UNIVERSIDADE ESTADUAL DA PARAÍBA
PRÓ-REITORIA DE PÓS-GRADUAÇÃO E PESQUISA
MESTRADO PROFISSIONAL EM CIÊNCIA E TECNOLOGIA EM SAÚDE

RAPHAEL MENDONÇA DA NÓBREGA

UM MODELO DE DECOMPOSIÇÃO DE REQUISITOS DE SEGURANÇA PARA PROJETOS NA INDÚSTRIA DE DISPOSITIVOS MÉDICOS

CAMPINA GRANDE
2016

RAPHAEL MENDONÇA DA NÓBREGA

UM MODELO DE DECOMPOSIÇÃO DE REQUISITOS DE SEGURANÇA PARA PROJETOS NA INDÚSTRIA DE DISPOSITIVOS MÉDICOS

Dissertação de Mestrado submetido à banca de avaliação do Programa de Pós-Graduação em Ciência e Tecnologia em Saúde da Universidade Estadual da Paraíba

Orientador: Prof. Dr. Paulo Eduardo e Silva Barbosa
Co-Orientador: Prof. Dr. Pablo Oliveira Antonino

CAMPINA GRANDE
2016

N337m Nóbrega, Raphael Mendonça da.
Um modelo de decomposição de requisitos de segurança para projetos na indústria de dispositivos médicos [manuscrito] / Raphael Mendonça da Nóbrega. - 2016.
69 p. : il. color.

Digitado.
Dissertação (Mestrado Profissional em Ciência e Tecnologia em Saúde) - Universidade Estadual da Paraíba, Pró-Reitoria de Pós-Graduação e Pesquisa, 2016.
"Orientação: Prof. Dr. Paulo Eduardo e Silva Barbosa, Pró-Reitoria de Pós-Graduação e Pesquisa".

1. Rastreabilidade. 2. Dispositivos médicos. 3. Safety. 4. Controle de riscos. 5. Software. I. Título.

21. ed. CDD 005.3

RAPHAEL MENDONÇA DA NÓBREGA

UM MODELO DE DECOMPOSIÇÃO DE REQUISITOS DE SEGURANÇA PARA PROJETOS NA INDÚSTRIA DE DISPOSITIVOS MÉDICOS

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Ciência e Tecnologia em Saúde da Universidade Estadual da Paraíba, como requisito para obtenção título de Mestre.

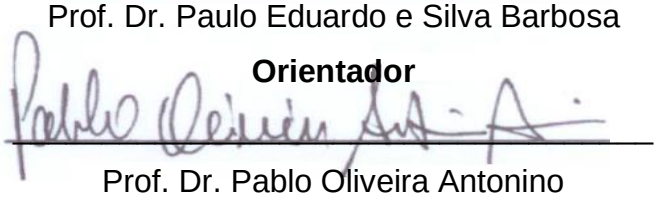
Área de concentração: Medicina 1

Aprovada em: 30/03/2016

BANCA EXAMINADORA:

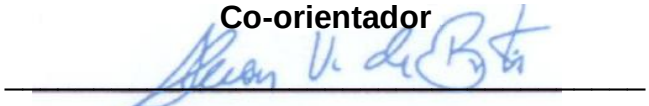
Prof. Dr. Paulo Eduardo e Silva Barbosa

Orientador



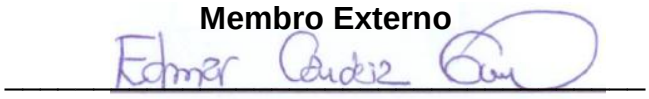
Prof. Dr. Pablo Oliveira Antonino

Co-orientador



Prof. Dr. Alisson Vasconcelos de Brito

Membro Externo



Prof. Dr. Edmar Candeia Gurjão

Membro Externo

RESUMO

Para a indústria de desenvolvimento de dispositivos médicos, produzir produtos com qualidade e segurança é o principal desafio na tentativa de evitar sérios danos ao paciente, operador ou ao ambiente. Por conta disto, os engenheiros envolvidos no processo de desenvolvimento precisam cada vez mais se comprometer com técnicas eficientes de análise, projeto e implementação de forma consistente para ter dispositivos mais confiáveis. Atualmente, indústria e academia têm fornecido evidencias que falhas de rastreabilidade entre os elementos de projeto deste tipo estão entre as principais causas de: (i) não certificação de dispositivos *safety-critical*, e (ii) falhas catastróficas. Infelizmente os engenheiros tem utilizado abordagens de rastreabilidade sem planejamento. Na prática, manter o rastro entre elementos é uma tarefa árdua, pois requisitos podem mudar e tipos de elementos podem ser diferentes tornando um projeto uma mistura de tipos de elementos. Neste trabalho, propomos estender o trabalho de Antonino e Trapp – *Improving Consistency Checks Between Safety Concepts and View Based Architecture Design* – desenvolvendo um modelo de decomposição de requisitos de *safety* com foco na indústria de dispositivos médicos, onde, adicionamos mais um nível, que representará uma análise prévia de riscos, prevista pelas normas reguladoras desta indústria (como a ISO 14971:2007 e a IEC 62304:2006), até elementos arquiteturais do sistema. Para dar suporte a este modelo, apresentamos uma ferramenta como extensão ao *Enterprise Architect* que cuida de fazer verificações no intuito de garantir que os mesmos seguiram as preocupações inerentes ao modelo de decomposição apresentado. É uma pesquisa de natureza exploratória, que está sendo desenvolvida no Núcleo de Tecnologias Estratégicas em Saúde – NUTES, em colaboração com o instituto Fraunhofer-IESE.

Palavras Chave: Rastreabilidade, Decomposição, Requisitos, TIM, Safety, Regulamentação.

ABSTRACT

Towards the development of medical device's industry, making products with quality and safety is the main goal in an attempt to avoid serious harms to the patient, operator or environment. For this reason, engineers involved on development process need increasingly commitment with efficient analysis techniques, projects and deployments in a consistent way to have reliable devices. Nowadays, industry and academics have been providing evidences that traceability between elements of projects are one of the main causes of: (i) non-certification of safety-critical devices, and (ii) catastrophic failures. Unfortunately, engineers have been using traceability approaches without planning. In practice, maintaining traceability between elements is a difficult task, as requirements can change and types of elements can be different, turning a project into a mixture of types of elements. Thus, maintaining traceability is a big challenge. In this work, it is proposed an extension of Antonino and Trapp's work – *Improving Consistency Checks Between Safety Concepts and View Based Architecture Design* – making a safety requirement decomposition model focused on a medical devices' industry, in which it was added one more level to represent a prior risk analysis, expected for the regulation standards of this industry (such as ISO 14971:2007 and the IEC 62304:2006), up to system architectural elements. In addition to that, it was presented an Enterprise Architect add-in that will perform model verifications in order to assure that the concerns of the model decomposition will be followed. This is an explored research, which has been developed at the Center for Strategic Technologies in Health with a Fraunhofer-IESE's collaboration.

Key-Words: Traceabilty, Decomposition, Requirements, TIM, Safety, Regulation.

LISTA DE TABELAS

LISTA DE ABREVIATURAS

ADFSA – Add-in For Safety Assurance

ASIL – Automotive Safety Integrity Level

DEA – Desfibrilador Externo Automático

EA – Enterprise Architect

EA – Event Analysis

ECG – Eletrocardiograma

FAA – Federal Aviation Administration

FTA – Fault Tree Analysis

GSN – Goal Structured Notation

IEC – International Eletrotechnical Commission

ISO – International Organization for Standardization

NCP – N-Copy Programming

NSCP – N Self-Checking Programming

NUTES – Núcleo de Tecnologias Estratégicas em Saúde

NVP – N-Version Programming

RcB – Recovery Blocks

RtB – Retry Block

SCT – Safety Concept Trees

SysML – Systems Modeling Language

TIM – Traceability Information Model

TIR – Technical Information Report

UI – User Interface

UML – Unified Modeling Language

UEPB – Universidade Estadual da Paraíba

UFCG – Universidade Federal de Campina Grande

SUMÁRIO

1. INTRODUÇÃO

Os sistemas *safety-critical* são aqueles que, em caso de falha, resultam em danos severos e até em morte de pessoas ou, prejudicam o ambiente em que estão inseridos [1]. É crucial identificar, entender e tratar acidentes, perigos e riscos neste tipo de sistema com o objetivo de evitar perdas humanas, ambientais, capitais ou materiais. Estas atividades consistem na necessidade de identificar o perigo, a sua natureza, o relacionamento com os acidentes e o efeito sobre o projeto do sistema. Tendo o risco como uma relação entre a probabilidade de um acidente acontecer e a severidade do dano, esta relação deve ser avaliada no intuito de concluir a aceitabilidade do perigo [2].

Diversos dispositivos médicos executam funções críticas para a manutenção da vida humana. Logo, diversos dispositivos médicos encontram-se classificados como sistemas *safety-critical.* A bomba de infusão, por exemplo, é um dispositivo médico que injeta uma quantidade pré-determinada de fluídos, como, drogas e nutrientes [3]. A aplicação desta atividade de forma manual é bastante complexa, pois é preciso considerar o controle do tempo de entrega do fluído, volume, pressão, entre outros parâmetros, e uma falha nesta entrega de fluídos pode resultar em sérios danos ao paciente [3].

Fabricantes e agências reguladoras, motivados por essa criticidade, buscam formas de evitar que equipamentos médicos sejam fontes de perigos. Eles tendem a projetar e implementar os equipamentos buscando sempre atingir alguns atributos de qualidade, dentre eles, o atributo de *safety* (segurança). Por sua vez, as agências reguladoras desenvolveram normas com recomendações a serem tomadas no desenvolvimento de dispositivos médicos [4]. A interação entre eles se dá pela exigência das normas reguladoras, de que os fabricantes devem fornecer documentos que evidenciem as medidas tomadas para a mitigação dos riscos associados ao produto [5]. Em geral, essas recomendações normativas conduzem bem as especificações de requisitos, design, implementação, testes e, de forma menos precisa, aspectos do processo de desenvolvimento, dentre eles a rastreabilidade de requisitos, processo que mostra o rastro entre requisitos de sistemas a estruturas arquiteturais [6].

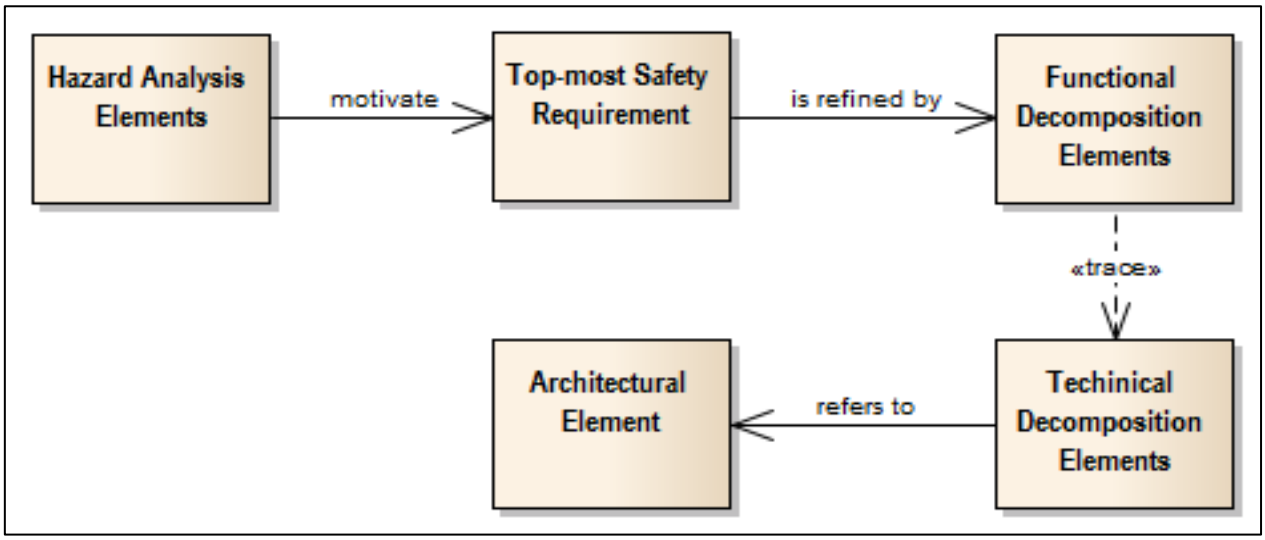
Não planejar a rastreabilidade em projetos de dispositivos médicos torna a atividade de criar a relação entre requisitos do sistema e artefatos arquiteturais uma tarefa difícil e quase impossível de se manter [7]. Esta atividade envolve verificar o rastro entre os requisitos determinados pelos *stakeholders* e/ou sistema e um determinado projeto requerido [8].

Atualmente, indústria e academia tem provido evidencias de que a falta de preocupação com a rastreabilidade é uma das principais causas da: (i) não-certificação de sistemas *safety-critical*; e (ii) falhas catastróficas [9]. Como contribuição para evitar estes tipos de problemas, Antonino e Trapp [9] estabeleceram um *Traceability Information Model (TIM)* que guia a decomposição de elementos de *safety* em projetos da indústria automotiva, adicionando conceitos da ISO 26262 [10]. Este tipo de modelo, TIM, é atualmente um dos principais focos dos pesquisadores no tocante a definir estratégias de gerencia de rastreabilidade [11].

