UNIVERSIDADE FEDERAL DE ALAGOAS
INSTITUTO DE COMPUTAÇÃO
PROGRAMA DE PÓS GRADUAÇÃO
EM INFORMÁTICA

JOSÉ CAVALCANTE REIS NETO

Especificação Formal do Gerenciamento de Risco de Equipamentos Médicos baseado na ISO 14971:2009 utilizando Redes de Petri Coloridas

Maceió
Dezembro de 2014

JOSÉ CAVALCANTE REIS NETO

Especificação Formal do Gerenciamento de Risco de Equipamentos Médicos baseado na ISO 14971:2009 utilizando Redes de Petri Coloridas

Dissertação apresentada como requisito parcial para obtenção do grau de Mestre pelo Programa de Pós-Graduação em Informática do Instituto de Computação da Universidade Federal de Alagoas.

Orientador: Prof. Dr. Leandro Dias da Silva

Maceió
Dezembro de 2014

Catalogação na fonte
Universidade Federal de Alagoas
Biblioteca Central
Divisão de Tratamento Técnico
Bibliotecário: Valter dos Santos Andrade

R375e Reis Neto, José Cavalcante.
Especificação formal do gerenciamento de risco de equipamentos médicos baseado na ISSO 14971:2009 utilizando redes de petri coloridas / José Cavalcante Reis Neto. – Maceió, 2014.
75 f. : il.

Orientador: Leandro Dias da Silva.
Dissertacão (Mestrado em Informática) – Universidade Federal de Alagoas. Instituto de Computação. Programa de Pós-Graduação em Informática. Maceió, 2014.

Bibliografia: f. 61-64
Apêndices: f. 65-75.

1. Gerenciamento de risco. 2. Redes petri coloridas. 3. ISO 14971:2009. Equipamentos médicos - Utilização. I. Título.

CDU: 004.7

UNIVERSIDADE FEDERAL DE ALAGOAS/UFAL
Programa de Pós-Graduação em Informática – PPGI
Instituto de Computação
Campus A. C. Simões BR 104-Norte Km 14 BL 12 Tabuleiro do Martins
Maceió/AL - Brasil CEP: 57.072-970 | Telefone: (082) 3214-1401

Membros da Comissão Julgadora da Dissertação de Mestrado de José Cavalcante Reis Neto, intitulada: "*Especificação Formal do Processo de Gerenciamento de Risco de Equipamentos Médicos baseado na ISO 14971:2009 utilizando Redes de Petri Coloridas*", apresentada ao Programa de Pós-Graduação em Informática da Universidade Federal de Alagoas em 29 de dezembro de 2014, às 16h00min, no Miniauditório do Instituto de Computação da UFAL.

COMISSÃO JULGADORA

Prof. Dr. Leandro Dias da Silva
UFAL – Instituto de Computação
Orientador

Prof. Dr. Evandro de Barros Costa
UFAL – Instituto de Computação
Examinador

Prof. Dr. Kyller Costa Gorgônio
UFCG – Universidade Federal de Campina Grande
Examinador

Ad Majorem Dei Gloriam

AGRADECIMENTOS

Agradeço primeiramente a Deus por dar-me força para conseguir, depois de tantas dificuldades, chegar nesta etapa final.

Agradeço a minha família que sempre me apoiou, me educou e fez de mim um ser humano melhor. Em especial agradeço a Jarbas, Adalgisa, Izaura, Lívia e Glória o amor de vocês é o que me alegra a cada manhã. Agradeço aos meus primos-irmãos que, mesmo morando tão perto, a correria do cotidiano atrapalha o convívio mais intenso. Agradeço a Anna Lyvia por estar ao meu lado nas dificuldades e nas alegrias pela paciência, compreensão e amor, obrigado.

Agradeço as Religiosas da Instrução Cristã por toda a formação e pela amizade, aprendi e aprendo muito com vocês.

Agradeço a Paulo Cunha e Álvaro Alvares pelo auxílio na realização deste trabalho.

Agradeço aos meus amigos-irmãos por todas as alegrias nos momentos de descontração e apoio. As Sociais e os amigos do Panda Fc por todos aos bons momentos.

A todos que me ajudaram de forma direta ou indireta para a realização deste trabalho, obrigado.

RESUMO

O avanço da medicina e da tecnologia da informação (TI) tem propiciado o surgimento de novas técnicas e equipamentos que, gradativamente, oferecem melhorias diretas ou indiretas à saúde dos pacientes como, por exemplo, as técnicas cirúrgicas minimamente invasivas e os novos equipamentos para diagnóstico e monitoramento de pacientes (HOLSBACH; NETO; HOLSBACH, 2013). É com a utilização destes equipamentos que se torna possível ter melhores condições de diagnóstico e tratamento de doenças, menor tempo de internação, maior praticidade e privacidade, permitindo inclusive ao paciente proceder com o tratamento domiciliar, contudo, o crescimento da quantidade de dispositivos nem sempre está aliada à qualidade. A má qualidade destes equipamentos é um problema que pode comprometer a saúde do paciente e do operador e, por isso, se faz necessária a utilização de técnicas e padrões que permitam a fabricação de equipamentos médicos mais seguros, tais como a técnica *Análise dos Modos de Falha Efeitos e Criticidade* (FMECA) e o padrão International Organization for Standardization (*ISO*) 14971 (ABNT - ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2009). A *ISO 14971* foi desenvolvida com o propósito de indicar os controles e os cuidados básicos que devem ser observados pelo fabricante em todo o ciclo de vida de um equipamento médico. De acordo com esta ISO, segurança é a ausência de riscos não aceitáveis e a verificação se os riscos encontrados são aceitáveis ou não acontece durante o processo de gerenciamento de risco, porém, os fabricantes ao adotar o gerenciamento de risco descrito em linguagem natural, que é ambígua, estão suscetíveis a problemas tais como, falta de compreensão das etapas do processo de gerenciamento de risco, criação de processo demasiadamente complexo ao qual terão dificuldade de aplicar ou simplista demais que não contempla todo o gerenciamento de risco. Com a finalidade de solucionar o supracitado problema é apresentado neste trabalho um estudo de caso explorando o processo de gerenciamento de risco baseado na *ISO 14971* com a técnica *FMECA*, com o objetivo de realizar a especificação de segurança de um equipamento médico de Eletrogastrografia (EGG). Esse estudo de caso foi realizado no Hospital Universitário da Universidade Federal de Alagoas e contou com o auxílio de um especialista em desenvolvimento de sistemas de aquisição de sinais biomédicos. Esse estudo é a base para a construção do modelo formal em Redes de Petri Coloridas do processo de gerenciamento de risco. O modelo em Redes de Petri Coloridas auxilia no entendimento da ISO, ao reduzir a subjetividade inerente a descrição em linguagem natural. Além disto, este modelo auxilia nas etapas de verificação e validação do equipamento médico e possibilita uso do modelo como uma ferramenta didática para o ensino e treinamento do processo de gerenciamento de risco.

Palavras-chaves: ISO14971:2009. Redes de Petri Coloridas. Gerenciamento de Risco.

ABSTRACT

The advance of medicine and Information Technology (IT) has allowed the emergence of new techniques and medical device to provide direct or indirect improvements to the people's health, such as the minimally invasive surgical techniques and new devices for diagnosis and patient monitoring (HOLSBACH; NETO; HOLSBACH, 2013). The use of such devices provides a better diagnosis procedure and better diseases treatment, shorter hospital stay, convenience and privacy, as well as the possibility of the patient to proceed with home treatment. However, the growth of the number of devices is not always based on quality. The poor quality of such device is a problem that may compromise people's health. Therefore, in order to mitigate the risks of failures during the development of these medical devices, the manufacturers must follow safety standards specifications, such as the International Organization for Standardization (*ISO*) 14971 (ABNT - ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2009) and the technique Failure Mode, Effects and Criticality Analysis (FMECA). The *ISO 14971* was specified to guide the controls and basic care to be observed by the manufacturer throughout the development of all stages during the medical device's life cycle. According to this standard, security is freedom from unacceptable risk, and the discovery and verification if the risk is unacceptable or not happen during the risk mannagment process. However the *ISO 14971* was described in natural language, which is an error-prone description, ambiguous and is susceptible to problems such as misunderstanding of the stages of the risk management process, creating too complex process which will be difficult to be applied or too simplistic that does not address all risk management. Within this context, we use the *ISO 14971* standard with the *FMECA* technique to provide a case study that performs the security specification of the Electrogastrography (EGG) device. This case study was performed at the Federal University of Alagoas Hospital, with the support of an expert in the development of biomedical signal acquisition systems. This case study was the basis to develop a Colored Petri Net that describes the risk management process, reducing the problems on natural language descriptions. In addition, this model helps in the verification and the validation steps of medical devices manufacturing and allows the use of modeling as a tool for teaching and training the risk management process.

Keywords: ISO14971:2009. Colored Petri Net. Risk Management.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO

O avanço da medicina e da Tecnologia da Informação (TI) tem propiciado o surgimento de novas técnicas e equipamentos que, gradativamente, oferecem melhorias diretas ou indiretas à saúde dos pacientes. Como, por exemplo, as técnicas cirúrgicas minimamente invasivas e os novos equipamentos para diagnóstico e monitoramento (HOLSBACH; NETO; HOLSBACH, 2013). Entende-se por equipamento médico todo dispositivo que é usado com o propósito de auxiliar na melhoria da saúde do pacientes, seja para o diagnóstico, monitoramento, terapia ou cirurgia (BLOOMFIELD et al., December 2012). Existe um grande número de dispositivos médicos que são utilizados para desempenhar estes propósitos (BLOOMFIELD et al., December 2012). Neste contexto, deve-se considerar que é cada vez mais frequente a quantidade de dispositivos médicos que possuem *software* embarcado.

Os novos dispositivos com *software* embarcado, além dos propósitos convencionais, é também utilizado para o monitoramento, diagnóstico e a administração de medicamentos a distância de forma automática (KUMAR et al., 2013). Assim é possível prover melhores condições de tratamento de doenças, menor temp o de internação, maior comodidade, praticidade e privacidade, ofertando a possibilidade do paciente optar por um tratamento exclusivamente domiciliar (PATARA; VICARIO, 2014). Contudo, a fim de atender a crescente demanda por esses novos equipamentos médicos, a qualidade destes dispositivos é comprometida. Tratando-se especialmente da área médica, onde falhas, sejam relacionadas ao dispositivo médico ou sua má operação, podem causar danos irreparáveis aos usuários, a qualidade e o bom funcionamento são fatores essenciais.

Todo equipamento médico demanda um cuidado especial, principalmente no tocante à sua fabricação, manuseio, e aferições. Tendo em vista que até mesmo a imprecisão nas medições como, por exemplo, da glicemia, pode levar à adoção de um procedimento corretivo equivocado, acarretando assim em riscos à saúde do paciente (HATCLIFF et al., 2012). Evidencia-se, assim, que fabricar equipamentos médicos é um processo crítico, onde existe a necessidade da adoção de processos de fabricação confiáveis para detecção e eliminação de falhas em nível de *hardware* e *software*, considerando a manutenção da integridade física do paciente, operador e médico. Os Equipamentos Médicos Eletrônicos (EME) são exemplos de sistemas onde a tolerância a falhas é baixa. As falhas, quando existirem, devem ser excluídas ou minimizadas, a fim de garantir a integridade física dos pacientes e operadores. Sistemas com essas características são denominados de *sistemas críticos de segurança* (AMARENDRA, 2011).

Os *sistemas críticos de segurança* são sistemas desenvolvidos para atender às necessidades das áreas onde existe baixa tolerância a falhas como, por exemplo, a área de saúde do ser humano, a economia e transporte (AMARENDRA, 2011). Nos *sistemas*

críticos de segurança, a segurança humana é dependente do funcionamento correto do sistema, devendo existir somente as falhas consideradas toleráveis, ou seja, aquelas que não apresentam riscos de lesão ao operador e ao usuário. A segurança é avaliada em relação aos elementos físicos do equipamento médico, mas também, ponderando os problemas de *software* e limitações na capacitação dos operadores.

Os *sistemas críticos de segurança* devem ser projetados para atender a rigorosas especificações técnicas de fabricação. Os equipamentos médicos, em especial, seguem a International Organization for Standardization (*ISO*) 14971 (ABNT - ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2009). A *ISO 14971* foi desenvolvida com o intuito de indicar os controles e os cuidados básicos que devem ser observados pelo fabricante, nas fases de projeto, fabricação e pós produção do equipamento médico (JAIN et al., 2010). É definido nessa *ISO* o risco como uma função matemática composta pela combinação da probabilidade de ocorrência do dano (frequência) e a severidade desse dano, ou seja, *risco = probabilidade de ocorrência X severidade do dano* (HEGDE, 2011). A principal característica da *ISO 14971* é o gerenciamento de risco. Nessa atividade, estão presentes, de forma descritiva, os passos necessários para assegurar que os riscos foram controlados ou eliminados, e os riscos remanescentes podem ser considerados como aceitáveis. O gerenciamento de risco contempla todo o ciclo de vida do dispositivo médico e o registro das informações pertinentes a cada etapa é mantida no arquivo de gerenciamento de risco (HUFFMAN; BOWMAN; AKERS, 2013). No arquivo de gerenciamento de risco deve conter o registro sobre todos os riscos encontrados, assim com todas precauções e métricas de controle destes riscos e informações sobre os membros das equipes e suas respectivas atribuições no projetos. Os termos e expressões que foram adotados na *ISO* e são adotados neste trabalho estão descritos na Tabela 1.

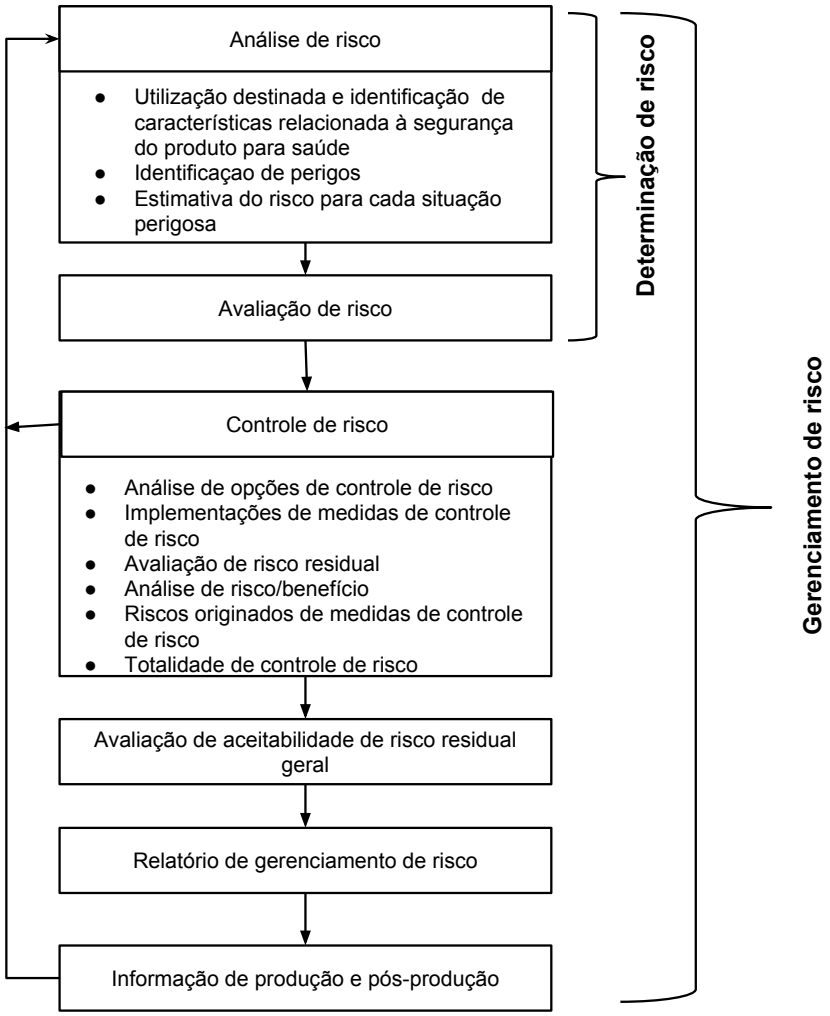
O processo de gerenciamento do risco na construção de equipamento médico inclui as fases de planejar, descobrir e mitigar os riscos. É compreendido por 4 etapas: análise do risco (*risk analysis*), avaliação do risco (*risk evaluation*), controle do risco (*risk control*) e informação de pós-produção (*post-production information*), como ilustrado na Figura 1. É ilustrado na Figura 1 as fases do gerenciamento de risco segundo (ABNT - ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2009), por intermédio destas etapas busca-se identificar e analisar os perigos e definir ações para controlá-los (BURTON; MCCAFFERY; RICHARDSON, 2006).

Tabela 1 – Termos e expressões baseados na *ISO* 14971.

Termos da ISO	**Descrição**
Dano	lesão física ou prejuízo à saúde da pessoa, ou prejuízo à propriedade ou ao meio ambiente
Perigo	fonte potencial de dano
Situação perigosa	circunstância em que pessoa, propriedade ou meio ambiente estejam expostos a um ou mais perigo(s)
Severidade	medida das possíveis conseqüências de um perigo
Risco	combinação da probabilidade de ocorrência de um dano e a severidade de tal dano
Análise de risco	utilização sistemática de informação disponível para identificar perigos e estimar riscos
Estimativa de risco	processo utilizado para designar valores à probabilidade de ocorrência do dano e à severidade de tal dano
Gerenciamento de risco	aplicação sistemática de políticas, procedimentos e práticas de gerenciamento às tarefas de análise, avaliação, controle e monitoração de risco
Segurança	ausência de riscos inaceitáveis

Fonte: (ABNT - ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2009)

Figura 1 – Fases do gerenciamento de risco



Fonte: (ABNT - ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2009)

Ao término do processo de gerenciamento de risco, quando solicitado, o mesmo deve ser enviado para uma agência reguladora. A agência reguladora é responsável por inferir que o equipamento é de fato seguro e pode ser lançado no mercado. No Brasil, a agência reguladora é a Agência Nacional de Vigilância Sanitária (*ANVISA*[1]). Nos Estados Unidos é responsabilidade do departamento Americano de Administração de Drogas e Alimentos (do inglês, *Food and Drug Administration* (*FDA*[2])). Ambos adotam como padrão de segurança a ISO 14971. É ilustrado na Figura 2 todo o cliclo de gerenciamento de risco segundo a ISO 14971, é baseado neste ciclo de vida que a especificação de segurança é realizada. A validação do equipamento é realizado principalmente utilizando o arquivo de gerenciamento de risco, pois é nele que estão contidas as informações de todos os riscos identificados, as soluções para os riscos e os níveis para serem classificados como riscos aceitáveis ou não (ABNT - ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2009).

No FDA, após a conferência e a constatação de segurança, os arquivos de gerenciamento de risco são persistidos na base de dados denominada *Manufacturer and User Facility Device Experience*, MAUDE (BARTOO, 2003). Infelizmente, a *ANVISA* não dispõe de nenhum mecanismos semelhante ao MAUDE, pois é com base nos dados contidos neste banco de dados que muitos estudos sobre segurança de equipamento médicos podem ser elaborados. Um desses estudos é apresentado em (ALEMZADEH et al., 2013). Segundo o estudo, nas falhas em equipamentos médicos que apresentam alto risco à vida, 33,3% dos erros são erros de *software*. Os 66,7% restantes são distribuídos entre as falhas de: entrada/saída (I/O) (sensores, alarmes, botões, teclas), *hardware* (memória, chips, disco rígido, capacitor, curto-circuito), bateria (suprimento elétrico, carga e descarga de energia) e outros (auto-teste, reinicialização, documentação)(vide Tabela 2). Estes problemas podem ser evitados ou mitigados com a execução do gerenciamento de risco.

Tabela 2 – Classificação de falhas dos sistemas cadastrados no MAUDE.

Classe das Falhas	**Falhas**
Software	Banco de Dados, Código, Bugs, Atualizações, Versão
Entrada/Sáida (I/O)	Sensores, Alarmes, Botões,Teclas
Hardware	Mémoria, Chips, Disco Rígido, Capacitor, Curto-circuito
Bateria	Suprimento Elétrico, Carga , Descarga de Energia
Outros	Auto-teste, Reinicialização, Documentação

Fonte: (ALEMZADEH et al., 2013)

[1] <http://anvisa.gov.br>
[2] https://fda.gov

1.1 Objetivo do trabalho

É proposto neste trabalho, com intermédio da ISO 14971, um processo para controlar e gerenciar os riscos na fabricação de equipamentos médicos, todavia, por se tratar de um processo que é apresentado de forma descritiva, em linguagem natural, dá-se origem a problemas de subjetividade na interpretação da leitura. Esses problemas podem ser vistos na imprecisão de como classificar de forma apropriada os riscos, assim como determinar quando e como estes riscos devem ser controlados. Destaca-se também, a ausência de detalhes importantes como, por exemplo, quando se deve iniciar uma nova etapa do processo de gerenciamento do risco e quando encerrá-la. Com isto, foi desenvolvida neste trabalho uma metodologia que permite um melhor entendimento de todo o gerenciamento do risco e possibilita que, mesmo uma equipe reduzida de especialistas, possa realizar as especificações de segurança.

