: An exemplar open source medical device as a community resource, in: Medical Cyber Physical Systems Workshop, 2018.
- IMAGAWA, K.; MIZUKAMI, Y.; MIYAZAKI, S. Regulatory convergence of medical devices: a case study using iso and iec standards, *Expert Review of Medical Devices* (2018) 497504.
- JENSEN, K.; KRISTENSEN, L. M. Coloured Petri nets: a graphical language for formal modeling and validation of concurrent systems. *Communications Of The ACM* (2015) 6170.
- MERTZ, L. Automated insulin delivery: Taking the guesswork out of diabetes management. *IEEE Pulse*, Institute of Electrical and Electronics Engineers (IEEE), v. 9, n. 1, p. 8–9, jan 2018. Disponível em: <<https://doi.org/10.1109/mpul.2017.2772685>>.
- MUANGPRATHUB, J.; BOONJING, V. Online thai medical diagnostic system using case-based reasoning. In: 2014 International Computer Science and Engineering Conference (ICSEC). IEEE, 2014. Disponível em: <<https://doi.org/10.1109/icsec.2014.6978179>>.
- NIEZEN, G.; ESLAMBOLCHILAR, P. A human operator model for medical device interaction using behavior-based hybrid automata. *IEEE Transactions on Human-Machine Systems*, Institute of Electrical and Electronics Engineers (IEEE), v. 46, n. 2, p. 291–302, apr 2016. Disponível em: <<https://doi.org/10.1109/thms.2015.2487509>>.
- RATHORE, H.; WENZEL, L.; AL-ALI, A. K.; MOHAMED, A.; DU, X.; GUIZANI, M. Multi-layer perceptron model on chip for secure diabetic treatment. *IEEE Access*, Institute of Electrical and Electronics Engineers (IEEE), v. 6, p. 44718–44730, 2018. Disponível em: <<https://doi.org/10.1109/access.2018.2854822>>.
- SHARANYA, G.; ABHISHEK, C. S.; REDDY, K. M. Health monitoring device. In: 2017 2nd International Conference on Communication and Electronics Systems (ICCES). IEEE, 2017. Disponível em: <<https://doi.org/10.1109/cesys.2017.8321163>>.
- SILVA, L. C.; ALMEIDA, H. O.; PERKUSICH, A.; PERKUSICH, M. A model-based approach to support validation of medical cyber-physical systems, *Sensors* (2015) 27625-27670.
- SJAAHEIM, H.; ALBERT, B.; SETCHI, R.; NOYVIRT, A.; STRISLAND, F. A portable medical system for the early diagnosis and treatment of traumatic brain injury, in: 2014 IEEE International Conference On Systems, Man, And Cybernetics, 2014, pp. 2529-2534.
- SOBRINHO, A.; SILVA, L. D.; PERKUSICH, A.; CUNHA, P.; CORDEIRO, T. D.; LIMA, A. M. N. Formal modeling of biomedical signal acquisition systems: source of evidence for certification. *Software and Systems Modeling*, pp.1-19. 2017. Disponível em: <<https://doi.org/10.1007/s10270-017-0616-7>>.
- ZHANG, Y.; JONES, P. L.; JETLEY, R. A hazard analysis for a generic insulin infusion pump.

Journal of Diabetes Science and Technology, SAGE Publications, v. 4, n. 2, p. 263–283, mar 2010. Disponível em: <<https://doi.org/10.1177/193229681000400207>>.