Contudo, alguns aspectos propostos por eles não são adequados à indústria de equipamentos médicos, como, por exemplo, os ASIL *(Automotive Safety Integrity Level)* que são classificações de níveis integridade de *safety* dadas a elementos de projetos específicos para o contexto automotivo. Por sua vez, a norma IEC 62304 [12], que trata do processo de desenvolvimento de softwares na área médica, requer dos fabricantes uma classificação de *safety* específica, chamada, *Software Safety Class*.

Outros elementos importantes para a indústria médica, como, a descrição do uso pretendido do equipamento requerido pela ISO 14971 [5], também, não aparece no TIM proposto por Antonino e Trapp [9]. Desta forma, este trabalho propõe uma nova versão do trabalho de Antonino e Trapp focando na indústria de dispositivos médicos, apresentando uma forma de planejar e manter a rastreabilidade entre elementos de projetos de sistemas *safety-critical* na indústria de equipamentos médicos. A Figura 1 apresenta uma visão geral de como está estruturado o TIM proposto.

Figura 1- Visão Geral do TIM



Fonte: O autor

O elemento *Hazard Analysis Elements* representa, em um nível contextual, a análise de riscos que deve ser previamente elaborada, indicando, quais os perigos que precisam ser mitigados, exigência da ISO 14971 [5]. Destaco que a representação do *Hazard Analysis Elements* estende ao trabalho proposto por Antonino e Trapp. O elemento *Top-most Safety Requirement,* trata-se do principal requisito de *safety* elucidado para mitigação de um risco. É dele que partirá a decomposição representativa e detalhada da argumentação para mitigação do um perigo presente na *Hazard Analysis Elements*. Os elementos *Functional Decomposition Elements* e *Technical Decomposition Elements,* representam os requisitos de *safety* decompostos*,* a citar: as causas e tipos de falhas, elementos de tolerância (contenção e detecção), sendo, o *Functional Decomposition Elements* a representação dos requisitos funcionais de *safety* e o *Technical Decomposition Elements* em um nível técnico, representando como os componentes do sistema estarão envolvidos na implementação dos requisitos funcionais de *safety*. O menor item da granularidade desta decomposição é o componente arquitetural do sistema atuante na mitigação do risco, identificado na Figura 1 como *Architectural Element*, que trata de representar, por exemplo, um atuador, um alarme, um componente de software, dentre outros.

Adicionalmente, este trabalho propõe um suporte ferramental para rastrear requisitos de *safety* a modelos arquiteturais e modelos de *safety*. Este ponto é

importante, pois, a literatura tem discutido que abordagens não automatizadas dificilmente poderão ser integradas em ambientes reais de desenvolvimento [7] [13].

Esta dissertação está estruturada como a seguir. O capítulo 2 apresenta as abordagens usadas atualmente para representar argumentações de *safety*. O capítulo 3 descreve nossa abordagem proposta para argumentação de *safety* para industrial de dispositivos médicos. O capítulo 4 apresenta uma ferramenta de suporte à modelagem na decomposição de requisitos de *safety,* adicionado a isto, ainda no mesmo capítulo, apresento uma instanciação de um projeto de um desfibrilador automático externo (DEA) usando o TIM proposto. O capítulo 5 apresenta a metodologia empregada. Por fim, no capítulo 6 temos as conclusões e os principais desdobramentos do trabalho.

2. TRABALHOS RELACIONADOS

Podemos definir *safety* como a maneira que buscamos conhecer, entender e e escolher riscos aceitáveis [2]. Garantir *safety* demanda rigorosos processos e métodos controlados a serem atingidos durante o desenvolvimento de qualquer dispositivo *safety-critical* [9].

Técnicas que se caracterizam como uma tentativa de argumentar documentando as medidas protetivas em um projeto de sistemas são tidas como técnicas de argumentação de *safety* ou *safety argumentation*. Na prática, essa argumentação é feita através de documentos, planilhas, tabelas, diagramas e matrizes [9].

Quando bem escrito, argumentar *safety* em texto livre pode ser uma maneira rápida e usual, porém, na prática, esta abordagem tem o grande problema de conseguir com que todas as partes envolvidas no processo tenham o mesmo entendimento da argumentação *safety*. Isto se dá por problemas, como: textos mal escritos por dificuldades com a língua usada na escrita, muitas vezes nem todos os engenheiros tem um bom domínio da língua e podem gerar textos mal estruturados. Além disso, ter muitas referências cruzadas em um texto pode dificultar o entendimento da argumentação tornando difícil enxergar como os elementos do projeto se relacionam [14], como mostra o texto da Figura 2.

Figura 2 - Exemplo ruim de argumentação usando texto livre

> For hazards associated with warnings, the assumptions of [7] Section 3.4 associated with the requirement to present a warning when no equipment failure has occurred are carried forward. In particular, with respect to hazard 17 in section 5.7 [4] that for test operation, operating limits will need to be introduced to protect against the hazard, whilst further data is gathered to determine the extent of the problem.

Fonte - Arguing Safety - A Systematic Approach to Managing Safety Cases *[14]*

Na Tabela 1, temos um exemplo de argumentação de *safety* com o uso de tabelas. Tim Kelly [14], a Tabela 1 para representar uma argumentação de *safety* em

formato de tabela, sendo, a primeira coluna, ***Claim***, representa o objetivo principal a ser atingido com as medidas mitigadoras de falhas, a segunda, ***Argument***, representa uma descrição sucinta de como o objetivo deve ser atingido e, por fim, a última coluna, ***Evidence/Assumptions*** temos as evidências ou avaliações que provam a argumentação da segunda coluna. Kelly mostra que esta forma pode substituir bem a forma de texto livre traçando claramente as partes de uma argumentação. O problema é que a tabela pode limitar os passos de uma decomposição, que são 2: ***claim -> argument*** e ***argument->evidence***, a necessidade de argumentações mais complexas pode exigir uma decomposição destes ***claims*** ou força com que os ***arguments*** precisem se comunicar com outras estruturas de argumentação (outras tabelas). Isto pode dificultar o entendimento do fluxo da argumentação, principalmente quando é preciso um nível de granularidade alto para representar uma decomposição de argumentos em níveis mais baixos gerando uma quantidade alta de tabelas.

Tabela 1 - Argumentação de safety com uso de tabelas

Claim	**Argument**	**Evidence / Assumptions**
There is no fault in the software implementation	Formal proof of specified safety properties Formal proof that code implements its specification	The design is simple enough to be amenable to proof Proof tool is correct (or unlikely to make a compensating error) Compiler generates correct code (sub-argument might use formal proof, past experience, or compiler certification High quality V&V process ***Test results***
Software reliability exceeds system requirement	Reliability can be assessed under simulated operational conditions	***Statistical test results***

Fonte - Arguing Safety - A Systematic Approach to Managing Safety Cases [14]

Muito usada na engenharia de requisitos, as matrizes de rastreabilidade buscam mostrar os relacionamentos entre os requisitos do sistema [15] e elementos do sistema. Tim Kelly [14] menciona que esta técnica pode ser usada para argumentar safety evidenciando como requisitos de *safety* se relacionam com outros requisitos do sistema e/ou elementos do sistema. A Figura 3, mostra um exemplo de uma matriz de rastreabilidade. O problema desta abordagem é que só é possível representar uma camada de decomposição de argumentação de *safety* por vez e muitas vezes é preciso representar uma decomposição de argumentação em uma granularidade alta sendo possível não representar os possíveis conflitos em um nível muito baixo [16]. Além disso nas matrizes não é possível descrever as explicações e justificativas entre os relacionamentos apresentados.

Na tentativa de desenvolver uma forma de argumentação de *safety* que unisse a forma descritiva juntamente com a versatilidade de rastrear os

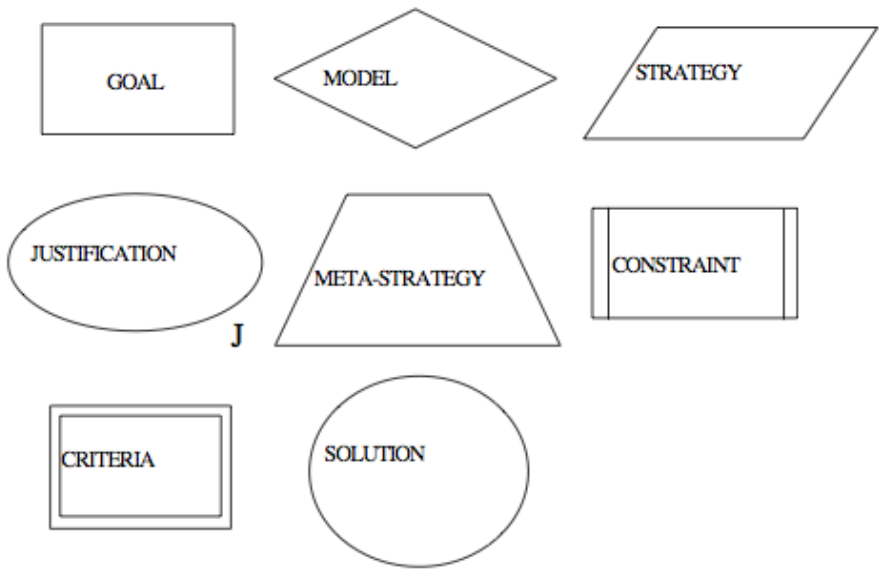
elementos que representam as decisões protetivas, Tim Kelly [14] apresentou a opção de utilizar a *Goal Structuring Notation* (GSN), que trata de uma abordagem gráfica representativa de uma de argumentação de safety.

Figura 3 - Matriz de rastreabilidade como forma de argumentação de safety

Design Feature	**Requirement**									
	TRIP	**PFD**	**STR**	**TIM**	**FIX**	**TST**	**F1**	**F2**	**UPD**	**SEC**
Redundant channels and thermocouples		■	■			■	■	■	■	
Fail-safe design features		■		■	■			■		■
Separate Monitor Computer					■	■				■
Design Simplicity	■			■						■
Formally Proved Software	■	■	■							

Fonte - Arguing Safety - A Systematic Approach to Managing Safety Cases [14]

Figura 4 – Elementos do GSN



Fonte - Arguing Safety - A Systematic Approach to Managing Safety Cases [14]

A Figura 4, mostra os elementos principais de uma estrutura montada usando GSN. Observamos que a argumentação parte de um objetivo principal até a solução definida, passando pela definição de estratégias, justificativas, restrições dentre outros. O problema é que o GSN não permite uma forma adequada de argumentação estrutural do sistema, ou seja, quando se deseja representar uma argumentação em um nível de arquitetural de sistemas descrevendo como a estrutura do sistema estará disposta a compreender o requisito de *safety* elucidado.

Tentativas de definir como criar argumentações mais estruturadas tem surgido no âmbito de pesquisas. Habli et al [17], é um exemplo, onde identificou como a rastreabilidade de casos de *safety*, definidas em GSN, unido a uma representação arquitetural em SysML, pode prover uma representatividade desta argumentação estrutural. Domis et al. [16] definiu as *Safety Concepts Trees (SCTs)*, modelagem que decompõe objetivos de *safety* em requisitos de *safety* mais detalhados, ou seja, partindo de níveis de requisitos mais analíticos (alto nível) refinando-os usando portas lógicas típicas como '*and*' e '*or*' a requisitos de *safety* mais apurados. O problema é que esta abordagem não contempla elementos da arquitetura que compõem estes requisitos tendo seu conteúdo voltado para representar apenas o domínio. Semelhante a esta abordagem, mas com foco na indústria automotiva, Birch et al. [18] mostra como argumentos de *safety* podem ser logicamente decompostos usando GSN. A abordagem basicamente propõe como usar a justificativa do GSN como um requisito de *safety*, porém esta argumentação não considera descrever os elementos estruturais de forma precisa não dando base suficiente para a existência destes requisitos de *safety*. Causas de falhas e modos de falhas também não são possíveis de identificar usando este modelo.

Denney e Pai [19], apresenta um padrão automatizado de instanciação de argumentos de casos de *safety* focada na decomposição de estrutura destes casos deixando a desejar na decomposição de requisitos de *safety*.

Na tentativa de garantir um bom projeto de um sistema *safety-critical,* engenheiros usam técnicas como: *Fault Tree Analysis (FTA)*, *Event Analysis (EA)*, entre outras, para avaliar as possibilidades de falhas de um sistema deste gênero [7]. Porém FTA e EA não são técnicas apropriadas para verificação do relacionamento entre artefatos em tempo de design de projeto, técnicas de gerenciamento de rastreabilidade geralmente são mais indicadas. Como prova disto,

temos que agências reguladoras, nas mais diversas áreas, requerem o gerenciamento de rastreabilidade como atividade essencial no processo de desenvolvimento [11].

Com foco no gerenciamento da rastreabilidade entre artefatos de um projeto, a norma FAA DO-178c [20], da indústria aviônica, provê diretrizes de rastreabilidade que verificam a ausência de conexões entre artefatos de um código-fonte de um programa e requisitos de baixo nível. Outra estratégia com foco no gerenciamento da rastreabilidade é usada por pesquisadores, e tem como objetivo prover uma boa formalização da rastreabilidade, usando um modelo de referência de rastreabilidade que deriva da *analysis queries* e padroniza os tipos de artefatos e seus tipos de links [11], entretanto nenhuma destas duas técnicas tem diretrizes próprias para a indústria médica.