É proposto neste trabalho, com intermédio da ISO 14971, um processo para controlar e gerenciar os riscos na fabricação de equipamentos médicos, todavia, por se tratar de um processo que é apresentado de forma descritiva, em linguagem natural, dá-se origem a problemas de subjetividade na interpretação da leitura. Esses problemas podem ser vistos na imprecisão de como classificar de forma apropriada os riscos, assim como determinar quando e como estes riscos devem ser controlados. Destaca-se também, a ausência de detalhes importantes como, por exemplo, quando se deve iniciar uma nova etapa do processo de gerenciamento do risco e quando encerrá-la. Com isto, foi desenvolvida neste trabalho uma metodologia que permite um melhor entendimento de todo o gerenciamento do risco e possibilita que, mesmo uma equipe reduzida de especialistas, possa realizar as especificações de segurança.

Foi realizado um estudo de caso aplicando os conceitos apresentados na ISO 14971:2009 com o objetivo de executar o gerenciamento de risco do equipamento médico de Eletrogastrografia (EGG) de superfície. Este equipamento é classificado segundo a *ANVISA* como equipamento de Classe II.

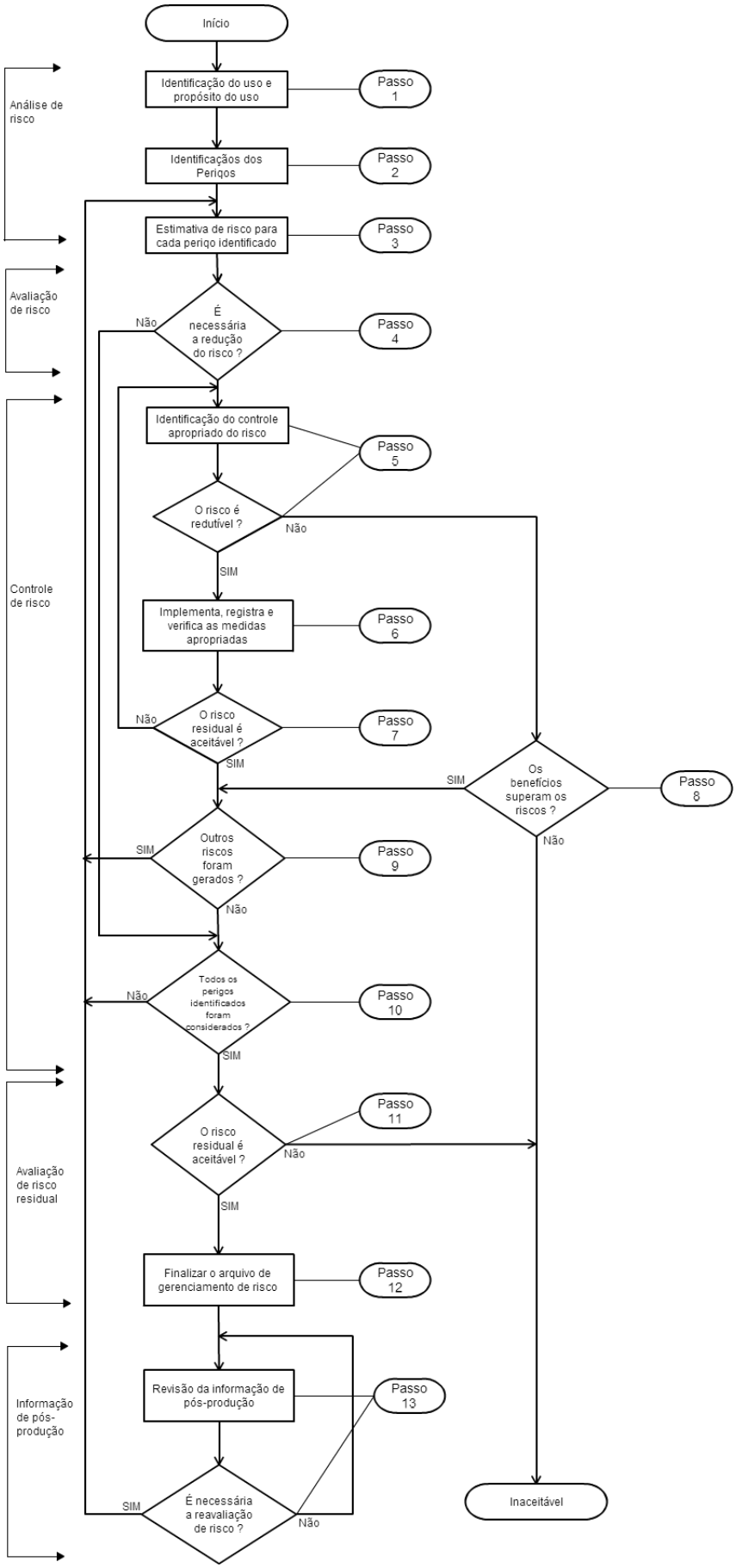
Após o estudo de caso, foi elaborado um modelo formal com o propósito de auxiliar na compreensão do processo de gerenciamento de risco através da ISO 14971. Para isso, é proposta a modelagem do processo de gerenciamento de risco utilizando Redes de Petri Coloridas (RPC) (JENSEN, 2009). Esta modelagem torna possível descrever um problema e suas etapas de forma não ambígua, diferentemente da descrição em linguagem natural que é ambígua. Além de permitir a simulação de todo o processo de gerenciamento de risco utilizando a ferramenta *CPN/Tools* [3]. A ferramenta *CPN/Tools* é uma ferramenta gráfica utilizada para editar, simular e analisar *RPC* e será melhor detalhada na seção 2.3.2.

[3] <http://cpntools.org/>

1.2 Organização do Trabalho

O restante desta dissertação está organizada em 4 capítulos além deste: No Capítulo 2 é apresentado o embasamento teórico, onde são apresentadas as informações necessárias para o melhor entendimento deste trabalho. No Capítulo 3 é detalhado o estudo de caso do gerenciamento de risco para a fabricação de um equipamento médico de Eletrogastrografia. No Capítulo 4 é discutido o modelo formal da ISO em *RPC*. Por fim, no Capítulo 5 são apresentadas as considerações finais e sugestões para trabalhos futuros.

Figura 2 – Passo-a-passo do ciclo de vida da *ISO* 14971



Fonte: (INTERNATIONAL ORGANISATION FOR STANDARDISATION, 2000)

2 EMBASAMENTO TEÓRICO

Neste capítulo são introduzidos os referenciais teóricos necessários para o entendimento sobre o processo de gerenciamento de risco de equipamentos médicos que possuem software embarcados. São apresentadas as informações relevantes para a concepção e análise do gerenciamento de risco, tendo como referência o dispositivo médico de Eletrogastrografia (EGG) e a modelagem utilizando *RPC*.

2.1 Eletrogastrografia

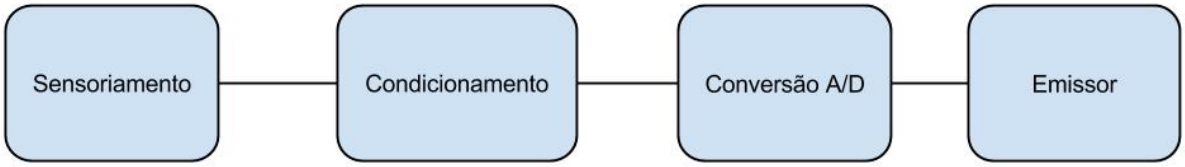
Eletrogastrografia é definida como o registro dos impulsos mioelétricos da musculatura lisa do estômago. É uma técnica não invasiva que utiliza sensores acoplados na pele do paciente para medir a frequência de propagação das contrações gástricas, denominadas ondas lentas (KOMOROWSKI; PIETRASZEK; GRZECHCA, 2012).

A Eletrogastrografia é utilizada para medir as disritmias gástricas que são definidas como *tachgastrya*, *bradygastria* e *arrhythmia*. Em seres humanos saudáveis a frequência dominante das atividades mioelétricas do estômago é 3 Ciclos Por Minuto (cpm) (MATSUURA et al., 2007). Quando a frequência dominante do estômago encontra-se em uma faixa abaixo de 0.5-2.0 cpm, denomina-se bradygastria (YIN; CHEN, 2013/Jan). A Bradygastria é caracterizada pela redução nas atividades contráteis do estômago, consequentemente, ocorre a diminuição do número de contrações dificultando o processo digestivo (MORELLO; CAPUA; LAMONACA, 2013). Por outro lado, tachygastria ocorre quando a frequência dominante encontra-se na faixa entre 4-9 cpm (PASKARANANDAVADIVEL et al., 2013), nesse caso, o estômago tem um comportamento atônico e a atividade elétrica apresenta amplitude insuficiente para induzir as contrações gástricas (PARKMAN et al., 2003). Por fim, a *arrhythmia*, caracteriza-se pela ausência de um ritmo dominante das ondas lentas. As disritmias gástricas estão associadas a problemas de saúde tais como vomito, anorexia, perturbação na digestão (KOMOROWSKI; PIETRASZEK; GRZECHCA, 2012). Atribui-se o nome de Eletrogastrografia (EGG) tanto ao registro dos impulsos mioelétricos da musculatura lisa do estômago, quanto ao equipamento que realiza os registros (YIN; CHEN, 2013/Jan)

2.1.1 Equipamento

O EGG estudado caracteriza-se por ser um equipamento médico de baixo custo e baixo consumo de energia. Possui como matriz energética de todo sistema uma bateria de 9 volts. A aquisição dos sinais mioelétricos é baseado em quatro etapas: Sensoriamento, Condicionamento, Conversão Analógico/Digital e Sistema Digital, ilustrado na Figura 3.

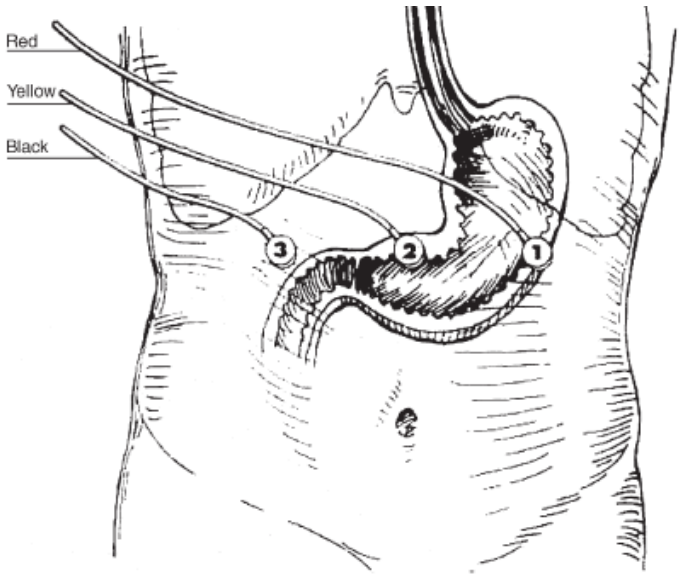
Figura 3 – As quatro etapas para aquisição dos sinais



Fonte: Elaborada pelo autor

A etapa *Sensoriamento* compreende o conjunto formado por cabos de blindagem e eletrodos. É nessa fase que os sinais biológicos são convertidos para elétricos. São acoplados à pele do paciente, na região do abdômen, sobre o eixo do antro do estômago, três eletrodos (MORELLO; CAPUA; LAMONACA, 2013; PARKMAN et al., 2003). Os eletrodos são ao todo três: dois de sinais e um de referência. Eles são acoplados à pele do paciente após ser realizada a assepsia da mesma. A assepsia é necessária para eliminar qualquer tipo de interferência entre a pele e o eletrodo, evitando ruídos no sinal. A ilustração da utilização dos eletrodos pode ser visto na Figura 4.

Figura 4 – Utilização dos eletrodos



Fonte: (PARKMAN et al., 2003)

A segunda etapa, *Condicionamento*, é composta por dois circuitos integrados: o amplificador de instrumentação biomédica e o amplificador operacional. O principal objetivo do amplificador de instrumentação biomédica é converter o sinal de tensão de entrada para um sinal que é baixo, em microvolts, amplificando o sinal de tensão até a escala de volts, possibilitando assim, o processamento desse sinal. O amplificador operacional por sua

vez é composto por dois filtros, filtro de passa-alta e de passa-baixa (LIM et al., 2007). O filtro de passa alta é utilizado para remover os ruídos provenientes do contato entre a pele e os eletrodos (LIM et al., 2007). Além do uso do filtro passa-alta, com o objetivo de eliminar o ruído de alta frequência acumulado, é necessário o uso do filtro de passa baixa. Esse filtro permite que apenas os sinais que estejam abaixo de uma determinada faixa de frequência sejam aceitos.

Na etapa de *Conversão A/D*, o sinal analógico, previamente amplificado e filtrado, é convertido para digital. A Conversão possibilita a manipulação do sinal nos sistemas digitais atuais. A etapa final consiste na utilização da tecnologia *(Bluetooth) IEE 802.15* [1] para o envio dos dados coletados.

2.2 ISO

A Organização Internacional para Padronização (*International Organization for Standardization* (*ISO*)) é uma federação mundial voltada para o estabelecimento de padrões e normas. O processo de preparação de Normas Internacionais é geralmente realizado através de comitês técnicos da *ISO*. Para a definição de uma nova *ISO* é criada uma comissão na qual os integrantes possuem conhecimento no assunto específico. Esta comissão é composta por membros de organizações internacionais, que podem ser governamentais e não-governamentais (ABNT - ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2009).

A ISO 14971 é um arcabouço que contém as obrigações mínimas que devem ser seguidas (SCHMULAND, 2005) para garantir que um determinado equipamento médico é seguro. Nesta ISO, não é especificado, por exemplo, qual o método de avaliação de risco que deve ser utilizado, quais sãos os riscos ou seus níveis, porém é de responsabilidade do fabricante garantir que a análise de risco seja realizada e que os riscos resultantes estejam em níveis de perigo aceitáveis e, por fim, manter o registro do método de avaliação e dos níveis de perigo utilizados (HUFFMAN; BOWMAN; AKERS, 2013).

A fase inicial de implantação da ISO é denominada plano de gerenciamento de risco. É nesta fase onde acontece o planejamento de todas as atividades necessárias para realizar o processo de gerenciamento de risco. Nessa fase destacam-se, a definição do escopo das atividades, atribuição de responsabilidade e autoridades e os critérios para aceitação do risco (ABNT - ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2009).

O gerenciamento de risco é um processo fundamental para garantir a segurança do equipamento e é utilizado para identificar os riscos associados aos dispositivos médicos, para estimar e avaliar os riscos identificados, para controlar esses riscos e para monitorar a eficácia desse controle (HEGDE, 2011). As quatro etapas que o compõe o GR são caracterizadas por:

[1] <http://standards.ieee.org/findstds/standard/802.15.1-2005.html>

Análise de risco: Nesta etapa são identificados o propósito do equipamento e a intenção do uso, assim como os perigos, situações perigosas e a estimativa do risco associado a cada perigo;

Avaliação de risco: Para cada situação perigosa identificada, o fabricante deve decidir, utilizando o critério definido no plano de gerenciamento de risco, se a redução de risco é necessária ou não (ABNT - ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2009).

Controle de risco: Caso a redução do risco seja necessária, então serão tomadas as decisões que farão com que o risco seja reduzido a um nível aceitável;

Informações Pós-produção: Processo de análise da informação obtida sobre o dispositivo médico na fase de pós produção;

2.2.1 Técnicas

Tratando-se de sistemas de segurança crítica é imprescindível realizar a descoberta dos riscos e suas causas (JAIN et al., 2010), por isso, utiliza-se técnicas de análise de segurança para melhor identificar, analisar e definir o que se deve fazer mediante as falhas. Na *ISO* 14971 (ABNT - ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2009) são citadas três técnicas, a saber: a análise da árvore de falha (*Fault Tree Analysis*, *FTA*), o estudo de operabilidade e riscos (*Hazard and Operability Study*, *HAZOP*) e o método de Análise de Criticidade e Modo de Efeito de Falhas (*Failure Mode Effects and Criticality Analysis*, *FMECA*).

A seguir é detalhada cada técnica de análise de segurança, demonstrando como o uso da mesma permite a melhor compreensão dos perigos envolvidos e, assim, possibilitando tomadas de decisões para resolver ou evitar tais perigos. A primeira técnica é a análise da árvore de falha (*FTA*), Seção 2.2.1.1. Depois será detalhada análise de falha e efeitos *FMECA*, Seção 2.2.1.2 e, por fim, o método de estudo de operabilidade e riscos (*HAZOP*) é discutido na Seção 2.2.1.3.

2.2.1.1 FTA - Análise de árvore de falha

A análise da árvore de falha foi originalmente desenvolvido em *1962* no Bell Laboratories por *HA Watson*, para atender a necessidade da Divisão de Sistemas Balisticos da Força Aérea Americana em avaliar o sistema de controle de lançamento denominado *Minuteman I Intercontinental Ballistic Missile (ICBM)* (JAVADI; NOBAKHT; MESKARBASHEE, SEPTEMBER 2011). O uso de árvores de falhas, desde então, ganhou apoio generalizado e é frequentemente utilizado como uma ferramenta de análise de falhas por especialistas de confiabilidade (JAVADI; NOBAKHT; MESKARBASHEE, SEPTEMBER 2011).

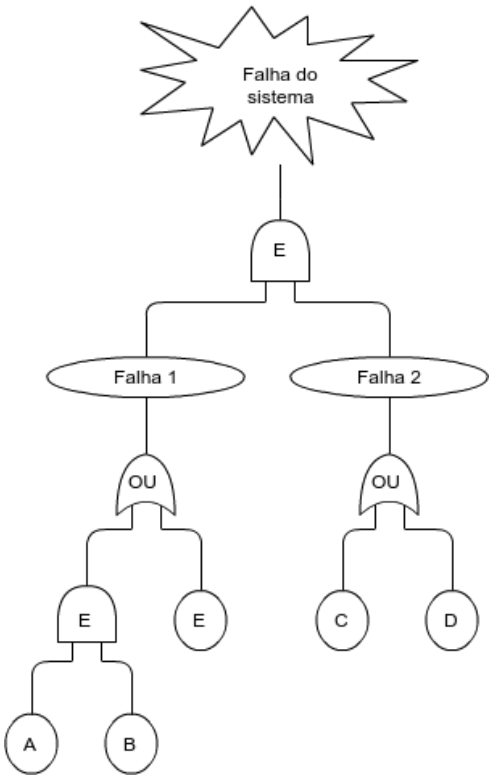
A análise da árvore de falha é utilizada para a identificação e análise das condições e fatores que causam ou podem potencialmente causar ou contribuir para a ocorrência de um denominado evento de topo (INTERNATIONAL ELECTROTECHNICAL COMMISSION, 2006). O evento de topo é um comportamento indesejado, uma situação perigosa. Assim, partindo desse evento de topo, de uma forma dedutiva, analisa-se as possíveis causas ou modos de falha do próximo nível inferior do sistema funcional que levaram com que o evento de topo ocorresse. Desta forma, de acordo com essa análise, a consequência indesejada é identificada (ABNT - ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2009). É uma análise *Top-Down* executada de forma dedutiva, onde o nível superior é a consequência e o nível inferior é a causa. Ao final do processo, o evento básico (a causa da falha) é encontrado (MAHMUD; WALKER; PAPADOPOULOS, 2011). O evento básico é o defeito que não depende de nenhuma outra causa. Os resultados são representados graficamente na forma de uma árvore de modos de falha. Em cada nível, na árvore, as combinações de modos de defeitos são descritas com operadores lógicos (***e*** *e* ***ou***) (KAISER; LIGGESMEYER; MäCKEL, 2003).

- A porta "ou" indica que pelo menos um evento de nível inferior é causa de um evento de nível superior (KAISER; LIGGESMEYER; MäCKEL, 2003).
- A porta "e" indica que todos os eventos de nível inferior são simultaneamente causas de um evento de nível superior (KAISER; LIGGESMEYER; MäCKEL, 2003).

É ilustrado na Figura 5 um exemplo de árvore de falha onde a falha do sistema (*Falha do Sistema*) é o evento de topo e é originado pela *Falha 1*) e falha *Falha 2*. Onde, por sua vez, a *Falha 2* é a consequência do evento C ou D. Estes eventos, assim como, A, B, C e D são denominado eventos básicos.

Árvore de falha é uma técnica de análise de segurança eficaz, porém na proporção em que a árvore cresce a demanda computacional para criar a representação da árvore também aumenta, o que torna o processo computacionalmente custoso. Esta característica torna difícil a verificação de árvore de falhas quando estas árvores são muito grandes. Outro ponto negativo é que a construção da árvore é um processo lento e repetitivo. Para a construção de uma *FTA* é necessário um profundo conhecimento do comportamento e dos componentes do dispositivo médico que está sendo construído, pois o método dedutivo que se baseia em encontrar os perigos a partir da situação perigosa não é intuitivo.

Figura 5 – Exemplo de aplicação do FTA



Fonte: Elaborada pelo autor

2.2.1.2 FMECA - Análise dos Modos de Falha Efeitos e Criticidade

A *FMECA* (Análise dos Modos de Falha Efeitos e Criticidade) foi desenvolvida pelo exército dos Estados Unidos, consiste em uma técnica de avaliação da confiabilidade para determinar o efeito das falhas do sistema e dos equipamentos. As falhas encontradas são classificados de acordo com seu impacto sobre o sucesso da missão e a segurança do pessoal e dos equipamentos (US DEPARTMENT OF DEFENSE, 24 november 1980). Consiste em uma análise sistemática onde as consequências de um modo de falha (condição na qual o sistema pode apresentar uma falha) são identificadas e avaliadas separadamente, na maioria dos casos, analisando uma única condição de falha por vez (ABNT - ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2009). É uma técnica semelhante ao *HAZOP* e baseia-se em montar uma equipe de especialistas e elaborar perguntas que irão auxiliar na detecção dos defeitos como, por exemplo, "O que acontece com a saída se .....?". Ao contrário do *FTA*, que é uma abordagem dedutiva, *FMECA* é uma abordagem indutiva ou *bottom-up* (ABNT - ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2009), nesta abordagem o passo inicial é encontrar a causa, e a partir da causa encontrar a falha (efeito).

A *FMECA* é um procedimento de análise que documenta todas as falhas prováveis em um sistema, determina por meio de análise o efeito de cada falha no funcionamento do sistema, identifica os pontos únicos de falha, e classifica cada falha de acordo com

a classificação da gravidade do efeito de falha (US DEPARTMENT OF DEFENSE, 24 november 1980). É uma abordagem semi-quantitativa realizada através da análise de criticidade e hierarquização do risco, utilizando o Número Prioritário de Risco (RPN) ou também denominado de Índice de Risco - IR (TEIXEIRA, 2009).

O *RPN* é calculado através do produto da *Severidade* (S), *Ocorrência* (O) e *Detecção* (D). A severidade permite avaliar a gravidade dos efeitos causados por um modo de falha sobre o sistema em análise. A *Ocorrência* representa a frequência ou a probabilidade de ocorrência de cada modo de falha. A *Detecção* representa a probabilidade de que o sistema atual não possa detectar o modo de falha ou causa (ZHAO; BAI, 2010). Um exemplo com os valores de severidade, ocorrência e detecção podem ser vistos nas tabelas 3, 4 e 5.

Tabela 3 – Tabela da Severidade

Severidade	Valor
Catastrófico	5
Crítico	4
Sério	3
Pequeno	2
Desprezível	1

Fonte: Elaborada pelo autor

Tabela 4 – Tabela da Ocorrência

Frequência	Valor
Improvável de acontecer	1
Remoto	2
Ocasional	3
Provável	4
Frequente	5

Fonte: Elaborada pelo autor

Tabela 5 – Tabela da Detecção

Detecção	Valor
Muito alta	1
Alta	2
Media	3
Baixa	4
Muito baixa	5

Fonte: Elaborada pelo autor

A equipe de especialistas deve discutir analisando, para cada falha, as potencias causas, seus potenciais efeitos, as formas de controle, a probabilidade da ocorrência e a severidade.

2.2.1.3 HAZOP - Estudo de operabilidade e riscos

O *HAZOP* foi desenvolvido em *1963*, na *Imperial Chemical Industries*, para análise de processos químicos. O conceito de um estudo*HAZOP* apareceu pela primeira vez com o objetivo de identificar possíveis riscos presentes em instalações que administram materiais altamente perigosos (DUNJÓ et al., 2010). O objetivo era eliminar qualquer fonte que levasse a ocorrência de acidentes graves, tais como emissões tóxicas, explosões e incêndios.

O *HAZOP* é uma técnica caracterizada por ser dedutiva e indutiva. A análise da falha tem início segundo a abordagem dedutiva analisando as consequências das falhas e por conseguinte encontrar as causas (HOEPFFNER, 1989) e utiliza a abordagem indutiva para detectar os comportamentos inesperados do sistema. Caracteriza-se, portanto, como um método *top-down* e *bottom-up* (DUNJÓ et al., 2010). O HAZOP é utilizado para estudar não apenas os perigos de um sistema, mas também os seus problemas de operabilidade, explorando os efeitos de quaisquer desvios de projeto (DUNJÓ et al., 2010). Para executar a análise do perigo, por intermédio desta técnica, deve-se montar uma equipe que possua conhecimento sobre o dispositivo médico que será construído e, em seguida, realizar um debate para avaliar os riscos do processo e os resultados de seus estudos devem ser reorganizados e descritos no formato de um relatório (KANG; YOON; SUH, 2001). O debate consiste em definir e utilizar as palavras guias (eg., sem, mais, menos, nenhum, maior, menor) combinado com os parâmetros do processo (e.g., temperatura,fluxo, pressão), que visam revelar desvios no projeto como, por exemplo, menor fluxo, maior temperatura e nenhuma pressão. Tendo determinado os desvios, a equipe de peritos explora suas possíveis causas e consequências (DUNJÓ et al., 2010). Um exemplo da planilha do *HAZOP* pode ser analisado na Figura 6.

Figura 6 – Exemplo de aplicação do *HAZOP*

Parametros / Palavra Guia	Mais	Menos	Nenhum	Reverter	Assim como	Parte de	Além de
Pressão	Pressão alta	Pressão baixa	Vácuo		Delta-P		Explosão
Temperatura	Temperatura Alta	Tempeatura Baixa					
Nível	Nível alto	Nível Baixo	Nenhum Nível		Nível direfente		
Tempo	Muito longo /Muito demorado	Muito curto/ Muito cedo	Passo sequencial ignorado	Retroagindo	Esquecendo passos	Ações extras	tempo errado
Reação	Reação rápida	Reação lenta	Sem reação				Reação inesperada
Inicializa/ Desliga	Muito rápido	Muito lento			Ações esquecidas		Fórmula errada
Manutenção			Nenhum				
Vibrações	Muito baixa	Muito alta	Nenhuma				Frequência errada

Fonte: Elaborada pelo autor

2.3 Redes de Petri Coloridas

2.3.1 Rede de Petri

Redes de Petri *(RP)* é um formalismo matemático, e que possuí uma representação gráfica utilizado para especificar sistemas concorrentes. Possui um conjunto de elementos para modelar as diversas características de um sistema computacional, tais como assincronicidade, distributividade e concorrência (MURATA, 1989).

A *RP* é graficamente representada por um grafo bipartido que possui os elementos definidos por lugares, transições e arco (CHEN et al., 2012). Os lugares são componentes passivos que representam as variáveis de estado do sistema. As transições, por outro lado, são elementos ativos, representam ações que podem ocorrer e modificar o estado do sistema. Os arcos são os componentes utilizados para fazer a ligação entre os lugares e as transições.

Ao modelar um sistema através de *RPC* o objetivo é representar os estados antes e depois de cada evento neste sistema. O elemento responsável por indicar qual o estado de uma Redes de Petri é o Token (ficha). É, portanto, de acordo com a transição da ficha através dos componentes que a Redes de Petri é executada (GIRAULT; VALK, 2001).

A *RP* adotada é uma Redes de Petri hierárquica de alto-nível denominada de Redes de Petri Coloridas (RPC). Com a utilização de hierárquia é possível criar vários níveis de abstrações através do uso das superpáginas e subpáginas. A superpágina caracteriza-se por ser a página de maior abstração, por outro lado, a subpágina é o detalhamento de uma superpágina, de forma a esclarecer alguns detalhes omitidos na representação em alto nível. Uma vantagem do uso de Redes de Petri hierárquica é que as subpáginas podem ser reusadas, além de facilitar no entendimento do modelo. Com as Redes de Petri Hierarquica é possível construir modelos mais compactos. A *RPC* é melhor detalhada na seção 2.3.2.

2.3.2 Redes de Petri Coloridas

RPC é uma técnica de especificação formal largamente difundida e adequada para modelagem de sistemas com atividades paralelas, concorrentes, assíncronas e não determinísticas (JENSEN, 2009). É a combinação da modelagem utilizando Redes de Petri com a linguagem Standard ML (JENSEN, 2009). A linguagem Standard ML fornece as primitivas para a definição de tipos de dados o que permite a manipulação dos dados e a construção de modelos compactos e parametrizáveis.

Na RPC, diferentemente da *RPC* de baixo nível, é permitido que a ficha possua tipos de dados diferentes (cores), e assim, distinguir os diferentes tipos de fichas (JENSEN, 2009). As cores não significam apenas padrões, podem representar tipos de dados complexos, usando a nomenclatura de cores apenas para referenciar a possibilidade de distinção entre as fichas (HUBER; JENSEN; SHAPIRO, 1991).

Um modelo em RPC de um sistema é, essencialmente, um modelo executável representado pela transferência das fichas pelos lugares e transições. Nas transições habilitadas o token é transferido para o lugar apenas após obedecer a uma condição de disparo. São nestas transições que o valor da ficha pode ser alterado. O lugar é um elemento passivo e define o estado do sistema. Cada lugar pode possuir um ou mais fichas e cada ficha possui um valor atribuído. A este valor atribuído dar-se o nome de *token colours* ou *cores do token* (JENSEN, 2009). É baseado na quantidade de tokens e as cores do token em um lugar específico que define o estado do sistema ou marcação da RPC (JENSEN, 2009). Segundo (AMMAR; NIKZADEH; DUGAN, 1997) uma RPC é composta por:

- Lugares (representado por elipses) : são locais que irão manter dados.
- Transição (representada por retângulos) : atividades que transformam o dado.
- Arcos (representado por setas) : ligam os lugares com as transições especificando o fluxo de dados. Podem conter inscrições onde, a inscrição em arcos de entrada especifica o dado que deve existir para que uma determinada atividade ocorra. As inscrições no arco de saída específicam os dados que serão produzidos se ocorrer uma determinada atividade. Guardas ou condição de guarda definem as condições que devem ser verdadeiras para que uma determinada ação ocorra.

As *RPC* são compostas por três partes :

Estrutura : A estrutura é formada por lugares, transições e arcos direcionados, de maneira semelhante à definida em *RP* de baixo nível;

Declarações : As declarações definem os conjuntos de cores, variáveis e operações usadas nas inscrições;

Inscrições : As inscrições por sua vez podem ser de quatro tipos: cores dos lugares, guardas, expressões dos arcos e inicializações.

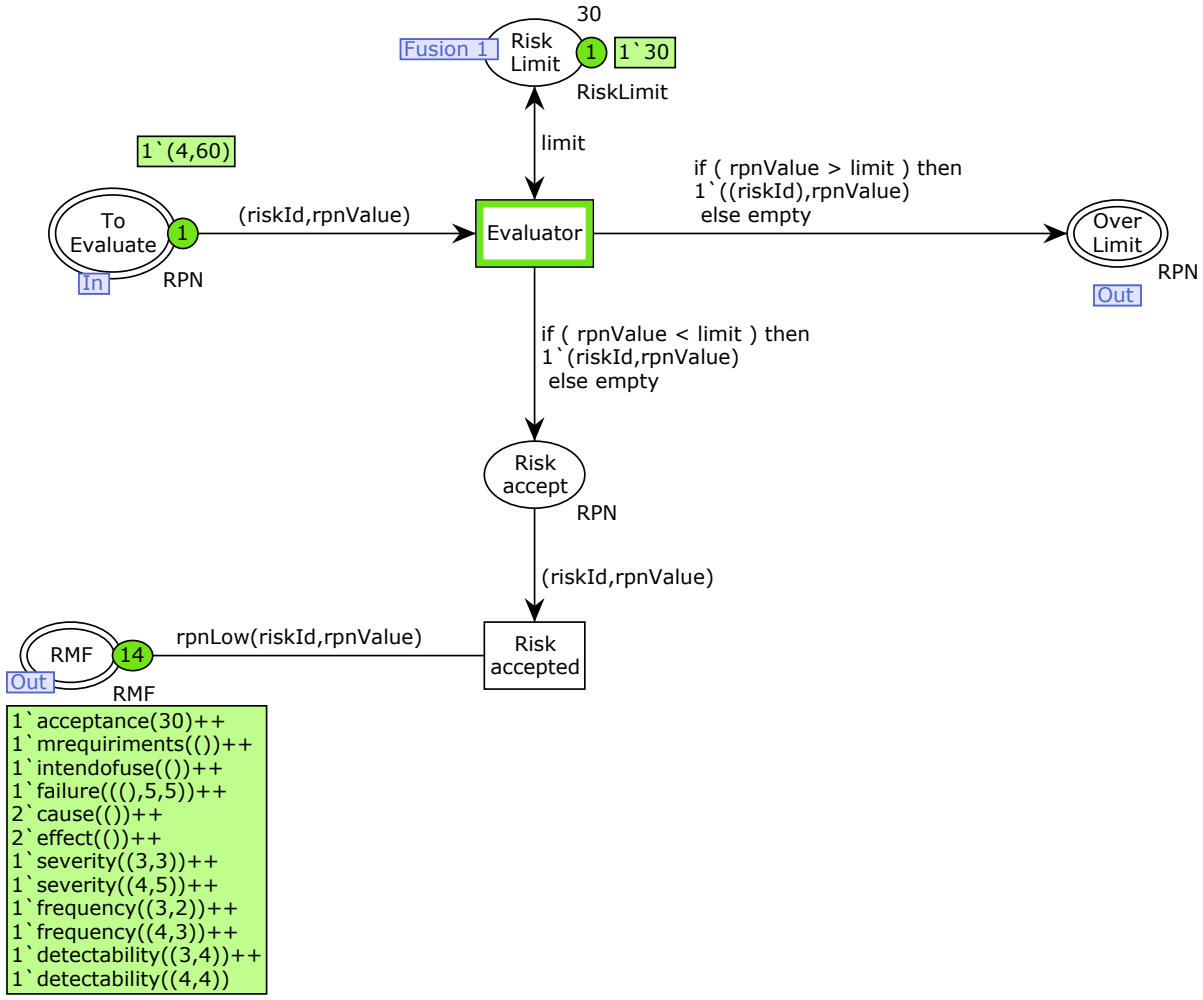
A vantagem da RPC é que esta permite o uso de *token color* e, com isso, é possível construir o modelo de grandes projetos de forma mais compacta. Redes de Petri Coloridas Hierárquica *RPCH* permitem construir um modelo maior a partir de um conjunto de *RP* menores denominados páginas ou sub-redes. As sub-redes são ilustradas através das caixas retangulares com linhas duplas como borda, denominada, transição de substituição (JENSEN, 2009). Para cada transição de substituição existe uma sub-rede (subpágina) associada e os lugares de entrada de cada transição de substituição são denominados *socket* de entrada e a saída *socket* de saída. Com a *RPCH* é possível transmitir fichas de uma sub-rede para outra utilizando lugares de fusão. Os lugares de fusão compartilham da mesma marcação e tudo que acontecer para o lugar pertencente ao mesmo conjunto de lugares de fusão, acontecerão a todos os outros lugares. Isto quer dizer que

todas as instancias dos lugares contidos no mesmo conjunto de fusão sempre irão apresentar a mesma marcação, o mesmo conjunto de cores e a mesma marcação inicial(JENSEN, 2009). Com isso, por intermédio de lugares de fusão a ficha pode ser levada de um lugar para outro estando este outro lugar na mesma sub-rede ou não.

É ilustrado na Figura 7, um exemplo de uma RPC contendo cinco lugares *(To Evaluate, Risk Limit, Over Limit, Risk accept e RMF)*, duas transição e seis arcos com inscrições. O lugar *To Evaluate* representa um *socket* de entrada da RPC que possui o *colorset* do tipo *RPN* e possui uma ficha com os valores (4,60) que representam respectivamente os valores de identificação do risco e o valor do RPN. A transição *Evaluator* está habilitada e a ficha pode ser enviada para o *socket* de saída *Over Limit* ou para o lugar denominado *Risk accept*. Como a transição *Evaluator* está habilitada e os lugares de entrada e saída são do tipo correto então a ficha pode ser enviado da transição *Evaluator* para o lugar *Over Limit* ou *Risk accept*. Porém os arcos que conectam essa transição aos lugares possuem em suas inscrições uma condição do tipo *if-then-else*, se o valor do RPN (*rpnValue*) for maior do que o valor limite (*limit*) a ficha será enviada para o *socket* de saída, caso o valor do RPN (*rpnValue*) seja menor do que o valor limite (*limit*) a ficha será enviada para o lugar denominado *Risk accept*. O lugar denominado *Risk Limit* é um lugar de fusão e está associado a outro lugar, com o mesmo nome, da sub-rede *Risk Managment Plan* (maiores informações sobre o plano de gerenciamento de risco são relatadas em 4.2.1). A execução da RPC nesta sub-rede termina quando a ficha é enviada para um dos dois *socket* de saída denominados (*RMF* e *Over Limit*). Informações mais detalhadas sobre esta sub-rede são apresentadas na Seção 4.2.3.

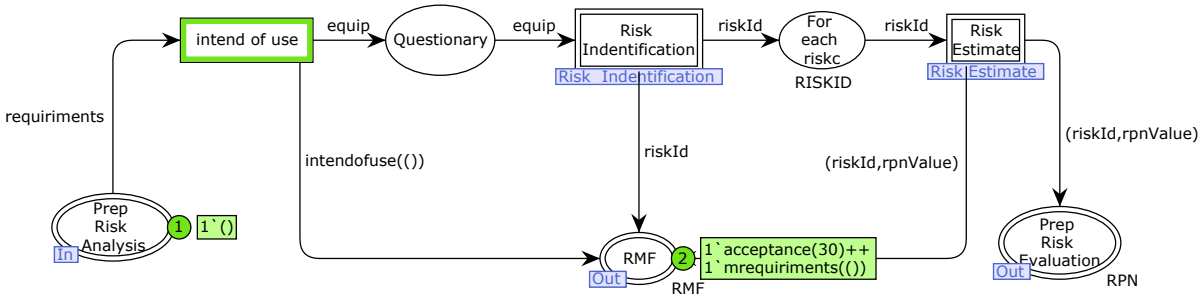
Um outro exemplo sobre RPC pode ser visto na Figura 8, neste exemplo, a sub-rede possui cinco lugares (Prep Risk Analysis, Questionary, For each risk, Prep Risk Evaluation e RMF), duas transições (*Risk Indentification* e *Risk Estimate*) e nove arcos com inscrições. Neste exemplo destaca-se que a sub-rede ilustrada é ao mesmo tempo uma sub-rede e uma superpágina, pois, possui duas transições de substituição (*Risk Indentification* e *Risk Estimate*). Estas transições de substituição, por sua vez, possuem sub-redes associadas e podem ser vistas nas Seções 4.2.2.1 (*Risk Indentification*) e 4.2.2.2 (*Risk Estimate*). Mais informações sobre a sub-rede ilustrada na Figura 8 pode ser vista na Seção 4.2.2.