3. TIM PARA DECOMPOSIÇÃO DE REQUISITOS DE SEGURANÇA PARA INDÚSTRIA DE DISPOSITIVOS MÉDICOS

Nesta seção, entenderemos como o modelo proposto neste trabalho busca argumentar e representar visualmente em forma de modelagem medidas protetivas em um nível estruturado, considerando desde a análise de riscos previamente feita até o elemento arquitetural envolvido, com foco na indústria de dispositivos médicos.

A rastreabilidade entre os artefatos de desenvolvimento é uma propriedade importante no suporte à descrição do relacionamento entre os elementos de um projeto, inclusive no tocante às dependências entre os elementos, refinamentos, especializações, dentre outros tipos de relacionamentos [21].

A definição prévia e aprovação da rastreabilidade em projetos de dispositivos *safety-critical* deve ser prioritária e não deve surgir durante o processo de desenvolvimento [11]. Abordagens irregulares de rastreabilidade tem se mostrado difíceis de implementar e quase impossíveis de manter [7].

Contudo, criar e manter esses relacionamentos sempre coerentes pode ser um trabalho árduo e falhas na rastreabilidade podem onerar muito o projeto. Na prática tem-se percebido que engenheiros tem adotado abordagens de rastreabilidade sem planejamento, quando as boas práticas indicam que o ideal é ter uma estratégia planejada, ignorar isto pode dificultar a implementação, manutenção avaliação de um projeto [7].

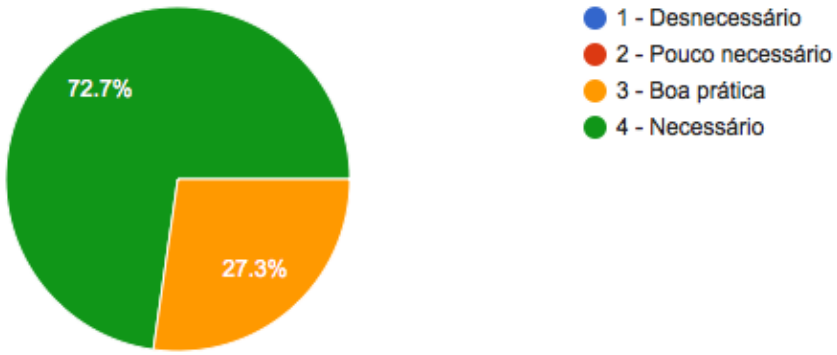
Antonino e Trapp [9] consideram que, na tentativa de garantir *safety* em projetos de sistemas automotivos complexos, pelo menos, dois problemas são comuns: (i) em tempo de desenvolvimento, os requisitos podem mudar todo o processo e (ii) é necessário considerar a diversidade dos diferentes artefatos. O primeiro problema remete à manutenção do projeto e o segundo à avaliação do mesmo.

A ISO 14971 indica que toda atividade de gerenciamento de risco deve ser previamente planejada [5]. Referindo-se, especificamente, ao planejamento do software embarcado em dispositivos médicos ou software como dispositivo médico a IEC 62304 [12], indica, no item 5.1.1 – *Software development plan,* que o planejamento da rastreabilidade entre os requisitos de sistema, requisitos de

software, testes e a implementação em software de suas medidas de controle de riscos devem ser planejadas e documentadas.

Em uma pesquisa interna feita no âmbito do NUTES, envolvendo 22 pessoas dentre elas engenheiros de software, engenheiros eletricistas e estudantes de computação e engenharia elétrica, identificamos que 72,7% dos entrevistados entendem que é necessário apresentar elementos de normas reguladoras na documentação arquitetural do dispositivo médico e 27.3% acreditam que isso é uma boa prática. A figura 5 mostra o gráfico obtido na pesquisa. Destacamos que todas as questões e resultados desta pesquisa interna podem ser conferidos no Apêndice A.

Figura 5 - Necessidade de elementos de normas reguladoras na documentação arquitetural

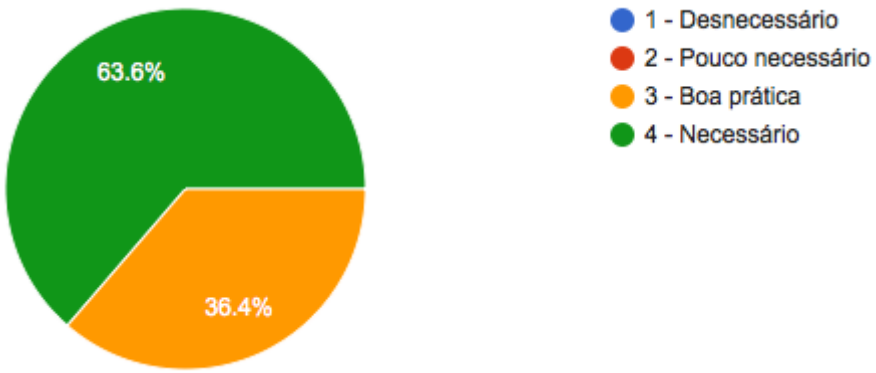


Fonte: O Autor

No entanto, definir e documentar a estratégia de rastreabilidade em projetos como este ajudam a mitigar problemas inerentes à definição, a citar: má avaliação dos elementos do projeto e dificuldade de manutenção. Ter essa definição prévia pode ajudar a demonstrar a disposição dos sistemas em termos de segurança e *safety* [7], conduzindo os engenheiros detectarem quais artefatos do projeto estão conectados a artefatos de *safety* indicando assim os itens *safety-critical.*

Voltando à pesquisa interna feita no âmbito do NUTES (ver Apêndice A), também, identificamos que 63,6% dos entrevistados entendem que é necessário ter um modelo para guiar o planejamento da rastreabilidade entre requisitos de *safety* e elementos arquiteturais do sistema, outro 36,4% entendem que isso é uma boa prática como podemos conferir na Figura 6.

Figura 6 - Necessidade de modelo para guiar o planejamento da rastreabilidade entre requisitos e elementos arquiteturais

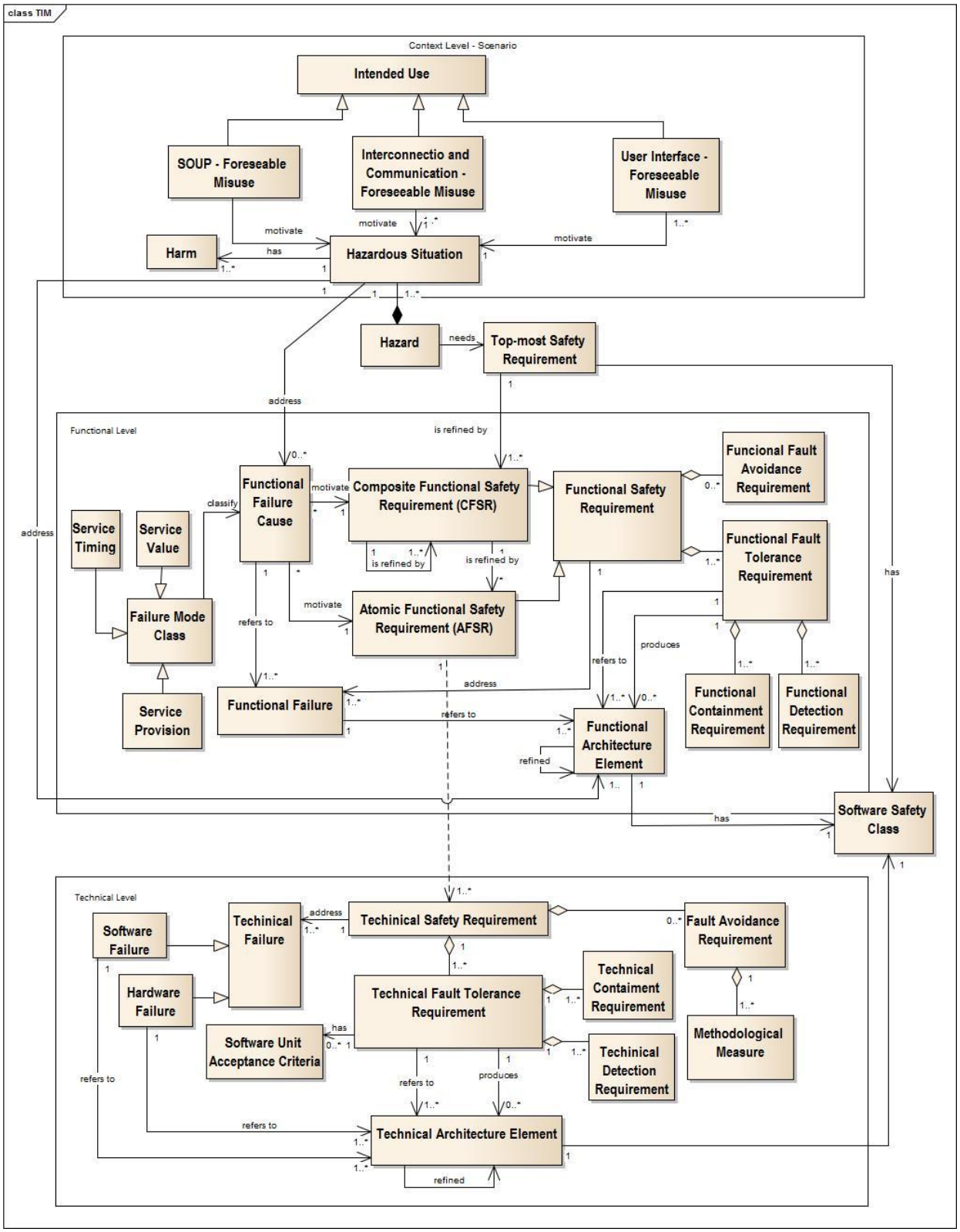


Fonte: O Autor

A elaboração de um *Traceability Information Model* (TIM) é uma abordagem com foco no gerenciamento da rastreabilidade e usada por projetistas nas fases preliminares do desenvolvimento de um projeto na tentativa de planejar a rastreabilidade [7]. Ele é composto basicamente por artefatos rastreáveis e de relacionamentos entre eles. O TIM, define, também, que tipos de artefatos poderão relacionar-se entre si [21]. O resultado disto é uma abstração do uso pretendido da rastreabilidade em um projeto [8], e pode ser representada, por exemplo, por uma linguagem de modelo gráfico, como o a *Unified Modeling Language* (UML) [21].

Baseado no TIM proposto por Antonino e Trapp [9], mas adaptando-o à indústria de dispositivos médicos, aqui apresentaremos um TIM com elementos direcionados a esta indústria, como mostra a Figura 7. Com elementos baseados em preocupações das principais normas reguladoras para produtos da saúde, este TIM pode servir como artefato documental de evidências comprovando o cumprimento de tais exigências. Além de auxiliar no planejamento da rastreabilidade (boas práticas)

Figura 7 - Traceability Information Model para desenvolvimento de dispositivos médicos



Fonte: O autor

O TIM, proposto neste trabalho, consiste basicamente em três níveis: (I) nível de contexto, contendo artefatos de uma análise de riscos; (II) nível funcional, contendo artefatos que remetem a uma decomposição de requisitos em um nível funcional do sistema e (III) nível técnico, com artefatos que remetem a um nível mais técnico (componentes de software, componentes eletrônicos, dentre outros). A contribuição deste trabalho é a definição do nível de contexto, a integração com nível funcional e técnico (apresentados na Figura 5), além de ferramentas que dão suporte ao engenheiro produzir especificações de acordo com este modelo de decomposição.

Definir este TIM em camadas tem o principal objetivo de permitir representar várias camadas de decomposição de argumentação de *safety,* aumentando assim a capacidade de aumentar a granularidade sem perder o contexto de onde os elementos estão inseridos.