Figura 7 – Avaliação de risco



Fonte: Elaborada pelo autor

Figura 8 – Análise de risco (Risk Analysis)



Fonte: Elaborada pelo autor

A RPC é matematicamente definida por um tupla rdPc = (P, T, A, $\sum$, V, C, G, E, I), em que:

- P - é um conjunto finito de lugares;
- T - é um conjunto finito de transições, onde $P \cap T = 0$;
- A - é um conjunto dos arcos direcionados, onde $A \subseteq P$ X $T \cup T$ X P;
- $\sum$ - é um conjunto finito não-vazio de cores;
- V - é o conjunto finito das variáveis tipadas, tais que Tipo[v] $\in \sum$ para todo v $\in V$;
- C: $P \rightarrow \sum$ - é uma função que associa um tipo de cor definido em $\sum$ a cada lugar de P, ou seja.
- G:$T \rightarrow$ EXPRv, onde Tipo[$G(t)$]=bool - é uma função, denominada expressão de guarda, que associa uma guarda para cada transição t a uma resposta booleana (verdadeiro ou falso), ou seja.
- E:$A \rightarrow$ EXPRv - é uma função, chamada expressão de arco, que associa uma expressão a cada arco de a, onde o Tipo[E(a)] = C(p)$_{MS}$
- I - é uma função, chamada inicialização, que associa uma expressão de inicialização a cada lugar p, onde Tipo[I(p)] = C(p)$_{MS}$

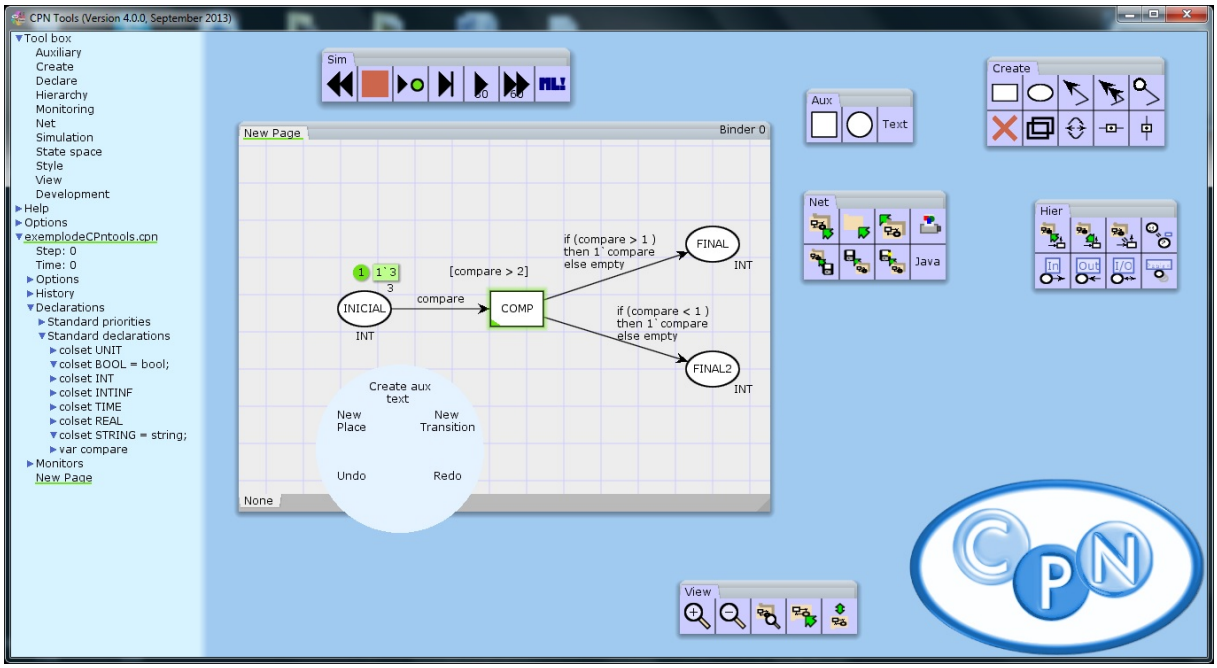
2.3.2.1 CPN/Tools

CPN/Tools é uma ferramenta gráfica utilizada para editar, simular e analisar RPC. Oferece um ambiente integrado para a especificação (por meio de edição gráfica), simulação e verificação dos modelos RPC (BRITO; BARROS, 2013). A interface gráfica do usuário (GUI) do CPN/Tools não tem barras de menu convencional e menus suspensos, mas é baseado em técnicas de interações, como paletas de ferramentas (*tool palettes*) e menus de marcação *marking menus* (JENSEN; KRISTENSEN; WELLS, 2007).

Os principais desenvolvedores dessa ferramenta foram *Kurt Jensen, Søren Christensen, Lars M. Kristensen, e Michael Westergaard.* A partir do outono de 2010, a ferramenta foi transferida para o grupo AIS, Eindhoven University of Technology, na Holanda que é a responsável por manter o projeto (WESTERGAARD; VERBEEK, 2014).

Um exemplo do uso do CPN/Tools é ilustrado na Figura 9 . Nesta figura é possível perceber, no canto esquerdo, as paletas onde estão contidas as ferramentas para a edição e manipulação da RPC. Já um exemplo do menu de marcação pode ser percebido pela sua forma circular com as funcionalidades de ("Refazer", "Desfazer","Novo Lugar", "No Estado","Criar auxiliar").

Figura 9 – Utilização da CPN/Tools



Fonte: Elaborada pelo autor

2.3.2.2 Validação e verificação

Através do uso da *CPN/Tools* é possível analisar o comportamento do modelo construído utilizando a validação e verificação. Ao fazer simulações do modelo RPC, é possível investigar diferentes cenários. A simulação pode ser realizada de duas formas distintas, modo interativo ou automático. O modo interativo é similar a uma depuração passo-a-passo de um software, investigando diferentes cenários e se o modelo está funcionando como o esperado. Durante uma simulação interativa, o modelador está no comando e determina o próximo passo, selecionando dentre os eventos ativos no estado atual. Já a simulação automática é semelhante a um programa em execução. O objetivo é simular o modelo tão rápido quanto possível e é tipicamente utilizado para o teste e análise de desempenho. Para fins de teste, o modelador normalmente configura pontos de parada adequados e critérios de parada e analisa a cada parada se o comportamento do sistema é o esperado (JENSEN; KRISTENSEN; WELLS, 2007).

Neste trabalho a verificação do modelo é realizada de forma automática utilizando a geração de espaço de estados e verificação de modelos (model checking) (CLARKE JR.; GRUMBERG; PELED, 1999). O conceito principal relacionado a essa verificação é a geração do conjunto de todos os estados alcançáveis bem como as mudanças de estado e representá-los como um grafo direcionado, onde os nós representam os estados e os arcos representam os eventos que ocorrem (JENSEN; KRISTENSEN; WELLS, 2007). Com isso, torna-se possível verificar se o modelo foi construído conforme as especificações, descobrindo possíveis erros e aumentando a confiança na corretude do modelo (JENSEN,

2009).

A principal desvantagem da geração do espaço de estados é o problema da explosão de espaço de estados: mesmo sistemas relativamente pequenos podem apresentar um número elevado de estados alcançáveis e analisar cada um desses espaços é computacionalmente custoso podendo facilmente esgotar os recursos de memória de uma máquina. Contudo, técnicas de redução podem adiar a chance de ocorrer a explosão de espaço de estados. Técnicas como redução de ordem parcial, Ordered Binary Decision Diagrams e Interpretação abstrata (RODRIGUES, 2004) são alguns exemplos.

3 ESTUDO DE CASO

Neste capítulo será descrito como realizar o processo de gerenciamento de risco em um equipamento de EGG baseado na ISO 14971 e na técnica FMECA. Este estudo de caso teve como objetivo aprimorar o entendimento da ISO e FMECA para a construção do modelo em *RPC*. Trata-se de uma especificação pré-mercado, tendo em vista que o equipamento médico construído não tem como objetivo primário a comercialização, mas um protótipo de equipamento médico de baixo custo e baixo consumo energético.

3.1 Descrição dos passos

Este estudo de caso foi divido nos seguintes passos: definição do equipamento; classificação segundo a *Anvisa* e gerenciamento do risco. A pesquisa direta ocorreu no período de 16 de janeiro de 2014 a 29 de julho de 2014, com um especialista em desenvolvimento de sistemas de aquisição de sinais biomédicos no Hospital Universitário da Universidade Federal de Alagoas.

A fase inicial consistiu em sucessivas entrevistas com o especialista buscando identificar o propósito do uso e os materiais a serem utlizados para a fabricação do EGG, dando assim, inicio ao plano de gerenciamento do risco. Após a conclusão do referido plano, foi iniciado o processo de gerenciamento do risco.

3.1.1 Plano de gerenciamento de risco

O gerenciamento de risco, teve início no dia 23 de janeiro de 2014 e, devido ao pequeno número de integrantes na equipe envolvida com a fabricação do equipamento, não foi necessária a *alocação das responsabilidades*. Por isso a primeira atividade do *plano de gerenciamento de risco* foi a *descrição do equipamento que será fabricado*. Nessa etapa foi registrado que o dispositivo a ser fabricado seria um equipamento de Eletrogastrografia usado para fazer o acompanhamento dos impulsos mioelétricos da musculatura lisa do estômago. Foi definido que o equipamento seria de baixo custo e baixo consumo de energia, composto basicamente por três eletrodos, cabos de blindagem (sensoriamento), um circuito integrado para realizar o condicionamento do sinal, a conversão Analógico/Digital (A/D) e a transmissão dos dados com um software embacardo e eletricamente alimentado por um uma bateria de nove volts (9V).

Após a descrição do dispositivo foi estabelecido o *critério para a aceitação dos riscos*. Esse critério foi estabelecido tendo como base os valores definidos para severidade, ocorrência e detecção, previamente explicado na Seção 2.2.1.2 e detalhado nas Tabelas 9, 10, 11. A partir desses valores, foi definido que o limite máximo de aceitação do risco seria

20%, totalizando (25) dos 125 pontos que é o máximo que o RPN pode chegar. Dessa forma, o critério foi :

- Risco aceitável abaixo de 20% do total possível, ou seja RPN <= 25;
- Risco tolerável entre 21% e 25% do total possível, ou seja 25 < RPN < 31, desde que, após ter sido realizada análise de risco/benefício, os benefícios superem os riscos;
- Risco intolerável acima de 25%, ou seja RPN >= 31. Deve ser reduzido.

Sendo a segurança definida como requisito essencial para a fabricação do equipamento, as falhas encontradas só seriam toleradas quando fossem menores que o limite de aceitação, ou menor que 25%, desde que na análise de risco/benefício, os benefícios superassem e que os riscos residuais deveriam ser evitados atendendo, assim, a condição que a segurança deve ser inerente ao projeto.

3.1.1.1 Análise de risco

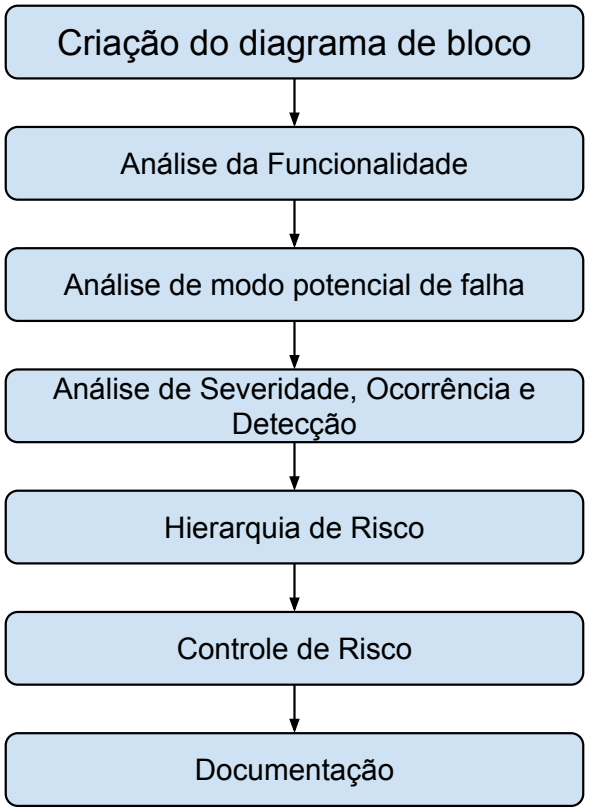
Durante a fase de análise de risco, as atividades iniciais tiveram o objetivo de melhorar o entendimento sobre o EGG e descobrir as situações perigosas. Por isso, foi realizado um *Brainstorm* com o especialista e participantes desta pesquisa cujo o objetivo foi melhor identificar qual o propósito do equipamento e como este deveria ser usado. Como um auxílio ao *Brainstorm* foi elaborado um questionário (ISO 14971:2009, Anexo C). Este questionário auxiliou na consolidação do entendimento sobre o propósito do uso do equipamento, bem como a forma correta do seu manuseio e conservação do equipamento e identificar novas situações de falhas que ainda não haviam sido percebidas.

Em seguida, foi prosseguida a aplicação da técnica FMECA. A aplicação foi dividida em etapas e baseada nos trabalhos (HERMAN; JANASAK, 2011; LUTHRA, 1991; KAWATHEKAR; MOORTHY; CHANDRAPPA, 2012; STANDARD, 24 NOVEMBER 1980). As etapas são ilustradas na Figura 10 e explicadas a seguir.

O passo **criação do diagrama de bloco**, consistiu em analisar o EGG como um sistema complexo composto de vários subsistemas. Foram identificados sete (7) subsistemas : **Sensoriamento, Amplificador de instrumentação, Amplificador operacional, Microcontrolador, Bluetooth, Bateria, Software**. O diagrama de bloco pode ser visto na Figura 11. Em seguida, foi realizada a análise das funcionalidades de cada um destes subsistemas. Os sete subsistemas e suas respectivas funcionalidades podem ser vistos na Tabela 6.

Para cada subsistema identificado foram analisadas as funcionalidades, situação de falha *(modo potencial de falha)* e as conseqências de tais falhas. Mediante esse estudo foram identificadas 19 (dezenove) falhas, todas as falhas e seus respectivos modos potenciais de falha e efeitos foram registrados na planilha FMECA e no RMF. Um exemplo das falhas encontradas pode ser visto na Tabela 7. As 19 falhas podem ser vistas no Apêndice.

Figura 10 – Fluxograma FMECA



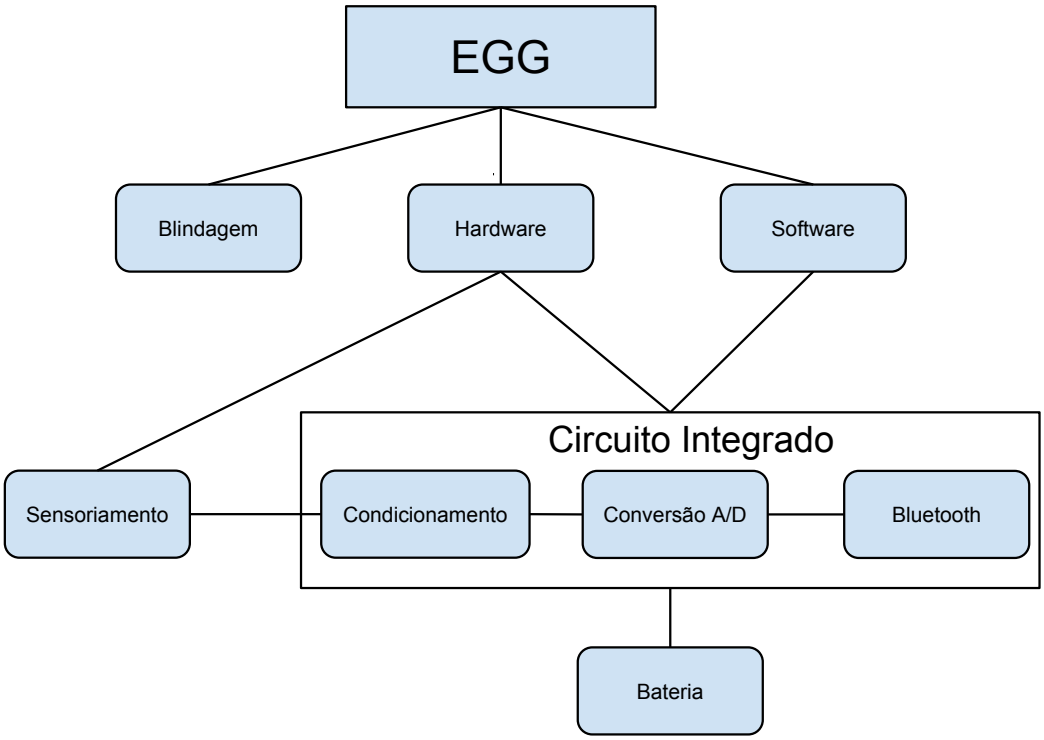
Fonte: Elaborada pelo autor

Tabela 6 – Tabela dos subsistemas e suas respectivas funções

Subsistemas	**Funções**
Sensoriamento	Registrar os impulsos mioelétricos do estômago
Amplificador de instrumentação	Converter o sinal de entrada de microvolt para volt
Amplificador operacional	amplificar a diferença entre dois sinais analógicos aplicados às suas entradas
Microcontrolador	Converter e condicionar o sinal analógico pra digital de 10 bits
Bluetooth	Enviar os dados do EGG
Bateira	Alimentação energética do equipamento
Software	Realizar o auto-teste, teste de bateria e impedância

Fonte: Elaborada pelo autor

Figura 11 – Diagrama de blocos do sistema EGG



Fonte: Elaborada pelo autor

Tabela 7 – Amostra dos resultados da tabela FMECA com as falhas encontradas

Componente	**Função**	**Modo Potencial de Falha**	**Efeitos potencias de falha**	**Causas potenciais/ Mecanismo de falha**
Microcontrolador	Converter o sinal analógico pra digital de 10 bits	Má conversão A/D	Perda da qualidade do sinal	Microcontrolador com defeito
Sensoriamento - Cabos de Blindagem	Conduzir os impulsos mioelétricos registrados pelo eletrodo até a etapa de condicionamento de sinal	Má qualidade dos cabos	Ruídos	Interferência Eletromagnética
Amplificador de instrumentação	Amplificar o sinal de microvolts para volts	Amplificador de instrumentação com defeito	Valores do sinal fora da faixa	Hardware mal construido pelo fabricante
Amplificador operacional	Amplificar a diferença entre dois sinais analógicos aplicados àss suas entradas.	Amplificador operacional com defeito	Valores do sinal fora da faixa	Hardware mal construido pelo fabricante
Bluetooth	Enviar os dados do EGG RN42	Problema no hardware do bluetooth	Erro na comunicação dos dados	Equipamento com defeito
Bluetooth	Enviar os dados do EGG RN42	Desvaneicimento e terminal oculto	Erro na comunicação dos dados	Barreiras fisicas ou distanciamento do equipamento
Bateria	Alimentação energética do equipamento	Baixa carga da bateria	Equipamento pode parar de funcionar	Falta de recarga do equipamento
Bateria	Alimentação energética do equipamento	Baixa carga da bateria	Erro na Leitura devido a baixa carga da bateria	Falta de recarga do equipamento
Sensoriamento - Eletrodo	Registrar os impulsos mioelétricos do estomago	Posicionamento errado do eletrodo	Leitura errada dos dados	Má capacitação do operador

Fonte: Elaborada pelo autor

Para classificar em níveis de prioridade as falhas encontradas, foi necessário relacionar cada falha aos valores de severidade, ocorrência e detecção. Todos os três componentes foram classificados de acordo com a escala de magnitude de 1 a 5 previamente explicada na Seção 2.2.1.2 e detalhada nas Tabelas 9, 10, 11.

Considerando que o EGG é um equipamento médico que tem por finalidade monitorar a frequência de propagação das contrações gástricas, foi definido que todos os riscos que interferissem na qualidade do sinal seriam considerados como severidade 5. Tendo em vista que na presença das interferências todo o monitoramento seria afetado, assim, todos os riscos foram classificados como severidade 5. Um exemplo da tabela contendo uma amostra dos riscos encontrados, valores dos componentes e do RPN pode ser visto na Tabela 8 e a tabela completa pode ser vista no Apêndice 31.

Tabela 8 – Amostra dos resultados da tabela FMECA com os riscos encontrados, valores dos componentes e RPN

Modo Potencial de falha	**Severidade**	**Ocorrência**	**Detecção**	**RPN**
Cabo com defeito	5	4	5	100
Interferencias externas	5	4	5	100
Impedância fora da faixa	5	3	3	45
Configuração errada do amplificador de instrumentação	5	3	2	30
Erro no teste da bateria	5	3	3	45
Má conversão A/D	5	1	1	5
Má qualidade dos cabos	5	2	1	10

Fonte: Elaborada pelo autor

Tabela 9 – Tabela da Severidade

Valor	**Severidade**	**Descrição**
1	Desprezível	Nenhuma perda do sinal
2	Pequeno	Pequenas interferências no sinal
3	Sério	interferências no sinal
4	Crítico	Grande perda no sinal
5	Catastrófico	Desconstrução total do sinal

Fonte: Elaborada pelo autor

Tabela 10 – Tabela da Ocorrência

Valor	Ocorrência	Descrição
1	Improvável	Probabilidade de ocorrência de falha Improvável (1 em 1500000 execuções)
2	Remota	Probablidade de ocorrência de falha muito baixa (1 em 15000 execuções)
3	Ocasional	Probabilidade de ocorrência de falha moderada (1 em 80 execuções)
4	Provável	Alta probabilidade da falha ocorrer (1 em 8 execuções)
5	Frequente	Muito alta probabilidade de ocorrência de falha (1 em 2 execuções)

Fonte: Elaborada pelo autor

Tabela 11 – Tabela da Detecção

Valor	Detecção	Descrição
1	Muito alta	O risco é fácil de ser identificado. Os métodos de verificação identificam o defeito
2	Alta	O risco pode ser identificado. Alta probabilidade dos métodos de verificação identificar o defeito
3	Média	Moderada probabilidade do risco ser identificado. Os métodos de verificação podem identificar
4	Baixa	Baixa probabilidade de identificar o risco. Os métodos de verificação provavelmente não irão identificar o risco
5	Muito baixa	Os métodos de verificação não irão identificar o risco

Fonte: Elaborada pelo autor

De posse desta classificação foi obtido o Número de Prioridade de Risco (RPN) mais elevado no subsistema *(Sensoriamento - Cabos de Blindagem)* para a falha (*Má isolamento elétricos sofrendo interferências externas e cabo de blindagem com defeito*) para estas falhas os valores de Severidade (5 - Catastrófico), Detecção (5 - Muito baixa), Ocorrência (4 - Provável) e RPN (100) foram idênticos. Os riscos que apresentam maiores valores de RPN possuem prioridade para serem trabalhados e com isso reduzidos.

Para ser considerado seguro, o equipamento médico deve apresentar apenas riscos que sejam considerados toleráveis, ou em situações especiais, possuir riscos acima do limite tolerável desde que os benefícios do uso superem esses riscos. A avaliação se o risco é tolerável ou se o controle do mesmo se faz necessário, é realizada na fase subsequente

denominada *Avaliação do risco*.

3.1.1.2 Avaliação de risco

Estabelecido durante a fase de *plano de gerenciamento de risco*, o limite de aceitação de risco é o ponto crucial na avaliação de risco. É baseado neste limite que se distingue se os riscos são aceitáveis ou não. Se os riscos forem acima do valor limite aceitável, então, dá-se início a uma nova fase, fase de controle de risco. Caso contrário, se os riscos forem abaixo do limite aceitável, para estes será necessário, apenas, registra-los no RMF.

Nesta fase apenas os riscos (*Microcontrolador- Má conversão A/D* e *Sensoriamento - Má qualidade dos cabos*) ficaram abaixo do limite definido, como ilustrado na Tabela 8, e foram registrados no RMF. Os demais riscos serão novamente referenciados na próxima fase, no controle dos riscos.

3.1.1.3 Controle do risco

O objetivo desta fase é, respeitando a ordem decrescente dos valores de RPN, analisar e adotar as melhores práticas que irão reduzir os riscos que possuem RPN maior do que o aceitável. Para isso, deve-se primeiro analisar quais são as origens do risco encontrado e o que pode ser feito para que este risco seja reduzido.

Todavia, ao adotar medidas corretivas com o intuitivo de reduzir o risco, novos riscos podem ser inseridos. Portanto, é necessário, após a adoção da medida corretiva, analisar a severidade, ocorrência e detecção desta medida a fim de certificar que o risco foi de fato reduzido e que nenhum risco novo foi inserido, caso contrario novas medidas de controle devem ser adotadas.

Na Tabela 12, onde é ilustrada um exemplo de três riscos e suas respectivas medidas de controle, é possível perceber que o risco *Posicionamento errado do eletrodo* possui o RPN de valor 45, maior que o limite aceitável. Esse risco deve ser reduzido de forma que os valores de Severidade (S - 5), Ocorrência (O - 3) e Detecção (D - 3), sejam reduzidos. Para isso, faz-se necessária a análise das causas pontências para constatar o que originou esta falha e, então, identificar uma medida de controle. Para este referenciado risco a medida de controle identificada foi *Capacitar o operador*. Após realizar a medida de controle os valores devem novamente ser analisados. Foi constatado que para este risco, dado que o operador foi capacitado a Ocorrência (O - 2) diminui, porém, o RPN continua acima do limite aceitável e dentro do limite tolerável, assim este risco precisa ser analisado segundo o princípio de risco/benefício na etapa de riscos residuais.

Tabela 12 – Amostra dos resultado da planilha FMECA com as falhas encotradas e as medidas de controle

Modo potencial de falha	S	O	D	RPN	Ações tomadas	S	O	D	RPN
Posicionamento errado do eletrodo	5	3	3	45	Capacitar o operador	5	2	3	30
Configuração errada do amplificador operacional	5	5	2	50	Revisão do projeto	5	2	3	30
Amplificador de instrumentação com defeito	5	3	2	30	Executar o teste do compontente	5	1	1	5

Fonte: Elaborada pelo autor

3.1.1.4 Avaliação de aceitabilidade do risco residual

Foram encontrados quatro riscos residuais que não puderam ser mitigados na fase de controle de risco, dois deles são ilustrados na Tabela 12 (*Posicionamento errado do eletrodo* e *Configuração errada do amplificador operacional*). Porém, por estarem dentro do limite razoável que varia de 20% a 25% do total dos 125 pontos possíveis e os benefícios destes superarem os riscos, foram tomados como aceitáveis, haja vista que, se tomadas as devidas providências de adequação do ambiente para realizar o exame, assim como o treinamento do operador, adotando sempre o uso de materiais novos, o risco é superado pelos benefícios, assumindo, assim, que estes riscos residuais são toleráveis.

4 MODELAGEM

Neste capítulo é apresentada de forma detalhada a modelagem formal do processo de gerenciamento de risco descrito na ISO 14971 e FMECA utilizando *RPC*. O modelo foi construído utilizando a ferramenta *CPN/Tools*. Essa ferramenta auxilia na construção de modelos baseados em RPC e permite a verificação e validação por intermédio das simulações, métodos de espaço de estado e *model checking* (JENSEN; KRISTENSEN; WELLS, 2007). Atualmente existem versões da CPN/Tools para Linux, Windows e Mac. Todas podem ser encontradas no endereço <*http:// cpntools.org/ download*>.

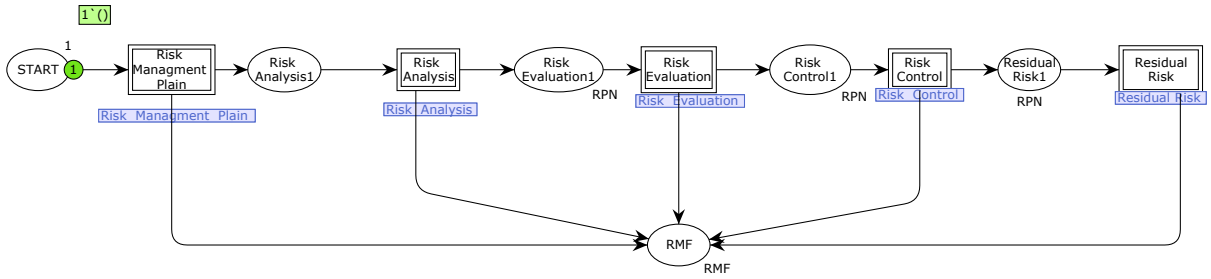
4.1 Descrição do problema

De acordo com (KORB et al., 2003; SIVAKUMAR et al., 2011), são essenciais para a concepção de equipamentos médicos seguros e confiáveis as etapas de verificação e validação destes equipamentos, a fim de que seja, previamente, possível constatar a pertinência de riscos. Contudo, muitas vezes, por não haver o claro entendimento da ISO 14971 e pela exigência imposta pelas agências regulamentadoras à adequação do processo de gerenciamento de risco a esta mesma ISO, muitas empresas acabam criando processos complexos aos quais não conseguem seguir (SCHMULAND, 2005). Pensando nisto, foi realizada a modelagem em *RPC* tendo como base o estudo de caso realizado bunscando, assim, reduzir a subjetividade encontrada na descrição em linguagem natural da ISO.

4.2 Modelagem Formal

A modelagem tem por finalidade representar o ciclo de desenvolvimento pré-mercado de um equipamento médico utilizando a ISO 14971. Foi desenvolvido um modelo hierárquico contendo cinco sub-módulos (*Risk Managment Plan*, *Risk Analysis*, *Risk Evaluation*, *Risk Control* e *Residual Risk*). Em todos os sub-módulos deve ser respeitado o requisito de registrar os dados no arquivo de gerenciamento de risco final (representado pelo lugar *RMF*). A rede de mais alto nível no modelo hierárquico é ilustrada na Figura 12. As próximas seções são descrições detalhadas de cada um dos sub-módulos (*Risk Managment Plan*, *Risk Analysis*, *Risk Evaluation*, *Risk Control* e *Residual Risk*), ilustrados nesta figura. Todas as variáveis utilizadas, assim como as funções criadas podem ser vistas no Apêndice A.1.

Figura 12 – Rede de mais alto nível no modelo hierárquico



Fonte: Elaborada pelo autor

4.2.1 Plano de gerenciamento de risco

A sub-rede *Risk Managment Plan* é ilustrada na Figura 13. Nessa fase se destaca a importância do planejamento inicial. Inicia com a etapa *planejamento*, modelada pela transição *planning*. Essa etapa consite na execução de três atividades, representadas por três lugares, definidas a seguir :

Allocation of responsabilities, tem a finalidade de alocar da melhor forma possível todos os recursos necessários para a fabricação do equipamento;

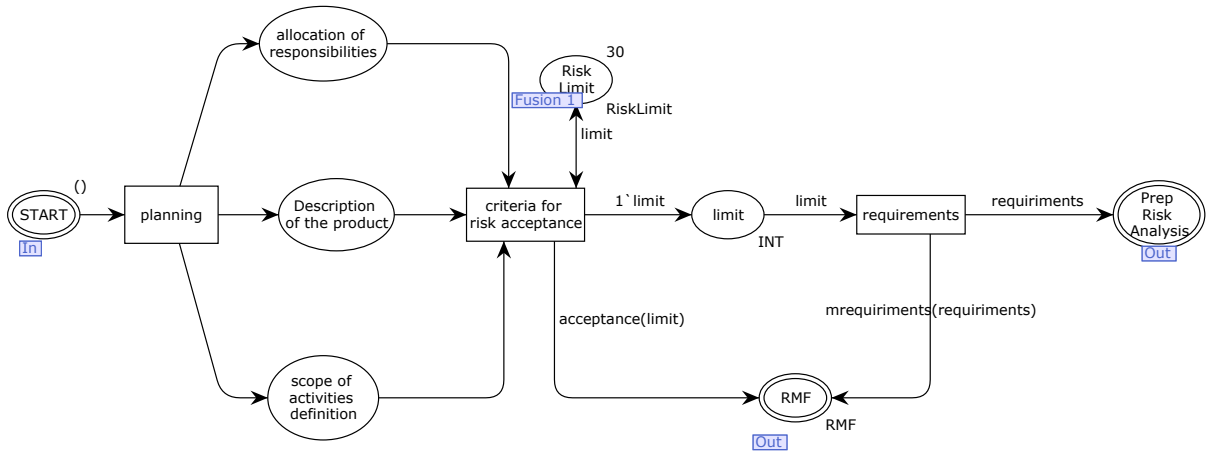
Description of the product, que tem por objetivo descrever de forma detalhada o que é o equipamento médico que está sendo construído;

Scope of activities definition, nessa atividade o resultado esperado é um plano com todas as atividades que serão necessárias para elaborar o equipamento médico.

Depois da finalização dessas atividades iniciais, representadas pela transição *planning* e pelos lugares *planejamento, alocação de responsabilidades, definição do escopo das atividades*, uma nova etapa no contexto do plano de gerenciamento de risco pode ser iniciada. Essa nova etapa é o critério para a aceitação dos riscos, representada pela transição *criteria for risk acceptance*.

O critério para aceitação do risco, representa o valor limite para distinguir quais riscos poderão ser assumidos como toleráveis e quais não poderão ser toleráveis, é representado pelo lugar *Risk Limit*. O valor limite para aceitação do risco deve ser registrado no arquivo de gerenciamento de risco, representado pelo lugar *RMF*. A etapa final do plano de gerenciamento de risco é denominada *requisito*, transição *requirements*, nessa etapa devem ser estipuladas as métricas mínimas de avaliação para os riscos considerados, a princípio, como não toleráveis, por exemplo, a comprovação através de um estudo clínico, a aprovação do especialista ou testes específicos. Assim como o limite de aceitação do risco, os requisitos devem ser registrados no RMF. Ao concluir essa etapa inicial os requisitos necessários para a criação do plano de gerenciamento de risco são finalizados. Dá-se, então, início a nova fase denominada *Analise do Risco*.

Figura 13 – Plano de gerenciamento de risco (Risk Managment Plan)



Fonte: Elaborada pelo autor

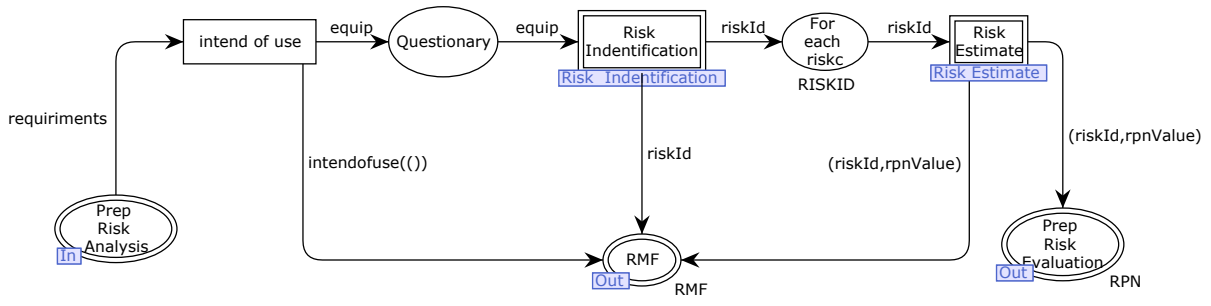
4.2.2 Análise do Risco

Na fase de *Análise do Risco*, conforme ilustrada na Figura 14, o objetivo é identificar todos os riscos que estão envolvidos com a fabricação do equipamento e avaliar qual o nível de severidade de cada risco.

A identificação dos riscos tem início a partir da definição sobre qual é o propósito de uso do equipamento médico. Perguntas simples como, "o que é o equipamento?", "Qual o propósito do uso?" e "Como o equipamento será usado?", ajudarão na identificação desse propósito. A identificação do risco é representado pela transição *intend of use* que recebe como entrada os requisitos definidos no plano de gerenciamento de risco e ao ser disparada dá início ao questionário. O propósito do uso é uma informação que deve ser mantida no arquivo de gerenciamento de risco, ilustrado pelo lugar *RMF*.

Em seguida, ainda com o intuito de descobrir os riscos, é aplicado o questionário que encontra-se no Apêndice C da ISO 14971:2009. Esse questionário é ilustrado pelo lugar *Questionary*. Ao responder o questionário o fabricante estará apto a iniciar a fase de *identificaçao dos Riscos*.

Figura 14 – Análise de risco (Risk Analysis)



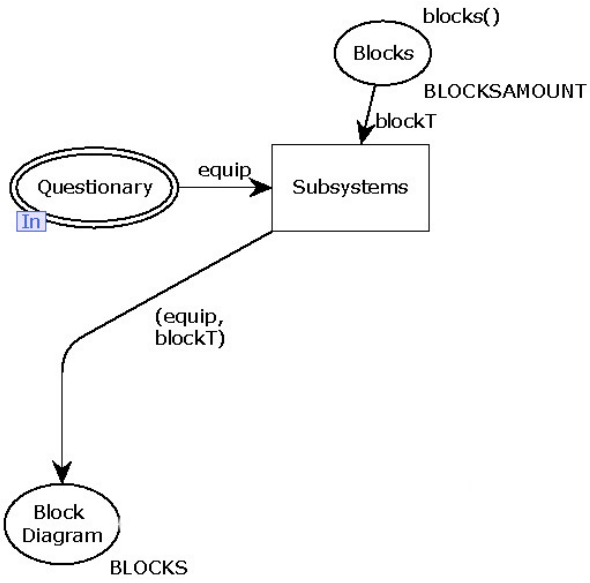
Fonte: Elaborada pelo autor

4.2.2.1 Identificação de riscos

A identificação de risco é uma fase longa no processo de gerenciamento de risco e é iniciada com a construção do diagrama de bloco onde, cada bloco representa um subsistema do equipamento médico.

Na Figura 15, é possível destacar que a transição *Subsystems* só será habilitada depois que as informações detalhadas do equipamento (resultado da aplicação do questionário, representada pelo lugar *Questionary*) for obtida, assim como a informação da quantidade de blocos que o equipamento é composto, ilustrada pelo lugar *Blocks*. A transição *Subsystems*, depois de habilitada, será disparada enviando a ficha para o lugar *Block Diagram* que possue o *colour set BLOCKS:UNITxINT* que representa a informação sobre o equipamento e a quantidae de blocos. Um exemplo do diagrama de blocos pode ser visto na Figura 11 no Capítulo 3.

Figura 15 – Construção do diagrama de bloco

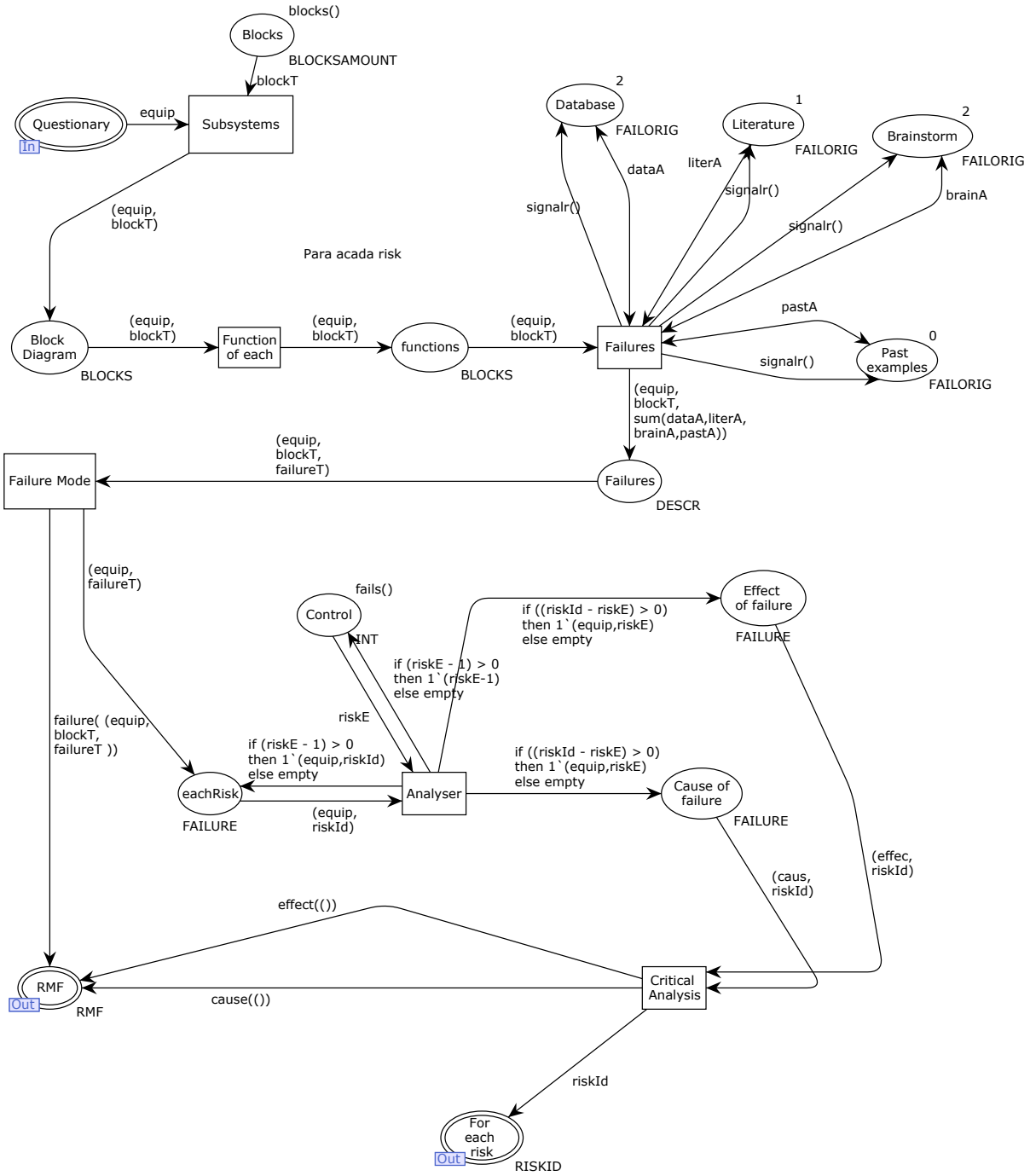


Fonte: Elaborada pelo autor

Em todo bloco identificado deve ser analisada a respectiva funcionalidade e quais são as possíveis falhas relacionadas a esse bloco. As possíveis falhas são informações que podem ser provenientes de diversificadas fontes tais como: banco de dados que contenha informações sobre falhas, literaturas sobre o equipamento médico, *brainstorm* com a equipe e principalmente experiências passadas. Essas informações são ilustradas no modelo pelos lugares *Database*, *Literature*, *Brainstorm*, *Past examples*. Após receber as informações sobre as possíveis falhas, a transição *Failures* pode ser disparada. O disparo desta transição acontece quando é obtida a informação sobre o equipamento, a quantidade total de blocos e todas as possíveis falhas. Para cada falha identificada é realizada uma análise crítica buscando entender o que ocasionou o surgimento dessa determinada falha e qual o efeito que a mesma tem no sistema. Os resultados encontrados devem ser

registrados no arquivo de gerenciamento de risco. A identificação de risco é ilustrada na Figura 16.