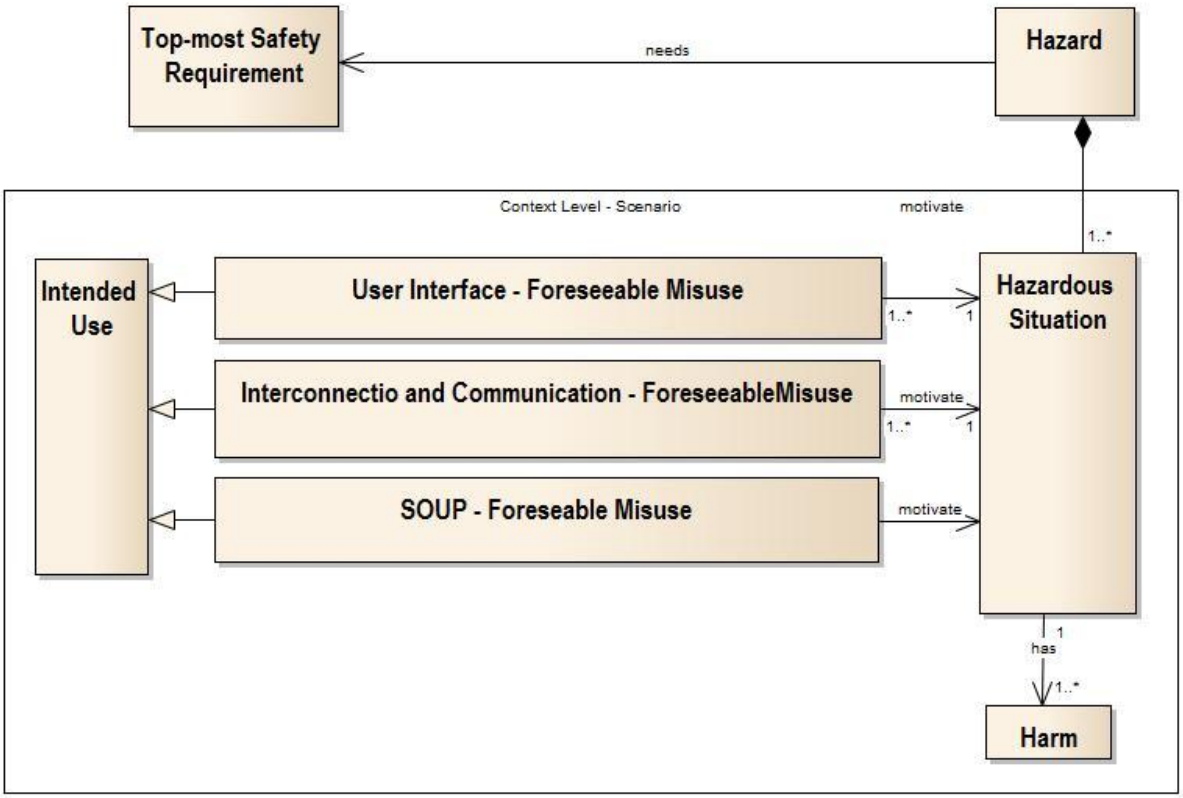
Uma característica fundamental do TIM é a definição dos tipos de relacionamentos entre os elementos [21]. Com esta abordagem é possível definir argumentações de *safety* com um nível maior de complexidade, como, por exemplo, decompor um elemento de alto nível (a citar: um requisito de *safety* global) até o elemento arquitetural do sistema (a citar: um atuador) sem perder sua semântica.

3.1. Nível de contexto – representação da análise de riscos

Ao construir projetos de sistemas *safety-critical* as equipes de desenvolvimento buscam formas rigorosas de análises de riscos para identificar situações perigosas em potencial e quais foram os fatores que contribuíram para isso [7]. Antonino e Trapp [9] em seu trabalho assumiram que esta análise deve ser previamente feita para então ser possível aplicar o TIM. Contudo, para o planejamento do gerenciamento da rastreabilidade ter conformidade com a ISO 14971 [5] é preciso que a análise de riscos seja representada.

Neste TIM, o nível de contexto, principal contribuição deste trabalho, mostrado na Figura 8 (também é possível visualizar este nível na parte superior da Figura 7), representa a análise de riscos previamente elaborada. Nele estão contidos elementos que indicam **uso pretendido, identificação de perigos, possíveis sequências indesejadas de eventos, situações perigosas e danos**.

Figura 8 - Nível de Contexto



Fonte: O autor

Quanto ao **uso pretendido**, a ISO 14971, indica que o fabricante deve documentá-lo, indiciando qual será o principal uso do aparelho e a quem o uso está destinado. Atrelado ao uso pretendido, as **possíveis sequências indesejadas de eventos,** que representam uma sequência de eventos que indicam o mal uso do equipamento devem, também, estar descritas. Também deve ser adicionada a descrição características quantitativas e qualitativas do equipamento que influenciam diretamente na segurança do dispositivo médico, que devem estar sempre presentes na especificação [5].

Descrevemos os elementos do nível de contexto que representam o uso pretendido e as sequências indesejadas de eventos da seguinte forma:

- **Intended Use – Elemento representativo do uso pretendido do dispositivo e todos seus os possíveis mal uso.**
  - **User interface foreseeable misuse** – Representação dos possíveis mal usos relacionados à interface com o usuário. Os problemas representados nestes elementos geralmente ocorrem

devido à complexidade das interfaces com o usuário (UIs) ou motivados pela confiança excessiva do operador no software de evitar situações perigosas.

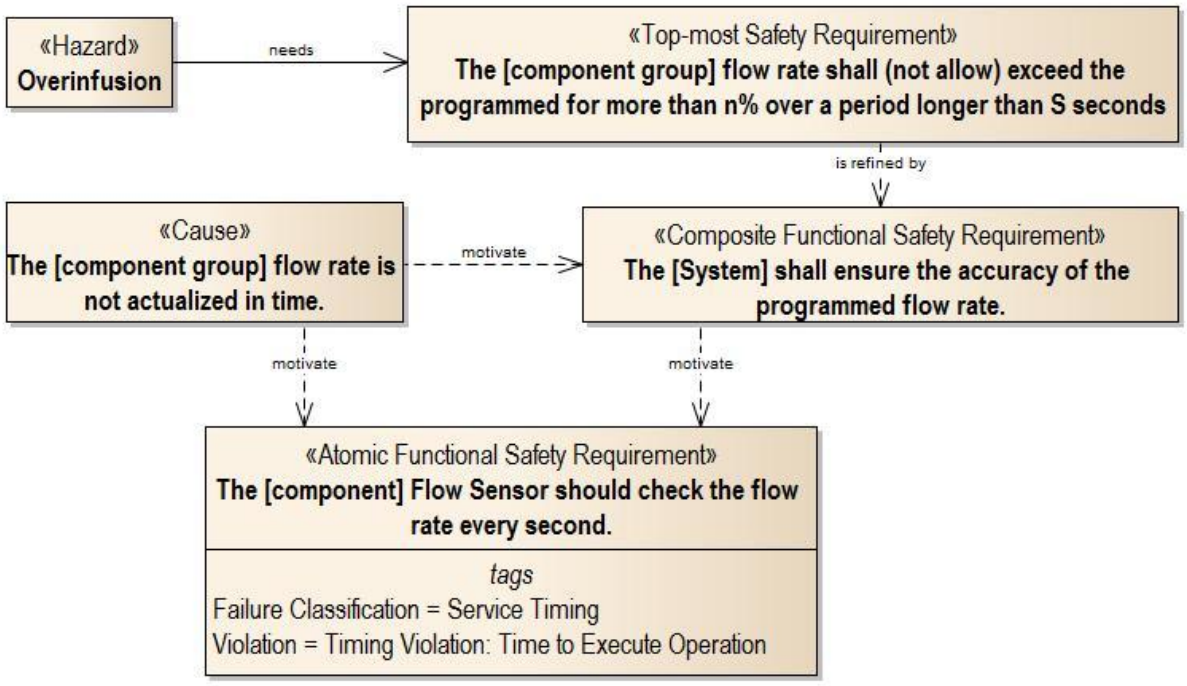
- **Interconnection and communication foreseeable misuse** – Representa os possíveis mal usos de interconexão e/ou comunicação entre os dispositivos médicos e outros sistemas ou outros dispositivos médicos.

Ainda de acordo com a ISO 14971 [5], o fabricante deve levantar uma lista com os possíveis *hazards* em condições normais ou adversas. Os ***hazards*** estão representados neste TIM e são descritos da seguinte forma:

- **Hazard** – Indica um perigo identificado na lista preliminar feita na análise de riscos. Este elemento motivará a criação de um requisito de *safety* a ser decomposto representando uma medida mitigadora do *hazard*.

Os ***hazards*** devem possuir um rastro para o seu elemento mitigador, o *Top-most Safety Requirement* (trataremos deste elemento mais adiante), como mostra a Figura 9.

Figura 9 - Elementos e seus links de interação



Fonte: O autor

Também fundamentais na análise de riscos, as ***hazardous situations*** (situações perigosas) originadas de **possíveis sequências indesejadas de eventos** darão origem aos ***harms*** (danos) [5].

Estes elementos estão justificados da seguinte forma no TIM:

- **Hazardous situations** – Representa as possíveis situações perigosas oriundas de um possível mal uso do equipamento. Estas situações devem ter pelo menos um *hazard* e um *harm* associados.
- **Harm** – Dano oriundo de uma *hazardous situation* identificada. Estes danos podem afetar pacientes, operadores e o ambiente.

3.2. Níveis Funcional e Técnico

Os elementos presentes nestes níveis foram herdados do trabalho produzido por Antonino e Trapp [9] e preservam em grande parte a estrutura original, com algumas mudanças pontuais que serão citadas no decorrer da seção dado os requisitos da indústria médica. A ideia é descrever os elementos com uma

conotação voltada para a indústria de dispositivos médicos tomando como referência as normas reguladoras da área.

Motivado pela existência de um *hazard* elucidado na análise de riscos (representado pelo nível de contexto), o elemento ***Top-most safety requirement*** contém a descrição do objetivo principal a ser alcançado para a mitigação do perigo eminente e é o ponto inicial da decomposição dos demais elementos, organizados em elementos pertencentes a um nível funcional ou a um nível técnico.

O nível funcional, presente na Figura 5, é composto por elementos que representam **O QUÊ** o sistema deve fazer para mitigar o perigo associado. Partindo do ***Top-Most Safety Requirement,*** os **requisitos funcionais de *safety* compostos *(Composite Functional Safety Requirement)*** podem ter associados mais de uma **causa de falha *(functional failure cause)*** sendo refinados até que só exista uma causa de falha associada, sendo descrita no **requisito funcional de *safety* atômico *(Atomic Functional Safety Requirement)***. No nível técnico basicamente representa o **COMO** o sistema resolverá o requisito funcional atômico descrito no nível funcional [9].

Adicionado aos requisitos é colocado uma classificação de severidade de dano, chamado de *Software Safety Class*, definido pela IEC 62304 [12] segue a seguinte classificação:

- Classe A – Livre de ferimento ou danos à saúde
- Classe B – Passível de ferimentos leves à saúde
- Classe C – Passível de morte ou sérios danos à saúde

Os demais elementos, de ambos os níveis, estão relacionados diretamente com técnicas de controle de falhas, como, medidas de detecção de falhas, contenção, prevenção, dentre outros. No intuito de detalhar a importância dessas técnicas, vamos então esclarecer como elas compõem uma descrição de medida de controle de riscos.

3.3. Medida de controle de riscos

Uma medida de controle de risco só é necessária quando uma determinada sequência de eventos contribui para uma situação perigosa que resulte em danos graves e que precisem de uma medida mitigadora para tornar esse dano aceitável.

Então, é possível que existam situações em que não se faz necessária a existência de uma medida de controle de risco [22].

A ISO 14971 [5], no item 6, requer que algumas medidas de controle de riscos sejam tomadas. No item 6.2, a norma coloca alguns pontos importantes de controle de riscos usando análise de artefatos. Uma dessas medidas incluem a análise do projeto como medida protetiva para garantir atingir o atributo de *safety* do dispositivo médico.

Quando faz-se necessário a aplicação de uma medida de controle de riscos esta norma indica que o fabricante deve usar pelo menos uma das opções enumeradas abaixo [5]:

- ***Safety* inerente do projeto;**
- Medidas protetivas do dispositivo médico em si ou no processo de fabricação [1];
- Informação para *safety* [2];.

Como já mencionado anteriormente, este modelo de decomposição tem sua aplicação na especificação do projeto estando diretamente relacionado ao design do projeto tornando-se uma ferramenta importante no controle de riscos inerentes do projeto. Assim usaremos o TIM como maneira de identificar características inseguras ou de mudanças no projeto que podem levar à implementação de forma mais segura contemplando o item de ***Safety* inerente do projeto** presente na ISO 14971 [22].

Uma das principais preocupações em tentar evitar possíveis situações perigosas é prover essa mitigação ainda em tempo de projeto. Portanto, o projeto deve fornecer informações importantes através de uma visão geral do sistema, mostrando como será o comportamento do sistema, como os componentes interagem e outras informações. Mudanças na arquitetura do sistema podem evitar situações perigosas e características desnecessárias. Usar o projeto para definir algumas regras do sistema pode diminuir custos no desenvolvimento e todos esses pontos requeridos pela TIR 80002:2009 [22] podem ser atingidos mais facilmente quando usamos um TIM para guiar a modelagem dos elementos mitigadores.

Quando se trata de mudanças (manutenção) na arquitetura do projeto, significa que teremos mudanças na interação entre os elementos do projeto e a

[1] Para maiores informações sobre esta medida o leitor pode procurar a ISO 14971:2007
[2] Para maiores informações sobre esta medida o leitor pode procurar a ISO 14971:2007

rastreabilidade entre eles pode ser comprometida. O uso do TIM ajuda a manter uma coesão na rastreabilidade entre elementos indicando quais são os tipos de elementos e o tipo de comunicação entre eles.

A decomposição de um elemento mitigador, como, por exemplo, de um requisito de *safety,* guiado pelo TIM, garante que regras do sistema tenham seus modelos sempre descritos usando os mesmos tipos de elementos e com os mesmos tipos de dependências e interações diminuindo as chances de que regras do sistema sejam escritas de formas diferentes ou até mesmo esquecidas. O TIM conduz a uma documentação mais confiável e coesa com as regras do sistema pré-estabelecidas, além disso, converge com o requisito da TIR 80002:2009 que indica que os projetos devem seguir regras pré-estabelecidas buscando evitar anomalias no software.