Figura 16 – Identificação de risco



Fonte: Elaborada pelo autor

4.2.2.2 Estimativa do risco

Após descobrir todas as falhas envolvendo a fabricação do equipamento, é necessário avaliar o impacto que essas falhas podem causar. Esse impacto é estimado tomando

como base três componentes, **severidade, frequência e detecção**, Esses componentes são respectivamente representados na Figura 17 como as transições *Severity*, *Frequency* e *Detectability*:

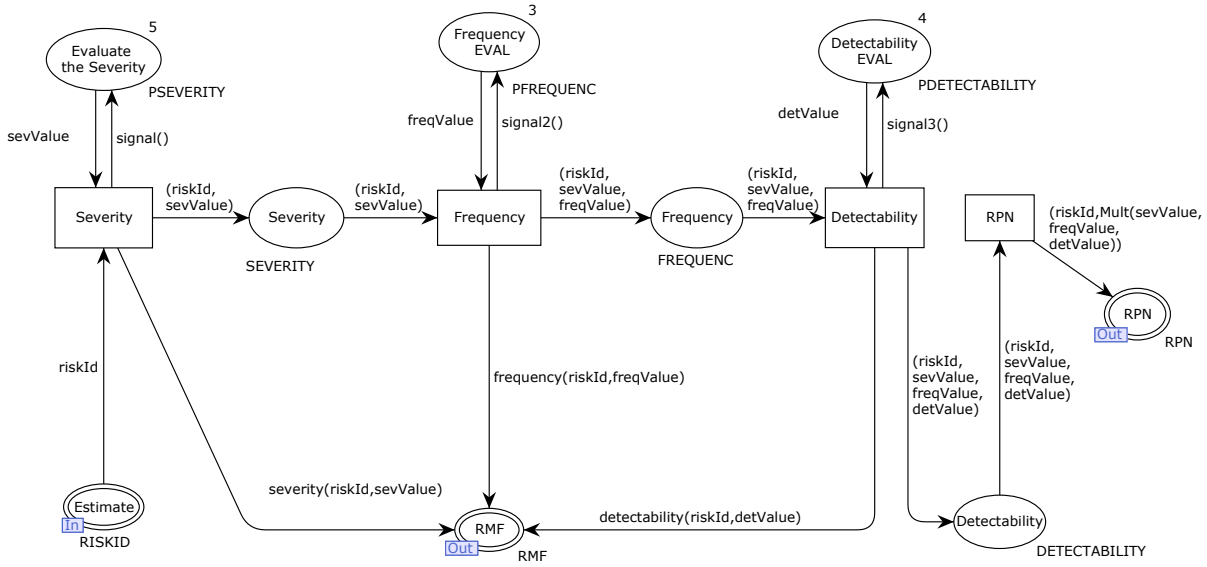
severidade : é uma representação em uma escala numérica onde, dada como verdadeira a ocorrência de uma falha, por exemplo choque elétrico, representa qual o dano que esta falha pode causar ao paciênte, médico ou operador do equipamento;

frequência : é uma representação em uma escala numérica que representa a quantidade de vezes que a falha irá acontecer;

detecção : é também uma representação em escala numérica que representa que dada como verdadeira a ocorrência da falha quais as chances de perceber que a falha está atuando.

É a partir da multiplicação dos valores adotados para cada um desses três componentes que o número de prioridade de risco (RPN - risk priority number) é estipulado. Esta multiplicação acontece no disparo da transição *RPN*. O valor máximo do RPN indica se o risco precisa ser reduzido e qual o risco que deve ser reduzido primeiro. Esta etapa é denominada *estimativa de risco* e é ilustrada na Figura 17.

Figura 17 – Estimativa do risco



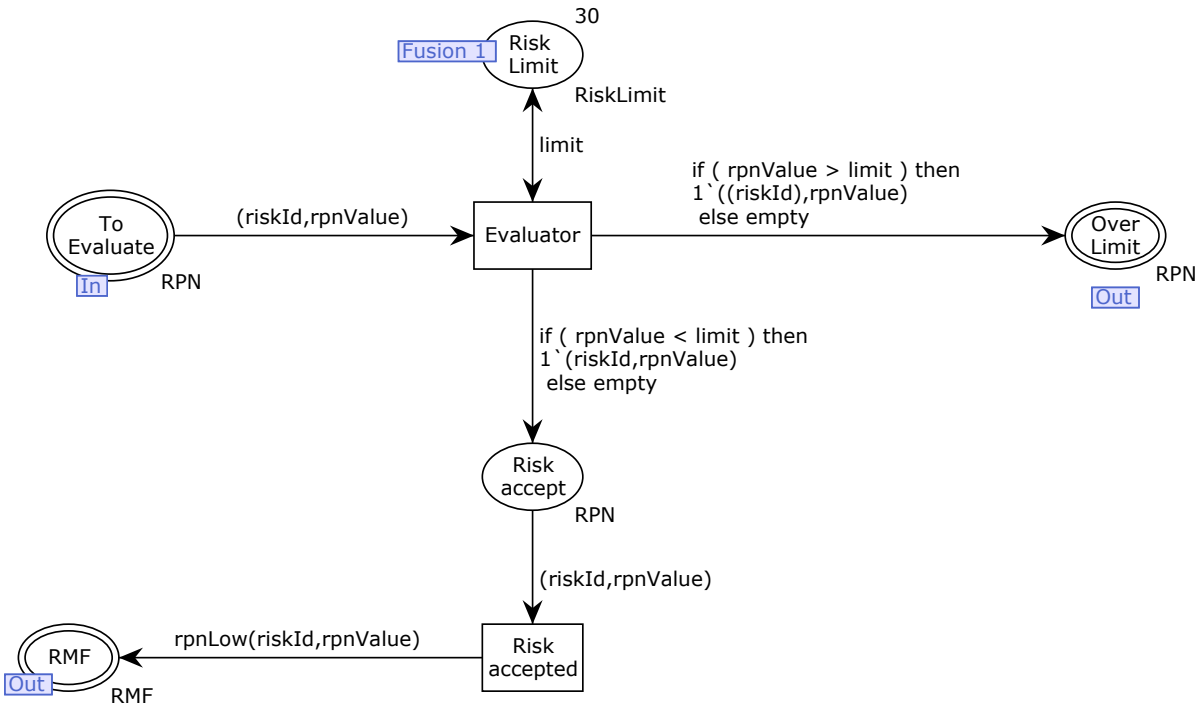
Fonte: Elaborada pelo autor

4.2.3 Avaliação de risco

A fase de avaliação de risco ilustrada na Figura 18, consiste em avaliar se a falha que está sendo analisada pode ser considerada como tolerável ou não. Essa avaliação é feita através da comparação entre o RPN e limite do risco estipulado durante o plano de

gerenciamento de risco, na transição *Evaluator*. Ao comparar os valores, se o RPN foi maior que o limite aceitável, então a ficha será enviada para o lugar denominado *Over Limit*, e então, dar-se-á início a fase de *controle do risco*. Caso contrário, a ficha será enviada para o lugar *Risk accept*, e será apenas necessário registrar as informações da falha no arquivo de gerenciamento de risco. A avaliação de risco é ilustrada na Figura 18.

Figura 18 – Avaliação de risco



Fonte: Elaborada pelo autor

4.2.4 Controle do risco

Quando uma falha considerada como não tolerável é encontrada, faz-se necessária a adoção de medidas corretivas para realizar a redução do risco. Com isso, o fabricante deve identificar medidas de controle de risco que sejam apropriadas a fim de reduzir os valores de **severidade, frequência e detecção**, previamente estipulados na fase de estimativa de risco.

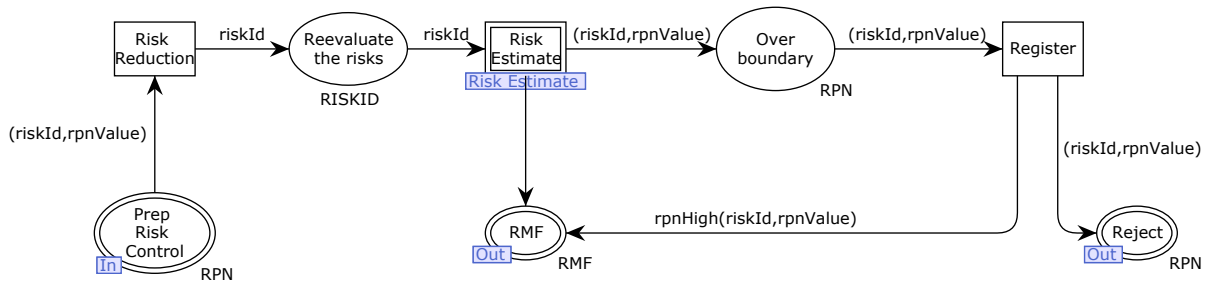
Considerando que o equipamento médico deve ser seguro o fabricante deve considerar a redução dos riscos baseado em uma ordem de prioridade. A primeira e maior prioridade é considerar segurança como um requisito inerente ao projeto. Desde a fase de projeto, todas as verificações e certificações para que o equipamento seja de fato seguro devem ser tomadas. A necessidade da redução do risco é representada pela transição *Risk Reduction* ilustrada na Figura 19.

Caso não seja possível garantir na fase de projeto que o equipamento médico não irá expor o paciente, o operador ou o médico a nenhuma situação perigosa, então, o

fabricante deverá fornecer medidas de proteção no próprio equipamento, mecanismos para evitar as situações perigosas, por exemplo, luzes de advertência e alertas sonoros. Por fim, caso nenhuma das medidas anteriores sejam aplicáveis, deve-se fornecer informações de segurança com o objetivo de informar ao usuário que existem determinadas situações perigosas e que estas podem causar danos.

As atividades de controle devem ser cuidadosamente escolhidas pois, ao tentar controlar o risco, novas falhas podem ser introduzidas (efeito colateral). Por isso, é essencial que, ao adotar uma atividade de controle, seja refeita a etapa de estimativa de risco. As medidas de controle de risco selecionadas devem ser registradas no arquivo de gerenciamento de risco, representada pela sub-rede *Risk Estimate*. Se a medida de redução de risco fizer com que o risco fique abaixo do limite aceitável então esta informação deve ser registrada no RMF, representado pelo lugar *RMF*. Caso contrário, deve ser iniciada a etapa de *risco residual*.

Figura 19 – Controle do Risco (Risk control)



Fonte: Elaborada pelo autor

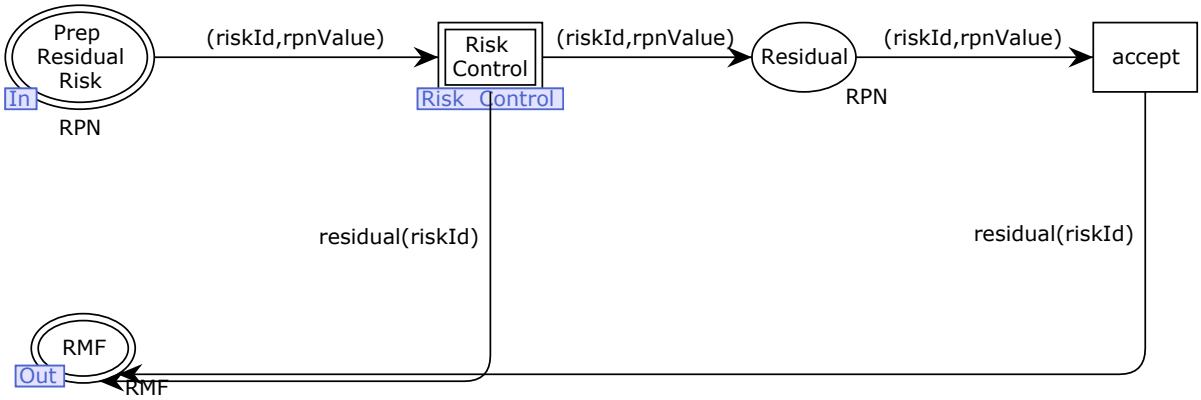
4.2.5 Risco residual

As medidas de redução do risco devem ser tomadas até que o RPN esteja no nível tolerável, representado pela sub-rede *Risk Control* na Figura 20. Se depois de ter passado por várias medidas corretivas, ainda assim o RPN permanecer acima do limite tolerável então a falha deve ser analisada como um risco residual. Este processo é ilustrado na Figura 20 e melhor detalhado a seguir.

Após a implementação das medidas de controle, os riscos residuais (aqueles que permanecem após terem sido aplicadas essas medidas) devem ser avaliados. Se nessa nova avaliação os riscos tornarem-se aceitáveis, então será necessário apenas registrar todo o processo no arquivo de gerenciamento de risco, representado pelo lugar *RMF*. Caso contrário, mais medidas de controle deverão ser aplicadas (GERARDO, Junho 2011). Se, ainda assim, as medidas de controle de risco não puderem ser aplicada, deverá ser feita a avaliação do risco residual baseado na análise risco/benefício, representado pela transição *accept*.

A análise risco/benefício consiste em discernir, por intermédio da literatura e análise crítica dos dados, se os benefícios de assumir a falha como tolerável superam os riscos. Se os benefícios médicos não superarem o risco residual então o risco residual continua inaceitável, precisando ser controlado. Se os benefícios superarem os riscos então o fabricante deverá criar uma informação de segurança para comunicar, da melhor forma possível, o risco residual. Os resultados obtidos nessa etapa devem ser registrados no arquivo de gerenciamento de risco.

Figura 20 – Risco Residual (Residual risk)



Fonte: Elaborada pelo autor

4.2.6 Análise e Validação do Modelo

Nesta seção é demonstrado, através da análise de espaço de estados o comportamento do modelo construído. Como previamente explicado na Seção 2.3.2.2, o conceito principal relacionado a verificação utilizando espaço de estados é a geração do conjunto de todos os estados alcançáveis (marcações), bem como as mudanças de estado, e representar esses como um grafo direcionado, onde os nós representam os estados e os arcos representam os eventos que ocorrem (JENSEN; KRISTENSEN; WELLS, 2007).

A validação do modelo foi realizada mediante três verificações do mesmo modelo: na primeira validação, denominada *modelo 1*, foi analisado o comportamento do modelo para quando o risco é sempre **maior** do que o limite de aceitação do risco; na segunda validação, denominada *modelo 2*, foi analisado o comportamento do modelo para quando o risco é sempre **menor** do que o limite de aceitação do risco e, na terceira validação, denominada *modelo 3*, foram analisados ambos os casos com os riscos acima e abaixo do valor de aceitação de risco. Foram gerados três relatórios de espaço de estados que serão melhor detalhados a seguir.

Com a utilização do espaço de estados foi possível constatar que o lugar *RMF* foi alcançado em todas as etapas, possibilitando assim ao fabricante construir o arquivo de gerenciamento de risco de forma correta.

A validação do modelo foi realizada através da análise do relatório de espaço de estados gerado pela ferramenta *CPN/Tools*. Nesses relatórios foram analisadas as seguintes propriedades :

Home properties: Propiedade utilizada para verificar a existencia de um estado específico, denominado *home*, que partindo de qualquer estado da rede pode-se atingir este estado específico.

Liveness properties: Propriedade utilizada para verificar a existência de transições vivas e mortas no modelo;

Boundedness properties: Propriedade utilizada para verificar a quantidade máxima e mínima de fichas que cada lugar pode conter;

Fairness properties: Propriedade utilizada para verificar a existência de transições disparando infinitas vezes.

O primeiro relatório corresponde a execução do modelo onde apenas riscos considerados como abaixo do limite são encontrados. O segundo relatório corresponde a execução do modelo contendo apenas riscos considerados acima do limite aceitável. Por fim, o último relatório que correspnde a execução onde riscos tanto aceitáveis como não aceitáveis são gerados. Para os dois primeiros relatórios a quantidade de fichas nos lugares foi limitada a 1 (uma) já no terceiro foi limitada a 2 (duas).

Primeiramente, foi analisada a propriedade equidade, *Fairness properties*. Esta propriedade foi igual para todos os modelos, o que prova que não existe nenhuma transição que dispara infinitamente em nenhum dos modelos estudados. A prorpriedade equidade é ilustrada na Figura 21.

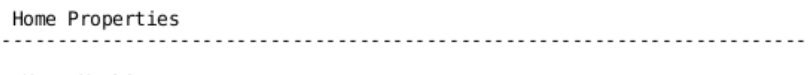
Figura 21 – Propriedade de equidade (*Fairness properties*)

```
Fairness Properties
------------------------------------------------------------------------
    No infinite occurrence sequences.
```

Fonte: Elaborada pelo autor

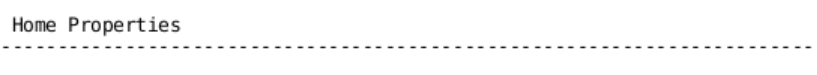
A segunda propriedade analisada foi a marcação *home*, *Home properties*. Apenas os dois primeiros relatório apresentaram a existencia de marcações *home*. As marcações *home [27]*, vide Figura 22, e marcação *[15]*, vide Figura 23. Ao analisar o modelo foi constatado que ambas são estados finais, sendo, assim, possível comprovar que a partir de qualquer estado do primeiro modelo é possível chegar ao estado final, representado no primeiro modelo pela marcação *[27]* e no segundo *[15]*. As marcações *[27]* e *[15]* são ilustradas também no Apêndice Figura 32 e Figura 33 respectivamente.

Figura 22 – Relatório 1, propriedade *Home*



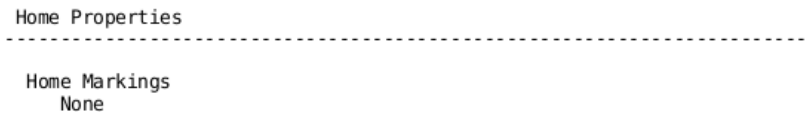
Fonte: Elaborada pelo autor

Figura 23 – Relatório 2, propriedade *Home*



Fonte: Elaborada pelo autor

Figura 24 – Relatório 3, propriedade *Home*



Fonte: Elaborada pelo autor

A terceira propriedade analisada foi a vivacidade, *Liveness properties*, propriedade utilizada para verificar a existência de transições vivas e mortas no modelo. De acordo com esta propriedade é possível destacar que nenhum modelo apresentou transições vivas. O último modelo, ilustrado na Figura 26, também não apresentou transições mortas (uma transição é denominada transição morta quando esta transição nunca é habilitada), o que representa que todas as transições foram habilitadas. Já os modelos 1 e 2, e seus respectivos relatórios, ilustrados nas Figuras 25 e 27, apresentaram transições mortas. Analisando o modelo 1, Figura 25, é possível destacar que o modelo executado com o valor do risco acima do limite tolerável não irá executar a transição para aceitar o risco durante a fase de avaliação de risco, que é o comportamento esperado para esta modelagem. Por outro lado, o modelo 2, Figura 27, por se tratar de uma simulação onde o valor do risco é abaixo do limite tolerável, todas as etapas referentes ao controle do risco não serão executadas, que é o comportamento desejado para este modelo.

Por intermédio da propriedade de vivacidade é possível destacar que os três modelos apresentaram marcações mortas, o modelo 1, Figura 25: marcação *[27]*; o modelo 2,

Figura 27: marcação *[15]*; e por fim, o modelo 3 Figura 26: que apresentou 403 marcações. Uma marcação morta, como por exemplo a marcação *[27]* na Figura 25, implica que nesta específica marcação não existe mais nenhuma transição habilitada (JENSEN, 2009). E analisando melhor as marcações mortas contidas nas figuras 25, 27 e 26 pode-se perceber que estas são também estados finais do sistema o que representa que o modelo terminou como esperado.

Figura 25 – Relatório 1, propriedade *Liveness*

```
Liveness Properties
----------------------------------------------------------------------

Dead Markings
   [27]

Dead Transition Instances
   Risk_Evaluation'Risk_accepted 1

Live Transition Instances
   None
```

Fonte: Elaborada pelo autor

Figura 26 – Relatório 3, propriedade *Liveness*

```
Liveness Properties
----------------------------------------------------------------------

Dead Markings
   403 [994,992,990,985,984,...]

Dead Transition Instances
   None

Live Transition Instances
   None
```

Fonte: Elaborada pelo autor

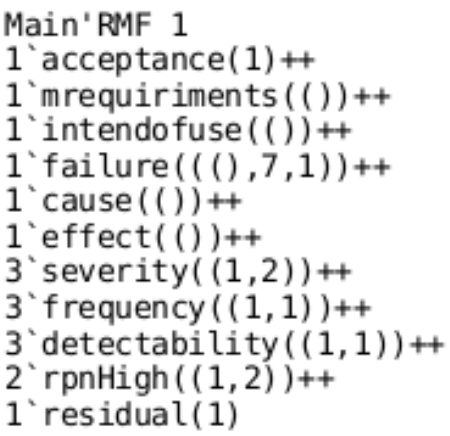
Figura 27 – Relatório 2, propriedade *Liveness*

```
Liveness Properties
-----------------------------------------------------------------------------

   Dead Markings
      [15]

   Dead Transition Instances
      Residual_Risk'accept 1
      Risk_Control'Register 1
      Risk_Control'Register 2
      Risk_Control'Risk_Reduction 1
      Risk_Control'Risk_Reduction 2
      Risk_Estimate'Detectability 2
      Risk_Estimate'Detectability 3
      Risk_Estimate'Frequency 2
      Risk_Estimate'Frequency 3
      Risk_Estimate'RiskPN 2
      Risk_Estimate'RiskPN 3
      Risk_Estimate'Severity 2
      Risk_Estimate'Severity 3

   Live Transition Instances
      None
```

Fonte: Elaborada pelo autor

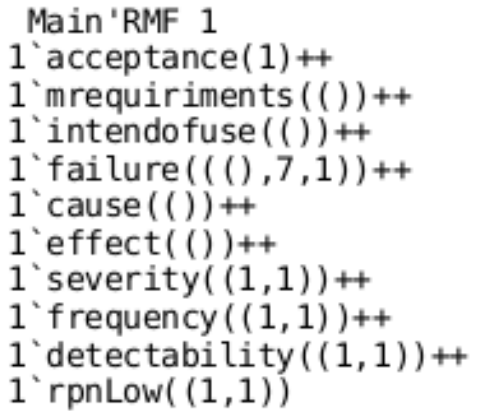
A última propriedade analisada foi a limitação, *Boundedness properties*. Desta propriedade, além de perceber a quantidade máxima e mínima de fichas que cada lugar poderia conter, o objetivo foi analisar através dos valores máximos quais fichas estavam no lugar denominado *Main'RMF*. No modelo 1, Figura 28, o comportamento esperado era que não houvesse nenhuma referência a *rpnLow*, o que acorreu conforme o esperado. Já no modelo 2, Figura 29, diferentemente do modelo 1, o esperado era que não houvesse nenhuma referência a *rpnHigh* e consequentemente a *residual*, indicando, assim, que de fato o modelo executou conforme o esperado. O modelo 3, Figura 30, de acordo com o que era almejado apresentou referência tanto para *rpnHigh* quanto para *rpnLow*.

Figura 28 – Relatório 1, propriedade *Boundedness*



Fonte: Elaborada pelo autor

Figura 29 – Relatório 2, propriedade *Boundedness*



Fonte: Elaborada pelo autor

Figura 30 – Relatório 3, propriedade *Boundedness*

```
 Main'RMF 1
1`acceptance(1)++
1`mrequiriments(())++
1`intendofuse(())++
1`failure(((),5,1))++
1`failure(((),5,2))++
2`cause(())++
2`effect(())++
3`severity((1,1))++
1`severity((1,2))++
3`severity((2,1))++
1`severity((2,2))++
3`frequency((1,1))++
1`frequency((1,2))++
3`frequency((2,1))++
1`frequency((2,2))++
3`detectability((1,1))++
1`detectability((1,2))++
3`detectability((2,1))++
1`detectability((2,2))++
1`rpnLow((1,1))++
1`rpnLow((2,1))++
2`rpnHigh((1,1))++
2`rpnHigh((2,1))++
1`residual(1)++
1`residual(2)
```

Fonte: Elaborada pelo autor

Além da análise do relatório de espaço de estado, foi utilizada a técnica de verificação de modelos (*model checking*). *Model checking* é uma técnica automática para verificar sistemas concorrentes finitos (CLARKE JR.; GRUMBERG; PELED, 1999), que faz uso da lógica temporal para a verificação de propriedades associadas ao modelo construído. Possui diversas vantagens se comparada com as abordagens tradicionais baseadas em simulação, teste e raciocínio dedutivo (CLARKE JR.; GRUMBERG; PELED, 1999). Neste trabalho foram verificadas três propriedades utilizando a lógica temporal *ASK-CTL* com o objetivo de aplicar a técnica de verificação de modelo (*model checking*) (CLARKE JR.; GRUMBERG; PELED, 1999). A lógica temporal é um formalismo usado para descrever sequências de transições entre os estados em um sistema, descrevendo a ordem em que os eventos acontecem no tempo sem utilizar de forma explicita o tempo. A lógica temporal pode ser descrita através da lógica de árvore computacional *(Computational Tree Logic - CTL)*, e neste trabalho será utilizada uma variação da *CTL* denominada *ASK-CTL*. Para a verificação destas propriedades são utilizados os operadores descritos na Tabela 13. É através da ASK-CTL que as três propriedades a serem verificadas foram especificadas. As três propriedades são:

1. Todos os resultados de cada etapa do gerenciamento de risco deve ser registrado no

arquivo de gerenciamento de risco;

2. Os riscos só podem ser avaliados depois de terem sido identificados e estimados;
3. Todos os riscos acima do limite aceitável devem ser reduzidos.

Tabela 13 – Operadores utilizados para a construção das fórmulas em *ASK-CTL*

Operadores	**Descrição**
EV (A)	É verdadeiro se o argumento, A, torna-se eventualmente verdadeiro para qualquer estado a partir do estado atual. O argumento A deve se tornar realidade dentro de um número finito de passos.
POS (A)	É verdadeiro caso seja possível chegar, a partir do estado atual, a um estado onde o argumento A é verdadeiro.
Modal (A)	MODAL, como uma fórmula estado, é verdade, se existe uma transição imediata, a partir de onde estamos agora, e se o argumento de MODAL, A, é verdade a partir desta transição. O argumento, A, deve ser uma fórmula de transição. MODAL, como uma fórmula de transição é verdadeiro se o seu argumento, A, é verdadeiro, no estado de destino.
NF (A)	NF é a função do nó e só faz sentido para usar como uma sub-fórmula de estado. Seus argumentos são uma String e uma função que leva um nó de espaço de estado e retorna um boolean.
AF (A)	AF é a função de arco e é análoga à NF e deve ser usada como uma sub-fórmula de transição.

Fonte: Elaborada pelo autor

Na primeira fórmula *(1)*, *failureMode, criticalAnalysis e isDetectability* são predicados relacionados aos lugares (*failureMode e criticalAnalysis*) e transição (*isDetectability*).

```
EV(POS(AND(AND(MODAL(AF("_",failureMode)),
   POS(MODAL(AF("_", criticalAnalysis)))),                    (1)
      POS(NF("Performed",isDetectability)))));
```

Já para a segunda fórmula *(2)*, *isEachRisk, riskPN e evaluator* são predicados relacionados aos lugares (*riskPN e evaluator*) e transição (*riskPN*).

```
EV(POS(AND(AND(NF("er",isEachRisk),
   EV(MODAL(AF("_",riskPN)))),                                    (2)
      EV(MODAL(AF("_",evaluator))))));
```

Por fim, a terceira fórmula *(3)*, *RiskReduction e RPN* são predicados onde *RiskReduction* está relacionado com a transição, já o predicado *RPN* está relacionado ao lugar.

```
POS(AND(MODAL(AF(RiskReduction)),
      EV(MODAL(AF(RPN))));                                        (3)
```

A validação e verificação através da análise do relatório de espaço de estados e da utilização de *model checking* são importantes para provar a consistência do modelo tomando como referência os resultados obtidos através das propriedades *home, boundness, liveness e fairness*, e demonstrar que o modelo construído atende a requisitos da *ISO 14971* tais como, registrar cada etapa do processo de gerenciamento de risco no arquivo de gerenciamento de risco e reduzir os riscos acima do limite aceitável.

5 CONCLUSÃO

A fabricação de equipamentos médicos seguros é um desafio. Exige por parte dos fabricantes o conhecimento de diversificadas técnicas de segurança, além da criação de um processo no qual se torne possível o reconhecimento das falhas e situações perigosas. Por isso, torna-se um processo difícil de ser aplicado e replicado, levando as empresas por muitas vezes a construírem processos exageradamente complexos ao ponto delas mesmas não conseguirem seguir (SCHMULAND, 2005), ou simplistas demais incapazes de gerar resultados confiáveis. Pensando nisto, foi proposto neste trabalho um modelo do gerenciamento de riscos na fabricação de equipamentos médicos utilizando a ISO 14971 e a técnica de análise de risco FMECA. Foi elaborada uma modelagem formal em *RPC* deste processo e realizado um estudo de caso, tendo como base um equipamento de Eletrogastrografia (EGG) de baixo custo. As principais contribuições deste trabalho são:

- Avaliação de três técnicas de análise de risco;
- Elaboração de um estudo de caso, do processo de gerenciamento de risco, para um equipamento médico.
- Modelagem formal da ISO 14971 e da técnica FMECA;
- Validação e verificação do modelo construído;

Foi realizado um levantamento bibliográfico sobre a ISO 14971 e, posteriormente, sobre as técnicas de análise de risco. Como resultado da avaliação das técnicas, foi adotada a FMECA por ser um método dedutivo que permite a análise crítica de cada modo de falha de forma individual.

Em seguida, foi realizado um estudo de caso do processo de gerenciamento de risco, pré-mercado, do equipamento médico de Eletrogastrografia de superfície. Este estudo teve o objetivo de obter um conhecimento mais aprofundado da ISO 14971:2009 (ABNT - ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2009), analisando esta ISO, etapa por etapa, a fim de criar um modelo formal em *RPC*.

Por fim, foi criado o modelo em *RPC* que auxilia a reduzir a subjetividade inerente a descrição em linguagem natural, haja vista que a má compreenção da ISO por parte dos fabricantes reflete na criação de modelos complexos aos quais não conseguem manter (SCHMULAND, 2005). Além disto, este modelo auxilia nas etapas de verificação e validação do equipamento médico, etapas essenciais para a fabricação de equipamentos médicos seguros (KORB et al., 2003; SIVAKUMAR et al., 2011). Destaque-se, também, a possibilidade do uso do modelo como uma ferramenta didática para o ensino e treinamento do processo de gerenciamento de risco. O entendimento da ISO é importante, pois

este é um padrão adotado por agências reguladoras tais como a ANVISA e o FDA para a especificação de segurança de equipamento médico.

Como trabalho futuro será aplicada a técnica de verificação de modelo (*model checking*) (CLARKE JR.; GRUMBERG; PELED, 1999), para mais três propriedades além das propriedades verificadas. Após a verificação do modelo, será implementado o *software* que baseado no modelo irá auxiliar no processo de gerenciamento de risco conforme as especificações da ISO 14971:2009. Este *software* irá tornar o processo de gerenciamento de risco mais interativo e menos suscetível a erros humanos. Será realizado outro estudo de caso do processo de gerenciamento de risco utilizando o modelo em *RPC* de um equipamento médico de Classificação III a fim de validar o modelo para equipamentos médicos mais complexos.

REFERÊNCIAS

ABNT - ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. *ISO 14971:2009, ABNT NBR : Produtos para a saúde — Aplicação de gerenciamento de risco a produtos para a saúde*. 2009.

ALEMZADEH, H. et al. Analysis of safety-critical computer failures in medical devices. *Security Privacy, IEEE*, v. 11, n. 4, p. 14–26, 2013. ISSN 1540-7993.

AMARENDRA, A. V. R. K. Safety critical systems analysis. *Global Journal of Computer Science and Technology*, v. 11, n. 21, 2011. ISSN 0975-4172. Disponível em: <http://computerresearch.org/stpr/index.php/gjcst/article/view/949/836>.

AMMAR, H.; NIKZADEH, T.; DUGAN, J. A methodology for risk assessment of functional specification of software systems using colored petri nets. In: *Software Metrics Symposium, 1997. Proceedings., Fourth International*. [S.l.: s.n.], 1997. p. 108–117.

BARTOO, G. Risk management [medical devices]. *Engineering in Medicine and Biology Magazine, IEEE*, v. 22, n. 4, p. 166–172, July 2003. ISSN 0739-5175.

BLOOMFIELD, R. et al. *Supplement G: Safety case use within the medical devices industry*. [S.l.], December 2012.

BRITO, I.; BARROS, J. Coloured petri net model of the bcms system using cpn tools. In: *Comparing Requirements Modeling Approaches Workshop (CMA@RE), 2013 International*. [S.l.: s.n.], 2013. p. 7–12.

BURTON, J.; MCCAFFERY, F.; RICHARDSON, I. A risk management capability model for use in medical device companies. In: *Proceedings of the 2006 International Workshop on Software Quality*. New York, NY, USA: ACM, 2006. (WoSQ '06), p. 3–8. ISBN 1-59593-399-9. Disponível em: <http://doi.acm.org/10.1145/1137702.1137705>.

CHEN, H.-C. et al. A petri net modeling approach based on boolean function transition. In: *Computer, Consumer and Control (IS3C), 2012 International Symposium on*. [S.l.: s.n.], 2012. p. 423–426.

CLARKE JR., E. M.; GRUMBERG, O.; PELED, D. A. *Model Checking*. Cambridge, MA, USA: MIT Press, 1999. ISBN 0-262-03270-8.

DUNJÓ, J. et al. Hazard and operability (hazop) analysis. a literature review. *Journal of Hazardous Materials*, v. 173, n. 1–3, p. 19 – 32, 2010. ISSN 0304-3894. Disponível em: <http://www.sciencedirect.com/science/article/pii/S0304389409013727>.

GERARDO, A. *COLOCAÇÃO NO MERCADO DE DISPOSITIVOS MÉDICOS ASSOCIADOS À M EDICINA FÍSICA E DE REABILITAÇÃO PARA UTILIZAÇÃO EM AMBIENT ASSISTED LIVING*. Dissertação (Mestrado) — Exa4Live HealthCare Solutions, Coimbra, Junho 2011.

GIRAULT, C.; VALK, R. *Petri Nets for System Engineering: A Guide to Modeling, Verification, and Applications*. Secaucus, NJ, USA: Springer-Verlag New York, Inc., 2001. ISBN 3540412174.

HATCLIFF, J. et al. Rationale and architecture principles for medical application platforms. In: *Cyber-Physical Systems (ICCPS), 2012 IEEE/ACM Third International Conference on*. [S.l.: s.n.], 2012. p. 3–12.

HEGDE, V. Case study 2014; risk management for medical devices (based on iso 14971). In: *Reliability and Maintainability Symposium (RAMS), 2011 Proceedings - Annual*. [S.l.: s.n.], 2011. p. 1–6. ISSN 0149-144X.

HERMAN, R.; JANASAK, K. Using fmeca to design sustainable products. In: *Reliability and Maintainability Symposium (RAMS), 2011 Proceedings - Annual*. [S.l.: s.n.], 2011. p. 1–6. ISSN 0149-144X.

HOEPFFNER, L. Analysis of the {HAZOP} study and comparison with similar safety analysis systems. *Gas Separation & Purification*, v. 3, n. 3, p. 148 – 151, 1989. ISSN 0950-4214. Disponível em: <http://www.sciencedirect.com/science/article/pii/0950421489800271>.

HOLSBACH, L. R.; NETO, F. J. K.; HOLSBACH, N. Utilização do instrumento de identificação de conhecimentos para administração segura de medicamentos com o uso de infusão automática. *Revista Brasileira de Engenharia Biomédica*, scielo, v. 29, p. 353 – 362, 12 2013. ISSN 1517-3151. Disponível em: <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S1517-31512013000400005&nrm=iso>.

HUBER, P.; JENSEN, K.; SHAPIRO, R. Hierarchies in coloured petri nets. In: ROZENBERG, G. (Ed.). *Advances in Petri Nets 1990*. Springer Berlin Heidelberg, 1991, (Lecture Notes in Computer Science, v. 483). p. 313–341. ISBN 978-3-540-53863-9. Disponível em: <http://dx.doi.org/10.1007/3-540-53863-1_30>.

HUFFMAN, D.; BOWMAN, K.; AKERS, J. What we can learn about reliability and safety analyses from different industries. In: *Reliability and Maintainability Symposium (RAMS), 2013 Proceedings - Annual*. [S.l.: s.n.], 2013. p. 1–6. ISSN 0149-144X.

INTERNATIONAL ELECTROTECHNICAL COMMISSION. *FAULT TREE ANALYSIS (FTA)*. [S.l.], 2006.

INTERNATIONAL ORGANISATION FOR STANDARDISATION. *ISO 14971 - Medical devices – Application of risk management to medical devices*. [S.l.], 2000.

JAIN, R. et al. Risk analysis of medical instruments - case study of cardiac output monitor. In: *Reliability, Safety and Hazard (ICRESH), 2010 2nd International Conference on*. [S.l.: s.n.], 2010. p. 637–641.

JAVADI, M. S.; NOBAKHT, A.; MESKARBASHEE, A. Fault tree analysis approach in reliability assessment of power system. *INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY SCIENCES AND ENGINEERING*, VOL. 2, n. NO. 6, SEPTEMBER SEPTEMBER 2011. Disponível em: <http://www.ijmse.org/Volume2/Issue6/paper9.pdf>.

JENSEN, K.; KRISTENSEN, L. M.; WELLS, L. Coloured petri nets and cpn tools for modelling and validation of concurrent systems. *Int. J. Softw. Tools Technol. Transf.*, Springer-Verlag, Berlin, Heidelberg, v. 9, n. 3, p. 213–254, maio 2007. ISSN 1433-2779. Disponível em: <http://dx.doi.org/10.1007/s10009-007-0038-x>.

JENSEN, L. K. K. *Coloured Petri Nets*. [S.l.]: Springer, 2009.

KAISER, B.; LIGGESMEYER, P.; MäCKEL, O. A new component concept for fault trees. In: *Proceedings of the 8th Australian Workshop on Safety Critical Systems and Software - Volume 33*. Darlinghurst, Australia, Australia: Australian Computer Society, Inc., 2003. (SCS '03), p. 37–46. ISBN 1-920-68215-5. Disponível em: <http://dl.acm.org/citation.cfm?id=1082051.1082054>.

KANG, B.; YOON, E. S.; SUH, J. C. Application of automated hazard analysis by new multiple process-representation models to chemical plants. *Industrial & Engineering Chemistry Research*, v. 40, n. 8, p. 1891–1902, 2001. Disponível em: <http://pubs.acs.org/doi/abs/10.1021/ie000745d>.

KAWATHEKAR, D.; MOORTHY, E.; CHANDRAPPA, N. Impact of fmea on improving software reliability of an ultrasound system designed for emerging market countries. In: *Proceedings of the 5th India Software Engineering Conference*. New York, NY, USA: ACM, 2012. (ISEC '12), p. 149–152. ISBN 978-1-4503-1142-7. Disponível em: <http://doi.acm.org/10.1145/2134254.2134281>.

KOMOROWSKI, D.; PIETRASZEK, S.; GRZECHCA, D. The wireless system for egg signal acquisition. In: *Electronics, Circuits and Systems (ICECS), 2012 19th IEEE International Conference on*. [S.l.: s.n.], 2012. p. 372–375.

KORB, W. et al. Risk analysis for a reliable and safe surgical robot system. *International Congress Series*, v. 1256, n. 0, p. 766 – 770, 2003. ISSN 0531-5131. {CARS} 2003. Computer Assisted Radiology and Surgery. Proceedings of the 17th International Congress and Exhibition. Disponível em: <http://www.sciencedirect.com/science/article/pii/S0531513103004023>.

KUMAR, S. et al. Mobile health: Revolutionizing healthcare through transdisciplinary research. *Computer*, v. 46, n. 1, p. 28–35, Jan 2013. ISSN 0018-9162.

LIM, E. et al. Design of low-power low-voltage biomedical amplifier for electrocardiogram signal recording. In: *Biomedical Circuits and Systems Conference, 2007. BIOCAS 2007. IEEE*. [S.l.: s.n.], 2007. p. 191–194.

LUTHRA, P. Fmeca: an integrated approach. In: *Reliability and Maintainability Symposium, 1991. Proceedings., Annual*. [S.l.: s.n.], 1991. p. 235–241.