3.3.1. Definição dos elementos arquiteturais técnicos no controle de riscos

Alguns elementos do nível técnico, Figura 5, descreverão as características requeridas na atividade de controle de riscos, como, por exemplo, o *Technical Safety Requirement* que representará o requisito de caráter técnico, ou seja, representando diretamente elementos de hardware e software necessários para a realização da atividade de um determinado requisito funcional de *safety,* descrevendo neste item os recursos (hardware e/ou software) mínimos necessários para sua realização, tempo necessário de processamento e se ele pode ter interrupções ou interferências de outros itens de *safety*.

Este *Technical Safety Requirement* representa uma falha técnica (*Technical Failure*) que pode ser de software ou hardware. São tidas como falhas quando um serviço entregue é diferente do especificado [23], neste caso a falha está diretamente associada ao elemento técnico de software ou hardware que pode ter o comportamento diferente do esperado. Para representar a entrega do serviço em conformidade ao especificado deve ser definido o requisito técnico de tolerância a falha (*Technical Fault Tolerance Requirement*).

3.3.2. Representação de prevenção de faltas em projetos de software

É importante que o controle de risco tenha a definição de como será feita a prevenção de faltas. Pullum [24] destaca que técnicas de prevenção e fortalecem a confiabilidade do sistema de software quando aplicadas durante o processo de desenvolvimento, reduzindo o número de faltas introduzidas no processo de construção do software.

Discutiremos agora algumas das técnicas que podem ser usadas com essa finalidade, as quais podem ser descritas nos elementos *Functional Fault Avoidance Requirement* e *Technical Fault Avoidance Requirement*. O primeiro terá a descrição da forma usada para livrar o sistema de falhas, o segundo descreve como o primeiro será implementado [9].

Em casos de *Technical Failure*s relacionadas a software, uma forma indicada para evitar falhas, garantindo a confiança no software, é aplicar algumas técnicas de tolerância a faltas. Essas técnicas são projetadas para permitir que sistemas de software sejam tolerantes a determinados tipos de faltas depois de seu desenvolvimento [24]. Pullum descreve 3 técnicas que buscam manter os serviços propostos pelo software em conformidade com o que foi especificado buscando evitar as falhas, as três técnicas propostas por ela são:

- *Single Version Software Environment* – consiste em técnicas de monitoramento, atomicidade de ações, verificação de decisões e manipulação de exceções que irão permitir uma tolerância parcial faltas de projeto de software, sendo a aplicação dessas técnicas indicada a um software de versão única.
- *Multiple Version Software Environment* – técnicas como *Recovery Blocks (RcB), N-version programming (NVP), e N self-checking programmnig (NSCP)*, são aplicadas a projetos de software de múltiplas versões que funcionalmente são equivalentemente independentemente da versão do software.
- *Multiple Data Software Environment* – técnicas aplicadas a um ambiente de grande diversidade de representação de dados utilizando diferentes representações de dados de entrada na tentativa de prover tolerância a faltas nos projetos de software, a citar: *Retry Blocks (RtB) e N-copy programming (NCP)*.

Essas técnicas devem ser descritas em *Technical Fault Tolerance Requirement* de acordo com a parametrização que contem palavras chaves relacionadas a técnicas supra citadas.

3.3.3. Representação da detecção e remoção das faltas em projetos de software

O elemento que representará a forma a ser usada para detecção de faltas é descrito em *Functional Detection Requirement* e a descrição de como este requisito será realizado fica em *Technical Detection Requirement*. A descrição do estado inicial (estado com falha) para o estado final (sem falha) são descritas em *Functional Containment Requirement* e em *Technical Containment Requirement* [9]. Estas técnicas descritas serão aplicadas no momento da validação e verificação do software e geralmente realizadas com testes de software, *formal detection* e *formal design proofs* aumentando a confiabilidade do sistema [24].

Falar em técnicas para remoção de faltas em software, na maioria das vezes, envolve **testes de software**. A descrição de testes de software indicará qual teste deve ser aplicado possibilitando a verificação se será um teste com cobertura suficiente para determinada aplicação e deve derivar de forma apropriada seus atributos de qualidade evidenciando-os. Uma outra ampla forma de tentar-se detectar e remover faltas em software, muito utilizada pela indústria é o ***Formal Design*** [24]**,** que se trata de um rigoroso processo de verificação do código do código fonte em busca de faltas, correção das faltas e verificação da correção.

Por fim e não menos importante forma de detectar e corrigir faltas em software são os ***Formal Design Proofs***, atividade que consiste em aplicar provas matemáticas de corretude em programas de software [24], por exemplo, executando *test cases* é possível melhorar a verificação no processo de software, muitas vezes são técnicas que exigem um alto conhecimento técnico, devido a esta complexidade é preferível aplicar técnicas deste tipo a pequenas porções de software e que quando bem utilizadas tem um grau bastante elevado de confidencialidade e uma baixa probabilidade de ocorrência de faltas em artefatos de software.

O TIM aqui proposto preocupa-se com a descrição destas técnicas a serem aplicadas e com a rastreabilidade para o elemento técnico arquitetural o qual receberá a aplicação destes testes.

4. DESENVOLVIMENTO DE FERRAMENTAL E RESULTADOS PRELIMINARES

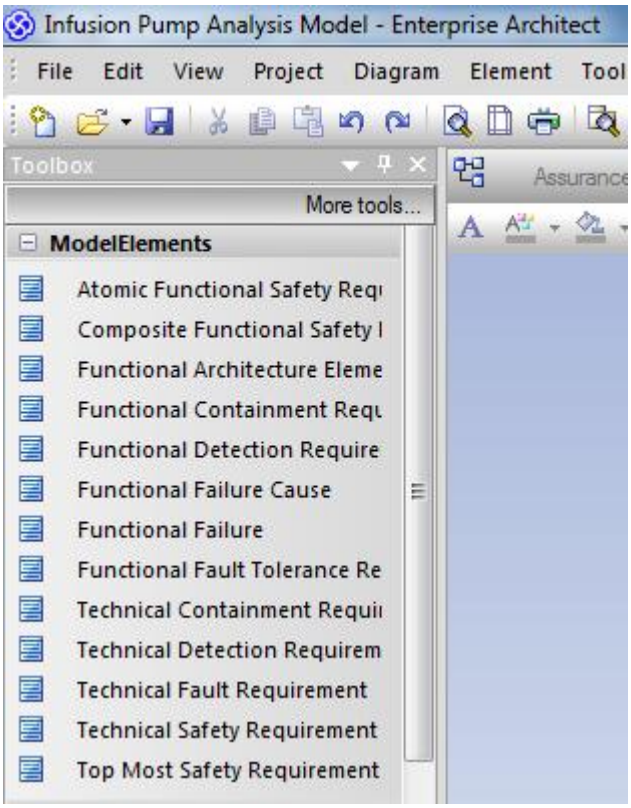
Como mencionado no capítulo anterior, criar e manter rastreabilidade em um projeto de sistemas críticos pode ser um trabalho árduo e consumir muito tempo de desenvolvimento. Mäder et al. [7] menciona algumas ferramentas, como o *Rational DOORs* ou o *Rational RequisitePRO,* que ajudam na manutenção e navegação de rastreabilidade e são intensamente usadas pelas mais diversas indústrias e acrescenta, software como estes possuem funcionalidades que fazem verificações no modelos no intuito de indicar ao usuário formas de montar a rastreabilidade entre os elementos.

Considerando facilitar o uso do modelo de decomposição proposto no capítulo 3 e garantir o desenvolvimento de um projeto seguindo as diretrizes inerentes ao TIM, foi desenvolvido uma ferramenta (*add-in*) para o *Enterprise Architect* (EA) [25] que, atualmente, recebe o nome de *Add-in for Safety Assurance (ADFSA)*. O EA é uma ferramenta de modelagem, visualização e plataforma de *design* de projetos baseada no padrão UML 2.5, que tem sido amplamente utilizada em projetos industriais [26], além disso, o EA é a ferramenta adotada pelo *International Eletrotecnical Commission* (IEC) como ferramenta de modelagem UML [27].

4.1. Caixa de ferramentas do ADFSA

Para facilitar a modelagem utilizando elementos tipados do TIM proposto no capítulo 3, o ADFSA possui uma caixa de ferramentas – toolbox, Figura 10, que se trata de um painel com ícones representando elementos diagramáveis.

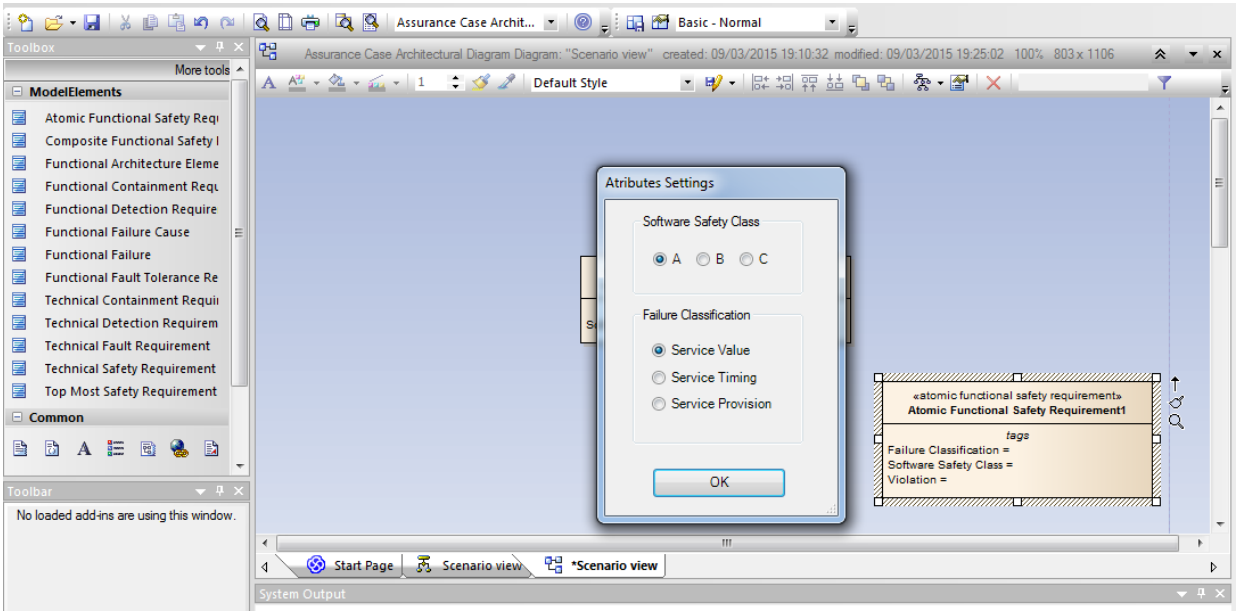
Figura 10 - ADFSA Toolbox



Fonte: O autor

Com esta toolbox é possível arrastar os ícones para a área de desenvolvimento do diagrama e caso o elemento possua alguma configuração obrigatória, será mostrado ao usuário uma janela solicitando a configuração necessária. Um exemplo está na Figura 11, que mostra a necessidade de classificar o elemento *Atomic Functional Safety Requirement* com a *Software Safety Class* correspondente, requisito essencial da ISO/IEC 62304, e o tipo de classificação de falha no momento em que o elemento é posto no diagrama.

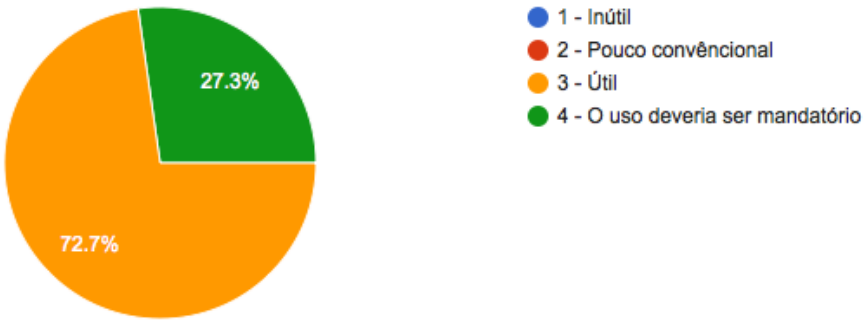
Figura 11 - Configuração de Elementos



Fonte: O autor

No capítulo anterior mencionamos uma pesquisa interna feita no âmbito do NUTES (para mais informações ver Apêndice A), nesta mesma pesquisa coletamos informações dos 22 participantes algumas informações a cerca do uso de ferramentas para auxiliar no gerenciamento da rastreabilidade seguindo os padrões propostos pelo TIM e, no tocante a definição e manutenção de parâmetros dos elementos, informações essas requeridas por normas técnicas, como, por exemplo, *Software Safety Class*, 27,3% dos entrevistados disseram ser útil ter uma ferramenta de valide essas informações durante a criação do diagrama e 72,7% entenderam ser útil, a Figura 12 reflete esse resultado.