MAHMUD, N.; WALKER, M.; PAPADOPOULOS, Y. Compositional synthesis of temporal fault trees from state machines. In: *Availability, Reliability and Security (ARES), 2011 Sixth International Conference on*. [S.l.: s.n.], 2011. p. 429–435.

MATSUURA, Y. et al. Dynamics analysis of electrogastrography using double-wayland algorithm. In: *Engineering in Medicine and Biology Society, 2007. EMBS 2007. 29th Annual International Conference of the IEEE*. [S.l.: s.n.], 2007. p. 1973–1976. ISSN 1557-170X.

MORELLO, R.; CAPUA, C. D.; LAMONACA, F. Diagnosis of gastric disorders by non-invasive myoelectrical measurements. In: *Instrumentation and Measurement Technology Conference (I2MTC), 2013 IEEE International*. [S.l.: s.n.], 2013. p. 1324–1328. ISSN 1091-5281.

MURATA, T. Petri nets: Properties, analysis and applications. *Proceedings of the IEEE*, v. 77, n. 4, p. 541–580, Apr 1989. ISSN 0018-9219.

PARKMAN, H. P. et al. Electrogastrography: a document prepared by the gastric section of the american motility society clinical gi motility testing task force. *Neurogastroenterology & Motility*, Blackwell Science Ltd, v. 15, n. 2, p. 89–102, 2003. ISSN 1365-2982. Disponível em: <http://dx.doi.org/10.1046/j.1365-2982.2003.00396.x>.

PASKARANANDAVADIVEL, N. et al. Automated classification of spatiotemporal characteristics of gastric slow wave propagation. In: *Engineering in Medicine and Biology Society (EMBC), 2013 35th Annual International Conference of the IEEE*. [S.l.: s.n.], 2013. p. 7342–7345. ISSN 1557-170X.

PATARA, F.; VICARIO, E. An adaptable patient-centric electronic health record system for personalized home care. In: *Medical Information and Communication Technology (ISMICT), 2014 8th International Symposium on*. [S.l.: s.n.], 2014. p. 1–5.

RODRIGUES, C. L. *VerificaÇÃo de Modelos em Redes de Petri Orientadas a Objetos*. Dissertação (Mestrado) — Universidade Federal de Campina Grande, Campina Grande, Paraíba, Brasil, Fevereiro 2004.

SCHMULAND, C. Value-added medical-device risk management. *Device and Materials Reliability, IEEE Transactions on*, v. 5, n. 3, p. 488–493, 2005. ISSN 1530-4388.

SIVAKUMAR, M. et al. Improving verification & validation in the medical device domain. In: O'CONNOR, R.; PRIES-HEJE, J.; MESSNARZ, R. (Ed.). *Systems, Software and Service Process Improvement*. Springer Berlin Heidelberg, 2011, (Communications in Computer and Information Science, v. 172). p. 61–71. ISBN 978-3-642-22205-4. Disponível em: <http://dx.doi.org/10.1007/978-3-642-22206-1_6>.

STANDARD, M. *Procedures for performing a failure mode, effects and criticality analysis*. 24 NOVEMBER 1980.

TEIXEIRA, P. A. M. *APLICAÇÃO DO FMECA A SISTEMAS DE ESTABILIZAÇÃO E REFORÇO DE MACIÇOS EM TÚNEIS*. Dissertação (Mestrado) — Universidade de Aveiro, 2009.

US DEPARTMENT OF DEFENSE. *MIL-STD-1629A : Procedures for Performing a Failure Mode, Effects and Criticality Analysis*. 24 november 1980.

WESTERGAARD, M.; VERBEEK, H. E. *CPN Tools*. 2014. Último acesso em 15/11/2014. Disponível em: <http://cpntools.org/>.

YIN, J.; CHEN, J. D. Z. Electrogastrography: Methodology, validation and applications. In: *J Neurogastroenterol Motil*. http://synapse.koreamed.org/DOIx.php?id=10.5056%2Fjnm.2013.19.1.5: Asian Neurogastroenterology and Motility Association; Korean Society of Neurogastroenterology and Motility, 2013/Jan. v. 19, n. 2093-0879, p. 13.

ZHAO, X.; BAI, X. The application of fmea method in the risk management of medical device during the lifecycle. In: *e-Business and Information System Security (EBISS), 2010 2nd International Conference on*. [S.l.: s.n.], 2010. p. 1–4.

APÊNDICE A – APÊNDICE

Tabela 14 – Tabela FMECA com as falhas encontradas

ID	Componente	Função	Modo Potencial de Falha	Efeitos potencias de falha	Causas potenciais/ Mecanismo de falha
10	Microcontrolador	Converter o sinal analógico pra digital de 10 bits	Má conversão A/D	Perda da qualidade do sinal	Microcontrolador com defeito
5	Sensoriamento - Cabos de Blindagem	Conduzir os impulsos mioelétricos registrados pelo eletrodo até a etapa de condicionamento de sinal	Má qualidade dos cabos	Ruídos	Interferência Eletromagnética
6	Amplificador de instrumentação	Amplificar o sinal de microvolts para volts	Amplificador de instrumentação com defeito	Valores do sinal fora da faixa	Hardware mal construido pelo fabricante
8	Amplificador operacional	Amplificar a diferença entre dois sinais analógicos aplicados às suas entradas.	Amplificador operacional com defeito	Valores do sinal fora da faixa	Hardware mal construido pelo fabricante
13	Bluetooth	Enviar os dados do EGG RN42	Problema no hardware do bluetooth	Erro na comunicação dos dados	Equipamento com defeito
14	Bluetooth	Enviar os dados do EGG RN42	Desvaneicimento e terminal oculto	Erro na comunicação dos dados	Barreiras fisicas ou distanciamento do equipamento
15	Bateria	Alimentação energética do equipamento	Baixa carga da bateria	Equipamento pode parar de funcionar	Falta de recarga do equipamento
16	Bateria	Alimentação energética do equipamento	Baixa carga da bateria	Erro na Leitura devido a baixa carga da bateria	Falta de recarga do equipamento
1	Sensoriamento - Eletrodo	Registrar os impulsos mioelétricos do estomago	Posicionamento errado do eletrodo	Leitura errada dos dados	Má capacitação do operador

Continua na próxima página

Tabela 14 – *Continua na próxima página*

ID	Componente	Função	Modo Potencial de Falha	Efeitos potencias de falha	Causas potenciais/ Mecanismo de falha
2	Sensoriamento - Eletrodo	Registrar os impulsos mioelétricos do estomago	Impedância fora da faixa	Erro na leitura dos dados	Eletrodos fora da validade
11	Microcontrolador	Condicionar o sinal e converter para digital	Microcontrolador mal programado de fábrica	Perda da qualidade do sinal	Equipamento mal configurado pelo projetista
12	Microcontrolador	Condicionar o sinal e converter para digital	Instabilidade da alimentação elétrica	Erro na programação e perda de sinal	Instabilidade no fornecimento eletrica
17	Software	Auto teste, teste de bateria e impedância	Erro no auto teste	Mensagem de erro e falha na comunicação com o computador	Auto teste mal programado
18	Software	Auto teste, teste de bateria e impedância	Erro no teste de bateria	Mensagem de erro e Impedir de fazer o exame	Auto teste da bateria mal programado
19	Software	Auto teste, teste de bateria e impedância	Erro no teste de impedância	Mensagem de erro e Impedir de fazer o exame	Auto teste da impedância mal programado
7	Amplificador de instrumentação	Amplificar o sinal de microvolts para volts	Configuração errada do amplificador de instrumentação	Valores fora da faixa	Equipamento mal configurado pelo projetista
9	Amplificador operacional	Amplificar a diferença entre dois sinais analógicos aplicados às suas entradas.	Configuração errada do amplificador operacional	Configuração errada	Equipamento mal configurado pelo projetista

Continua na próxima página

Tabela 14 – *Continua na próxima página*

ID	Componente	Função	Modo Potencial de Falha	Efeitos potencias de falha	Causas potenciais/ Mecanismo de falha
3	Sensoriamento - Cabos de Blindagem	Conduzir os impulsos mioelétricos registrados pelo eletrodo até a etapada de condicionamento de sinal	Má isolamento elétricos sofrendo interferências externas	Ruídos	Interferência Eletromagnética
4	Sensoriamento - Cabos de Blindagem	Conduzir os impulsos mioelétricos registrados pelo eletrodo até a etapada de condicionamento de sinal	Má conservação dos cabos	Não envio dos dados	Cabo com defeito

Fonte: elaborada pelo autor

Figura 31 – Tabela FMECA com os riscos encontrados, valores dos componentes e RPN

ID	Modo Potencial de Falha	S	O	D	RPN
10	Mal conversão A/D	5	1	1	5
5	Má qualidade dos cabos	5	2	1	10
6	Amplificador de instrumentação com defeito	5	3	2	30
8	Amplificador operacional com defeito	5	3	2	30
13	Problema no hardware do bluetooth	5	3	2	30
14	Desvaneicimento e terminal oculto	5	4	2	40
15	Baixa carga da bateria	5	4	2	40
16	Baixa carga da bateria	5	4	2	40
1	Posicionamento errado do eletrodo	5	3	3	45
2	Impedância fora da faixa	5	3	3	45
11	Microcontrolador mal programado de fábrica	5	3	3	45
12	Instabilidade da alimentação elétrica	5	3	3	45
17	Erro no auto teste	5	3	3	45
18	Erro no teste de bateria	5	3	3	45
19	Erro no teste de impedância	5	3	3	45
7	Configuração errada do amplificador de instrumentação	5	5	2	50
9	Configuração errada do amplificador operacional	5	5	2	50
3	Mal isolamento elétricos sofrendo interferências externas	5	4	5	100
4	Mal conservação dos cabos	5	4	5	100

Fonte: Elaborada pelo autor

Tabela 15 – Tabela FMECA completa

ID	Componente	Função	Modo Potencial de Falha	Efeitos potencias de falha	S	Causas potenciais/ Mecanismo de falha	O	D	RPN
10	Microcontrolador	Converter o sinal analógico pra digital de 10 bits	Má conversão A/D	Perda da qualidade do sinal	5	Microcontrolador com defeito	1	1	5
5	Sensoriamento - Cabos de Blindagem	Conduzir os impulsos mioelétricos registrados pelo eletrodo até a etapa de condicionamento de sinal	Má qualidade dos cabos	Ruídos	5	Interferência Eletromagnética	2	1	10
6	Amplificador de instrumentação	Amplificar o sinal de microvolts para volts	Amplificador de instrumentação com defeito	Valores do sinal fora da faixa	5	Hardware mal construido pelo fabricante	3	2	30
8	Amplificador operacional	Amplificar a diferença entre dois sinais analógicos aplicados às suas entradas.	Amplificador operacional com defeito	Valores do sinal fora da faixa	5	Hardware mal construido pelo fabricante	3	2	30
13	Bluetooth	Enviar os dados do EGG RN42	Problema no hardware do bluetooth	Erro na comunicação dos dados	5	Equipamento com defeito	3	2	30
14	Bluetooth	Enviar os dados do EGG RN42	Desvaneicimento e terminal oculto	Erro na comunicação dos dados	5	Barreiras fisicas ou distanciamento do equipamento	4	2	40
15	Bateria	Alimentação energética do equipamento	Baixa carga da bateria	Equipamento pode parar de funcionar	5	Falta de recarga do equipamento	4	2	40

Continued on next page

Tabela 15 – *Continua na próxima página*

ID	Componente	Função	Modo Potencial de Falha	Efeitos potencias de falha	S	Causas potenciais/ Mecanismo de falha	O	D	RPN
16	Bateria	Alimentação energética do equipamento	Baixa carga da bateria	Erro na Leitura devido a baixa carga da bateria	5	Falta de recarga do equipamento	4	2	40
1	Sensoriamento - Eletrodo	Registrar os impulsos mioelétricos do estomago	Posicionamento errado do eletrodo	Leitura errada dos dados	5	Má capacitação do operador	3	3	45
2	Sensoriamento - Eletrodo	Registrar os impulsos mioelétricos do estomago	Impedância fora da faixa	Erro na leitura dos dados	5	Eletrodos fora da validade	3	3	45
11	Microcontrolador	Condicionar o sinal e converter para digital	Microcontrolador mal programado de fábrica	Perda da qualidade do sinal	5	Equipamento mal configurado pelo projetista	3	3	45
12	Microcontrolador	Condicionar o sinal e converter para digital	Instabilidade da alimentação elétrica	Erro na programação e perda de sinal	5	Instabilidade no fornecimento eletrica	3	3	45
17	Software	Auto teste, teste de bateria e impedância	Erro no auto teste	Mensagem de erro e falha na comunicação com o computador	5	Auto teste mal programado	3	3	45
18	Software	Auto teste, teste de bateria e impedância	Erro no teste de bateria	Mensagem de erro e Impedir de fazer o exame	5	Auto teste da bateria mal programado	3	3	45

Continued on next page

Tabela 15 – *Continua na próxima página*

ID	Componente	Função	Modo Potencial de Falha	Efeitos potencias de falha	S	Causas potenciais/ Mecanismo de falha	O	D	RPN
19	Software	Auto teste, teste de bateria e impedância	Erro no teste de impedância	Mensagem de erro e Impedir de fazer o exame	5	Auto teste da impedância mal programado	3	3	45
7	Amplificador de instrumentação	Amplificar o sinal de microvolts para volts	Configuração errada do amplificador de instrumentação	Valores fora da faixa	5	Equipamento mal configurado pelo projetista	5	2	50
9	Amplificador operacional	Amplificar a diferença entre dois sinais analógicos aplicados às suas entradas.	Configuração errada do amplificador operacional	Configuração errada	5	Equipamento mal configurado pelo projetista	5	2	50
3	Sensoriamento - Cabos de Blindagem	Conduzir os impulsos mioelétricos registrados pelo eletrodo até a etapada de condicionamento de sinal	Má isolamento elétricos sofrendo interferências externas	Ruídos	5	Interferência Eletromagnética	4	5	100
4	Sensoriamento - Cabos de Blindagem	Conduzir os impulsos mioelétricos registrados pelo eletrodo até a etapada de condicionamento de sinal	Má conservação dos cabos	Não envio dos dados	5	Cabo com defeito	4	5	100

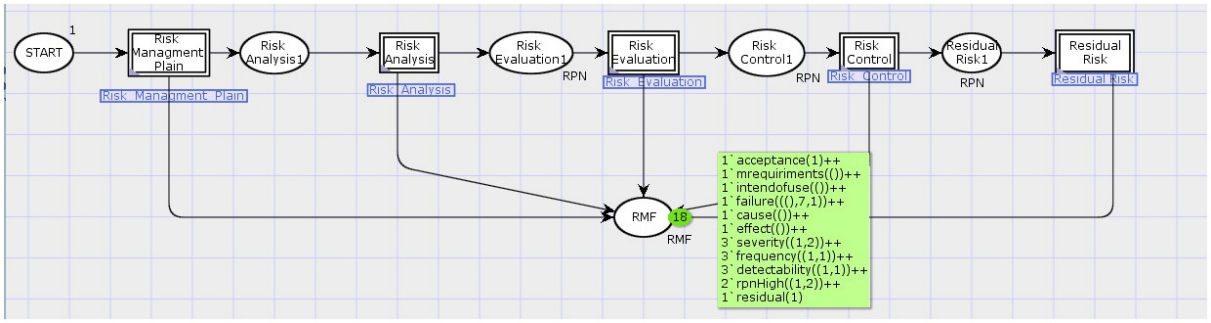
Fonte: elaborada pelo autor

Tabela 16 – Continuação da Tabela FMECA completa

ID	Ações Tomadas	Nova S	Nova O	Nova D	RPN
10	Executar o teste de reconstrução do sinal	5	1	1	5
5	Aquisição de cabos de qualidade	5	1	1	5
6	Executar o teste do compontente	5	1	1	5
8	Teste do componente	5	1	1	5
13	Teste de envio dos dados	5	1	1	5
14	Adequação do ambiente para o uso do equipamento	5	1	2	10
15	Alarme ou led para baixa energia	5	3	1	15
16	Alarme ou led para baixa energia	5	2	1	10
1	Capacitar o operador	5	2	3	30
2	Manutenção ou troca dos eletrodos	5	2	1	10
11	Executar teste e validação da programação	5	2	2	20
12	Monitoramento Eletrico	5	2	1	10
17	Teste do software	5	2	2	20
18	Teste do software	5	2	1	10
19	Teste do software	5	2	1	10
7	Revisão do projeto	5	1	3	15
9	Revisão do projeto	5	2	3	30
3	Prover um ambiente sem interferências eletromagnéticas	5	2	3	30
4	Capacitar o operador	5	3	2	30

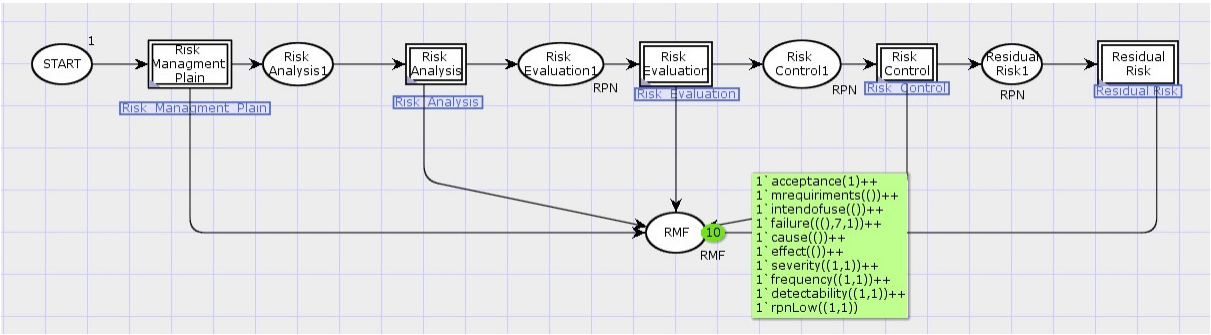
Fonte: elaborada pelo autor

Figura 32 – Ilustração da marcação *[27]* na rede de mais alto nível no modelo hierárquico



Fonte: Elaborada pelo autor

Figura 33 – Ilustração da marcação *[15]* na rede de mais alto nível no modelo hierárquico



Fonte: Elaborada pelo autor

A.1 Variáveis e funções

```
(* Standard priorities *)
     val P_HIGH = 100;
     val P_NORMAL = 1000;
     val P_LOW = 10000;
(* Standard declarations *)
     colset UNIT = unit;
     colset BOOL = bool;
     colset INT = int;
     var requiriments : UNIT;
     var equip : UNIT;
     colset RiskLimit = int with 25..30;
     colset FAILACOUNT = int with 1..7;
     fun fails()=FAILACOUNT.ran();
     colset FAILORIG = int with 0..2;
     colset BLOCKS = product UNIT * INT;
     colset BLOCKSAMOUNT = int with 1..7;
     fun blocks() = BLOCKSAMOUNT.ran();
     var blockT : BLOCKSAMOUNT;
```

```
     fun signalr() = FAILORIG.ran();
     colset DESCR = product UNIT * INT * INT;
     colset FAILURE = product UNIT * INT;
     colset RISKID = INT;
     var dataA : FAILORIG;
     var literA : FAILORIG;
     var brainA : FAILORIG;
     var pastA : FAILORIG;
     fun sum(R1,R2,R3,R4)= R1+R2+R3+R4;
     var limit : RiskLimit;
     var failureT : INT;
     var riskE : INT;
     var riskId : INT;
     var caus : UNIT;
     var effec : UNIT;
     colset PSEVERITY = int with 1..5;
     colset RISKINF = product INT * INT;
     colset SEVERITY = product RISKID * PSEVERITY;
     var sevValue: PSEVERITY;
     colset PFREQUENC =  int with 1..5;
     var freqValue : PFREQUENC;
     colset FREQUENC = product RISKID * PSEVERITY * PFREQUENC;
     colset PDETECTABILITY = int with 1..5;
     var detValue : PDETECTABILITY;
     colset DETECTABILITY = product RISKID * PSEVERITY * PFREQUENC* PDETECTABILITY;
     colset RPN = product INT * INT;
     var rpnValue : INT;
     fun Mult(R1,R2,R3) = R1 * R2 * R3;
     colset RMF = union  acceptance:INT + mrequiriments:UNIT + intendofuse:UNIT +
failure:DESCR + cause:UNIT + effect:UNIT + severity:RISKINF +
 frequency:RISKINF + detectability:RISKINF + rpnLow:RPN +
rpnHigh : RPN + residual:RISKID;
     fun signal() = PSEVERITY.ran();
     fun signal2() = PFREQUENC.ran();
     fun signal3() = PDETECTABILITY.ran();
```