Figura 12 - Utilidade de ferramentas automátizadas na gestão de rastreabilidade



Fonte: O autor

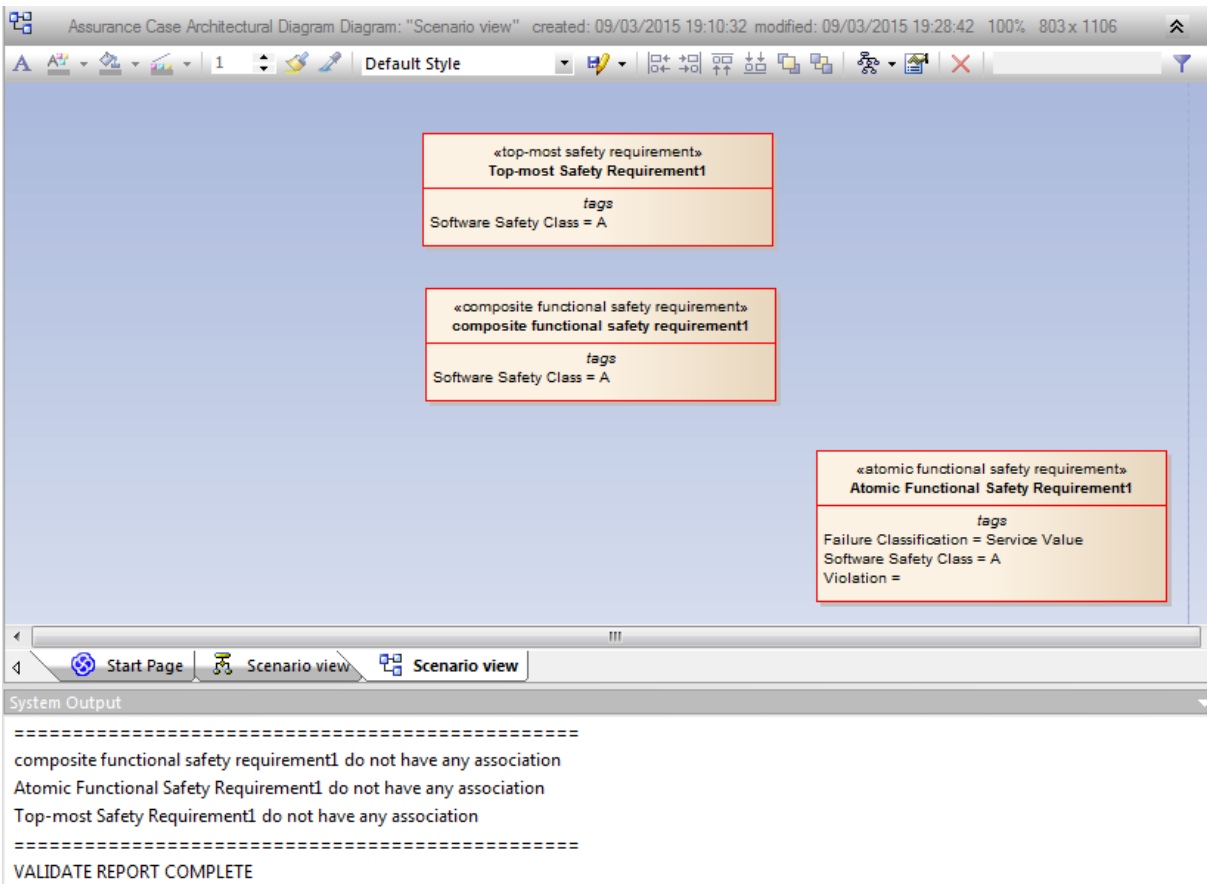
4.2. Validação em tempo de diagramação

O ADFSA faz validações nos diagramas que são montados usando os elementos desta *toolbox*, estas validações acontecerão em tempo de desenvolvimento e seguirão as diretrizes do TIM.

Atualmente são estas as validações do modelo feitas pelo *add-in*:

- Verificar se os elementos do diagrama possuem seus devidos relacionamentos, elementos sem relacionamento ficarão em vermelho, indicando uma irregularidade, além do destaque em vermelho, no *System Output* é mostrado uma lista de inconformidades. A Figura 13 mostra que todo *Top-most Safety Requirement* deve ser refinado a um *Composite Safety Requirement* e consequentemente a um *Atomic Safety Requirement*;

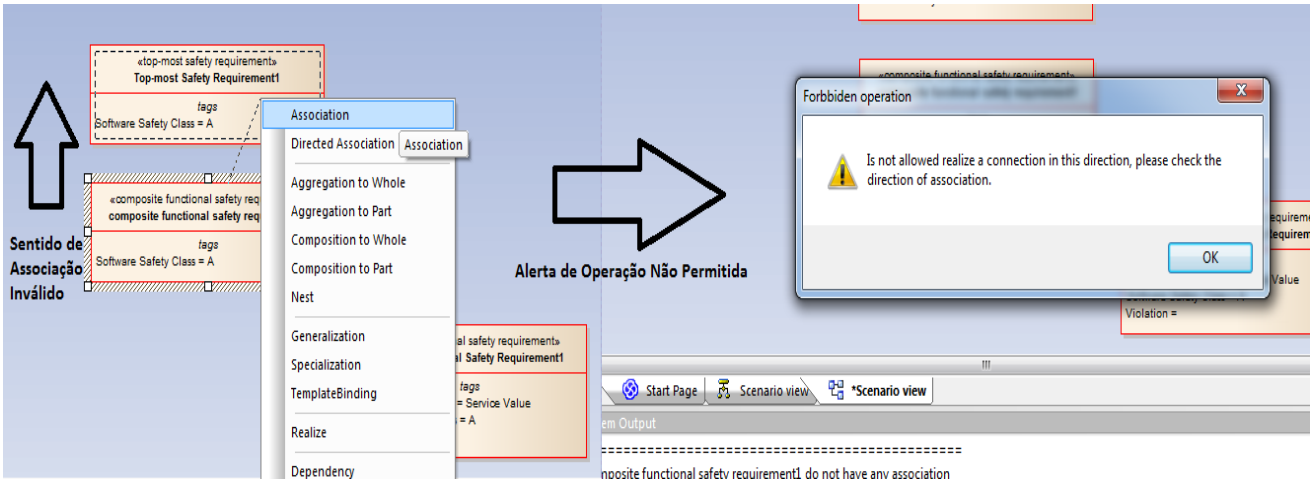
Figura 13 - Verificação de Relacionamentos



Fonte: O autor

- Verificar a direção do relacionamento entre os elementos. A Figura 14 mostra uma tentativa de associar um *Composite Safety Requirement -> Top-Most Safety Requirement* quando esta associação neste sentido não é permitida e sim no sentido contrário;

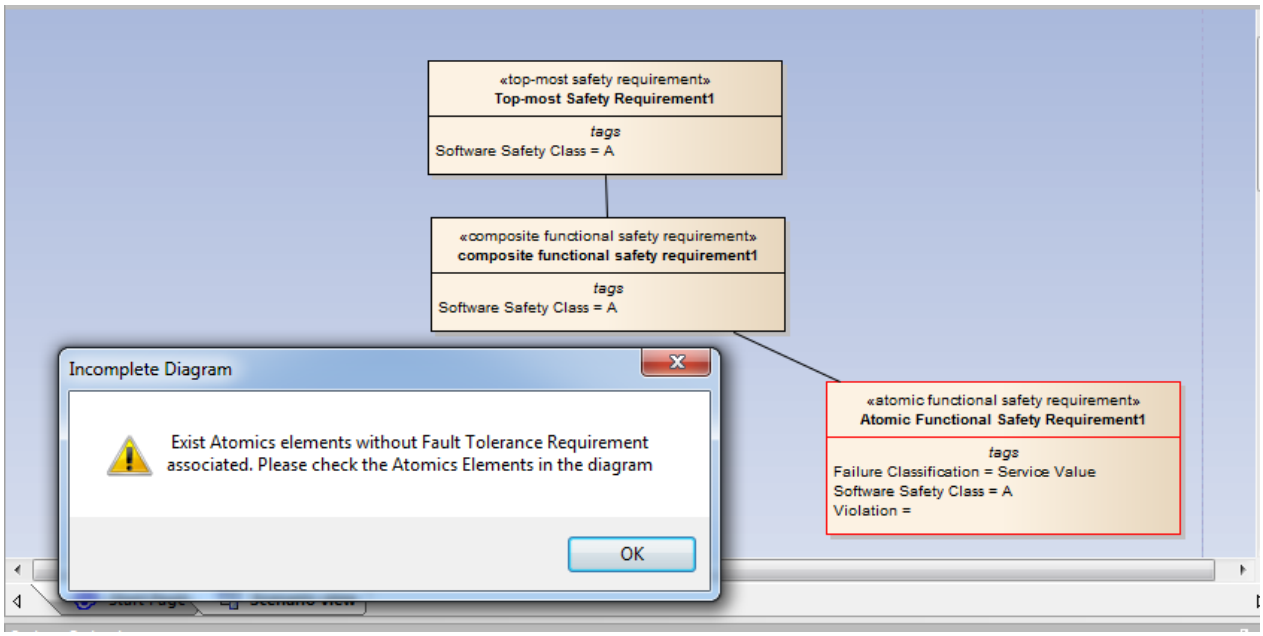
Figura 14 - Relacionamento não Permitido



Fonte: O autor

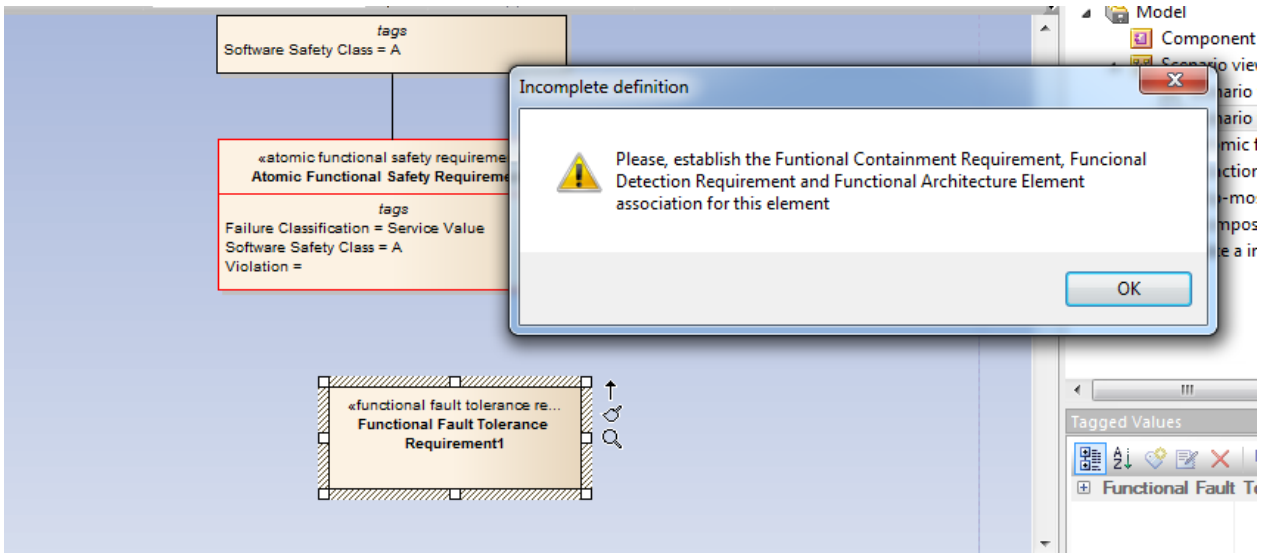
- Ao adicionar elementos ao diagrama que necessitam, obrigatoriamente, de outros elementos associados a eles, uma mensagem indicando essa necessidade é mostrada. A Figura 15 mostra que, ao adicionar um *Atomic Safety Requirement,* outro elemento deve ser adicionado ao diagrama e então associado ao requisito atômico. Outro exemplo é o caso da Figura 16, onde ao adicionar um *Fault Tolerance Safety Requirement* é preciso adicionar e associar a ele um *Functional Containment Requirement*, *Functional Safety Requirement* e um *Functional Architecture Element*.

Figura 15 - Dependência entre requisito atômico e requisito de tolerância a falha



Fonte: O autor

Figura 16 - Dependências de um requisito de tolerância a falhas

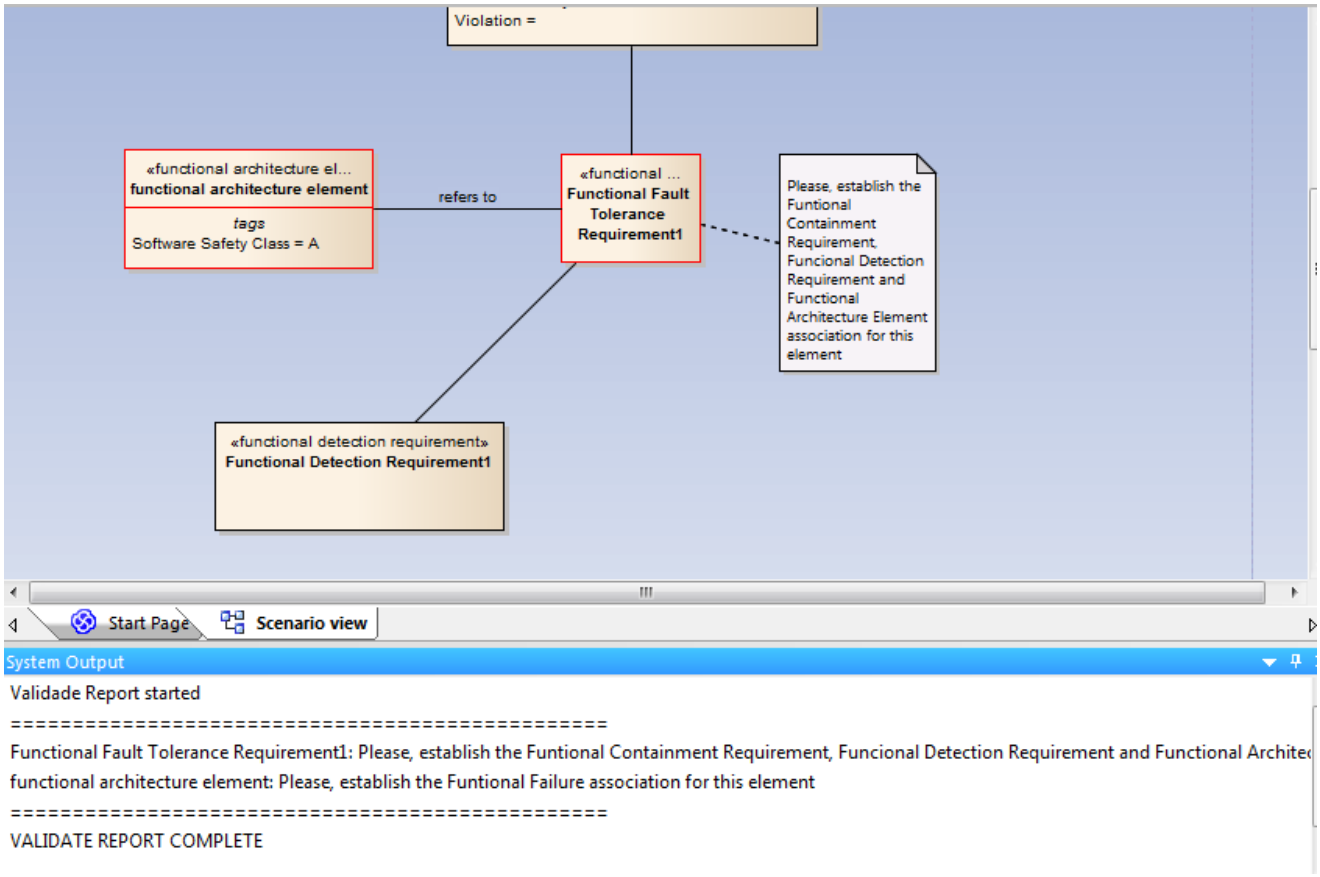


Fonte: O autor

Prevendo que o usuário pode simplesmente ignorar os alertas disparados pelo ADFSA, algumas medidas foram tomadas para que possa ser visível que há inconformidades no diagrama, como: o elemento que não está conforme tem seu contorno em vermelho e/ou uma nota é vinculada ao elemento com uma dica da ação que deve ser tomada para resolver a inconformidade. A Figura 17, mostra um

exemplo do uso de ambos os alertas. É possível perceber uma nota associada a um elemento indicando a ação que deve ser tomada e os elementos com contorno avermelhado indicando inconformidades [28]. É importante destacar também que todas as inconformidades são mostradas no *System Output* do EA.

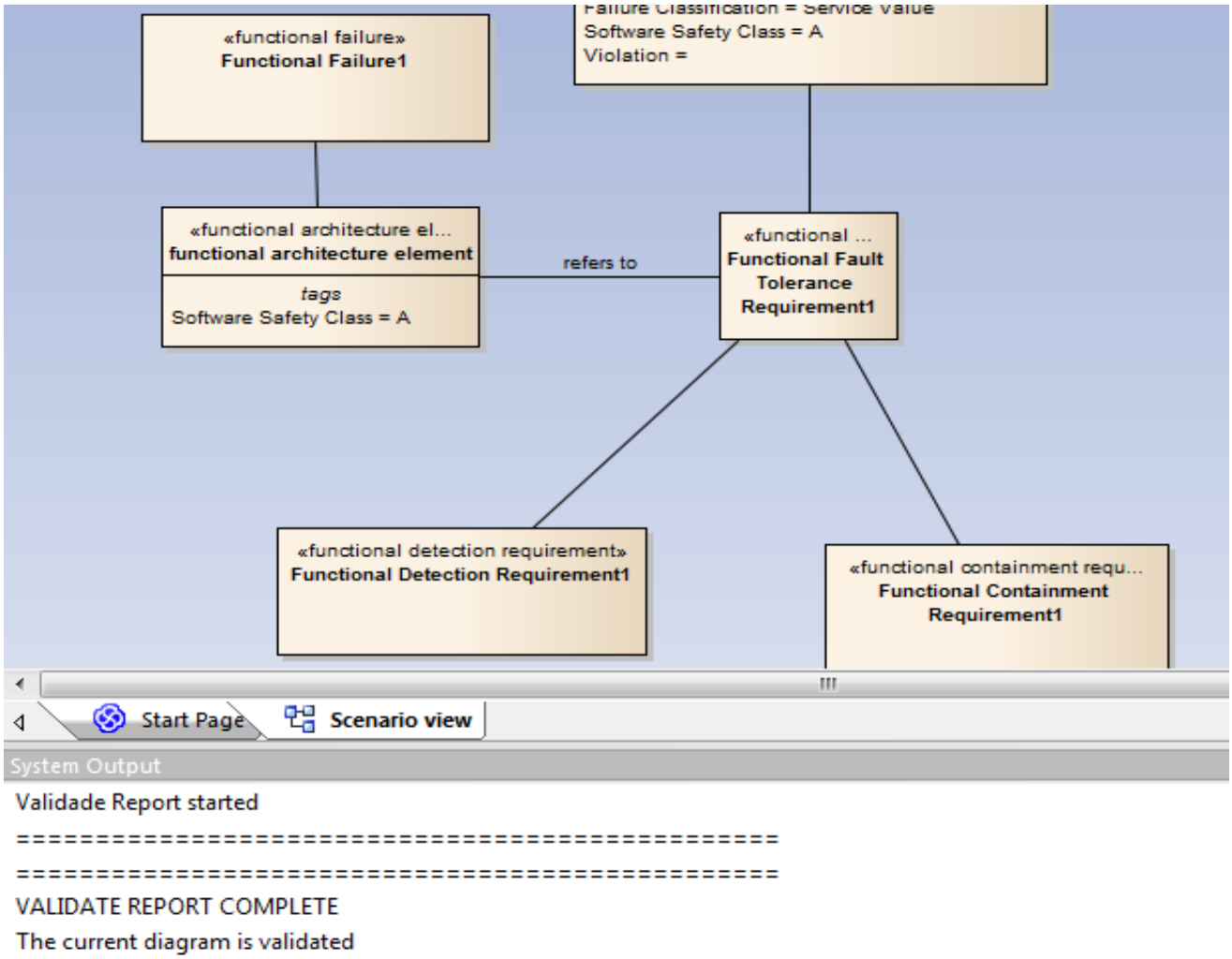
Figura 17 - Notas de alertas de inconformidade



Fonte: O autor

. Caso o diagrama esteja conforme o TIM, após acionar o botão de validação uma mensagem de sucesso é mostrada no *System Output* do EA, como mostra a Figura 18.

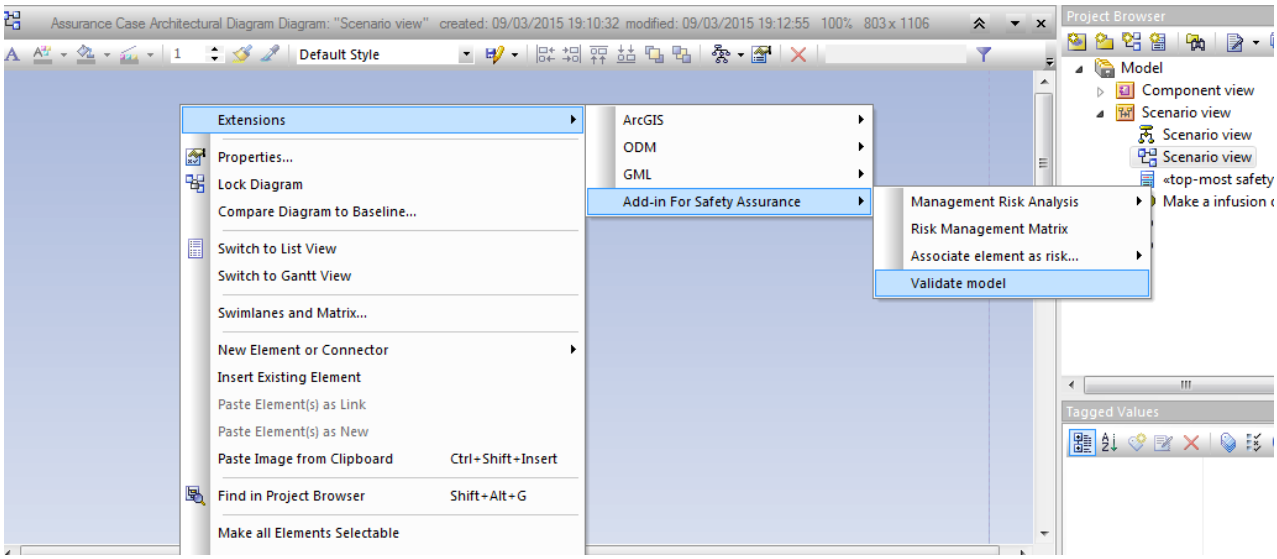
Figura 18 - Diagrama em conformidade com o TIM



Fonte: O autor

Estas verificações podem ser feitas a qualquer momento durante o desenvolvimento, basta acionar o botão *Validate Model* no menu do ADFSA presente no menu de extensões do EA, como mostra a Figura 19.

Figura 19 - Opção de Validação do Diagrama

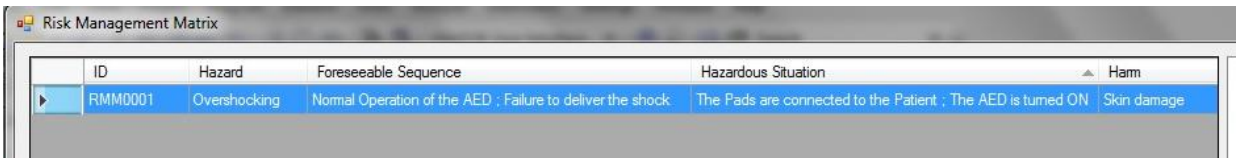


Fonte: O autor

4.3. Armazenando informações de análise de riscos

Uma característica importante do ADFSA é a possibilidade de guardar informações como *Hazards, Harms, Foreseeable Sequence* e *Hazardous Situations* de uma análise de riscos previamente executada, de acordo com a ISO 14971 [28]. Adicionado a isto é possível montar uma Matriz de Gerenciamento de Riscos, como mostra a Figura 20.

Figura 20 - Matriz de Gerenciamento de Riscos

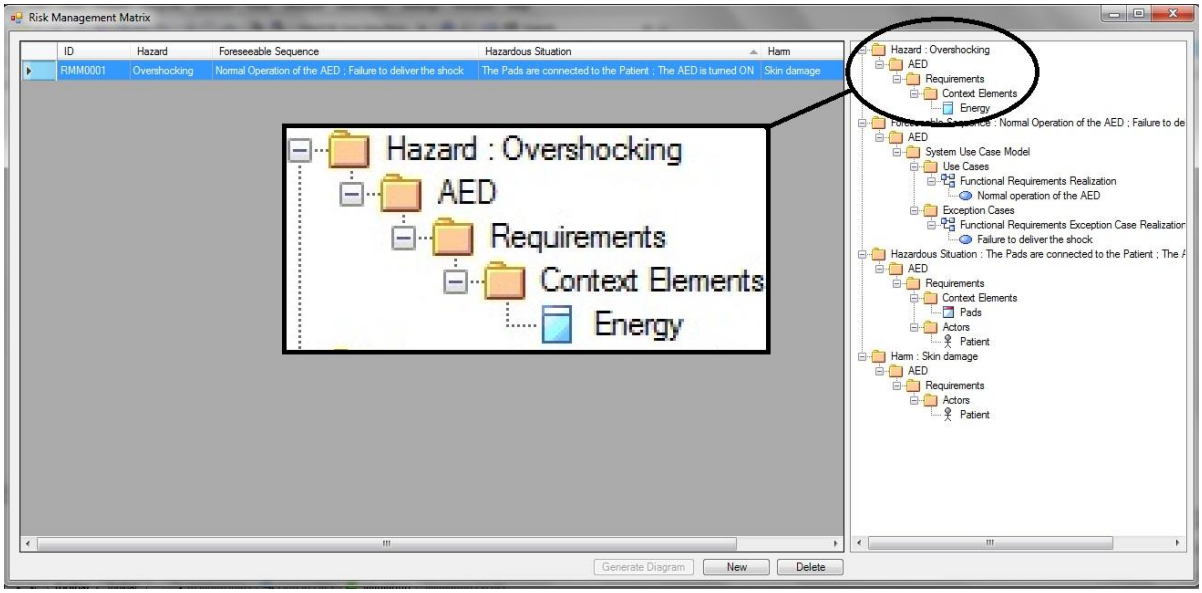


Fonte: O autor

Esta matriz foi elaborada seguindo as orientações do relatório técnico TIR 80002-1 da AAMI [22]. Através desta matriz é possível gerar automaticamente um diagrama de análise de riscos, selecionando a linha da matriz desejada e clicando no botão *Generate Diagram*. Veremos um exemplo deste diagrama gerado a partir da matriz na seção 4.4.

Cuidando em manter os elementos do projeto do EA rastreáveis as análises presentes na matriz, é possível indicar os elementos que devem ser rastreados a determinadas propriedades da matriz, por exemplo, é possível rastrear um *Harm* a um elemento de qualquer diagrama do projeto em desenvolvimento. A Figura 21 mostra um exemplo de rastreabilidade entre elementos de um projeto do EA a propriedades da matriz, a citar: O *Hazard: Overshocking* é rastreado até o componente arquitetural *Energy.*

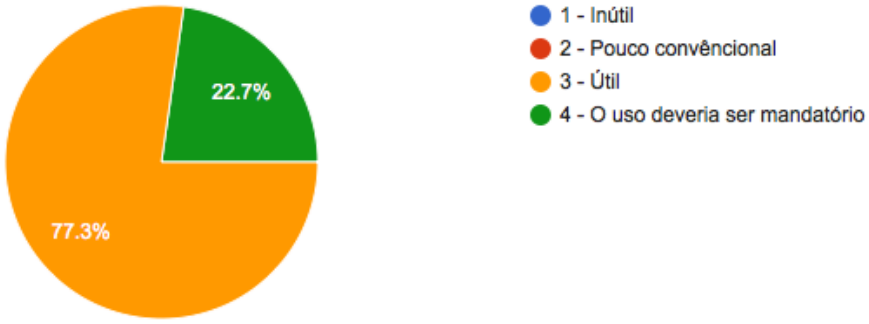
Figura 21 - Rastreabilidade na matriz de gerenciamento de riscos



Fonte: O autor

Mais uma informação que entendemos relevante elucidada na pesquisa interna feita no NUTES (para mais informações ver Apêndice A) refletida na Figura 22 se faz no tocante a analise de riscos e requisitos de *safety,* descobrimos que 22.7% dos participantes acham que o uso de ferramentas para este fim deveria ser mandatório e 77,3% consideraram útil.

Figura 22 - Utilidade de ferramenta automatizada para análise de riscos



Fonte: O autor

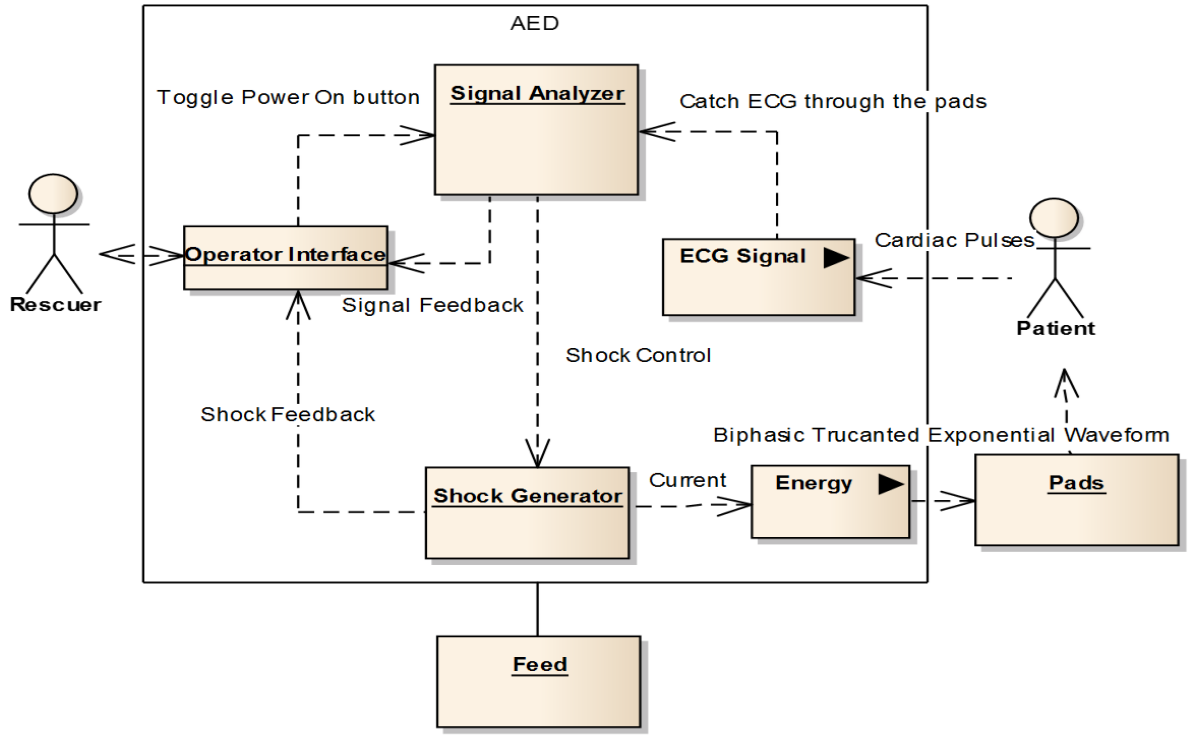
4.4. Exemplo - Requisitos de *safety* para um Desfibriladores Externos Automáticos (DEA)

Desfibriladores são equipamentos médicos que geram e aplicam impulsos de corrente elétrica no músculo cardíaco forçando uma contração simultânea das fibras cardíacas podendo restabelecer o ritmo cardíaco normal [29]. Desfibriladores Externos Automáticos (DEA) são portáteis, compactos e alimentados por bateria. Geralmente são operados por socorristas (*rescuer*, em inglês) que aplicam a corrente no peito do paciente [30].

No DEA, a entrega da corrente elétrica é feita baseada em uma análise automática do eletrocardiógrafo (ECG) acoplado ao aparelho. Quando estas entregas sofrem atrasos, as chances de sobrevivência do paciente diminuem de 7% a 10% por minuto de atraso tornando uma aplicação *safety-critical*, por isso é importante garantir e otimizar a recarga do equipamento no intervalo de cada aplicação.

Este caso de uso está inserido em projetos do Núcleo de Tecnologias Estratégicas em Saúde (NUTES) [31], trata-se de uma iniciativa do Ministério da Saúde Brasileiro que tem como um de seus principais objetivos promover o desenvolvimento de tecnologias para dispositivos médicos. Em um de seus esforços de desenvolvimento, o NUTES tem apresentado uma especificação de decomposição de requisitos de *safety* para o DEA na aplicação do choque. A Figura 23 mostra um diagrama com as principais unidades externas do DEA modelado, representando a interação geral entre elas.

Figura 23 - Diagrama de Contexto do EAD



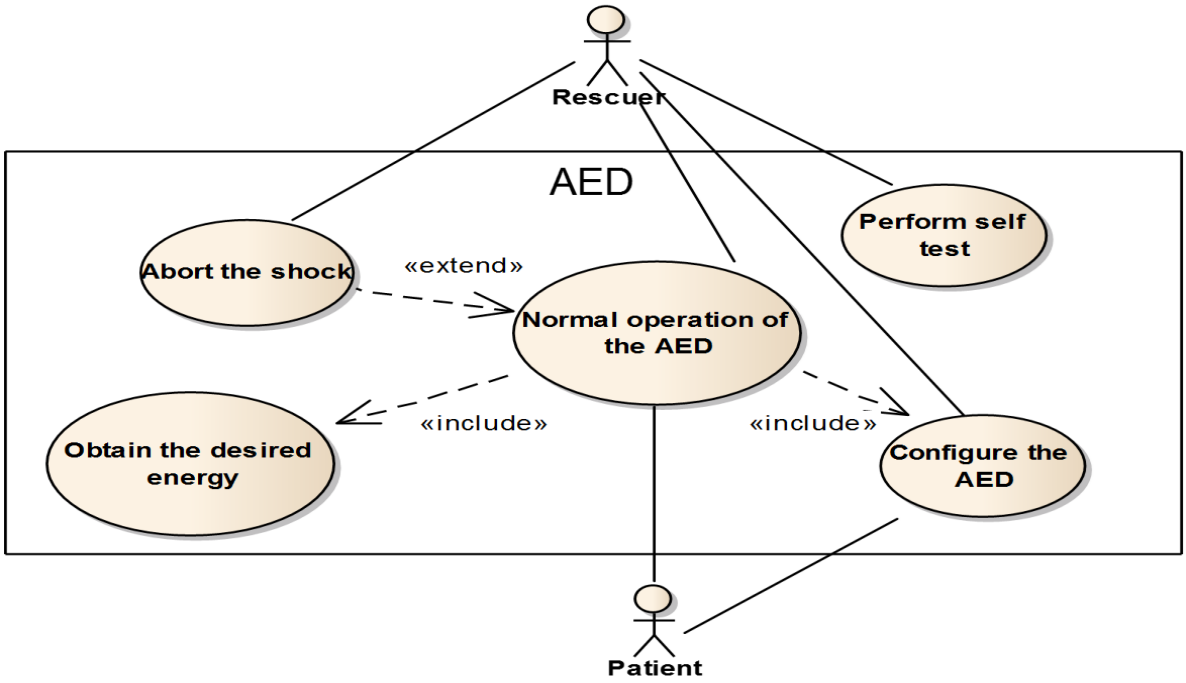
Fonte: O autor

Os principais módulos do sistema apresentado nesse diagrama de contexto são:

- *Operator Interface* – Captura os principais comandos do usuário e emite alertas e alarmes sobre o processo de aplicação do choque.
- *Signal Analyzer* – Detecta e analisa o sinal entregue pelo ECG verificando se houve uma parada cardíaca.
- *Shock Generator* – Em caso de detecção de uma parada cardíaca este elemento entrega ao peito do paciente através das pás (*Pads*) uma descarga controlada de energia.

A Figura 24 mostra caso de uso da aplicação principal do EAD em funcionamento normal.

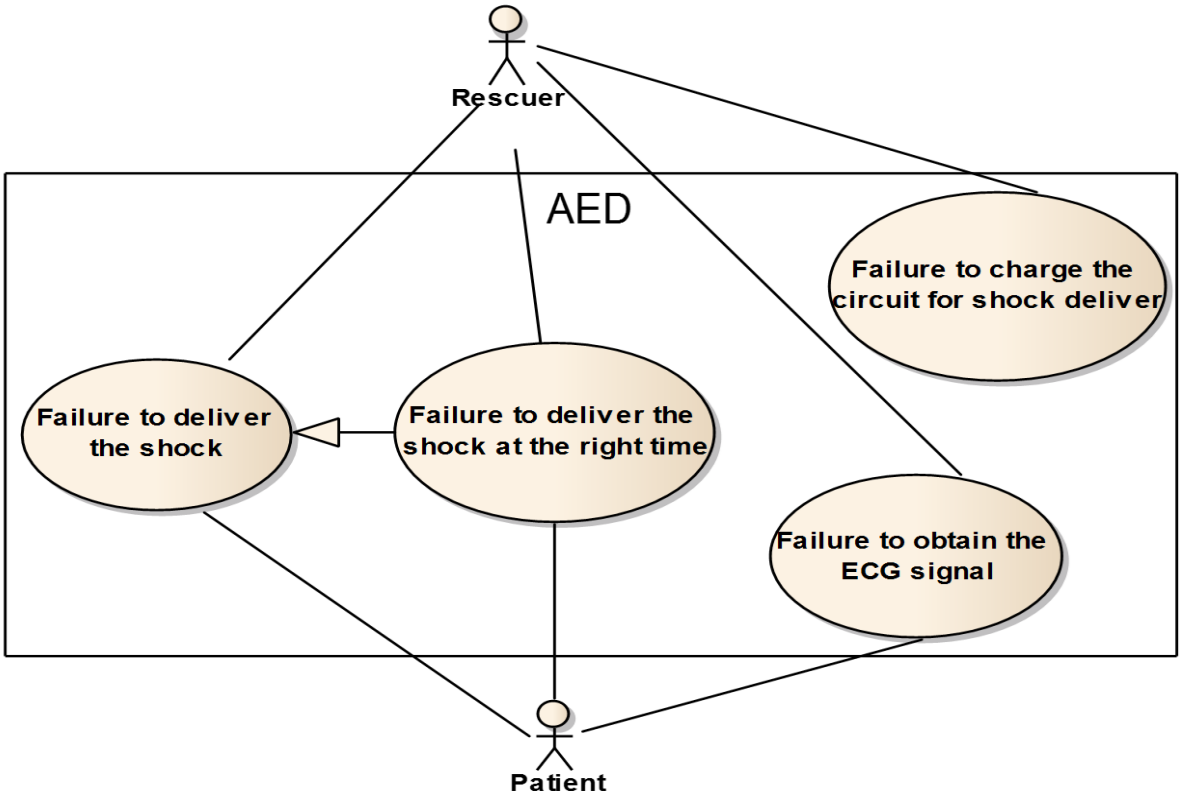
Figura 24 - Aplicação básica do EAD



Fonte: O autor

Utilizando-se do EA com o ADFSA o NUTES tem desenvolvido um modelo de decomposição dos requisitos de *safety*, resumida na Figura 25, na tentativa de argumentar uma mitigação do *Overshocking*, que um dos possíveis perigos inerentes a falhas durante a utilização deste aparelho.

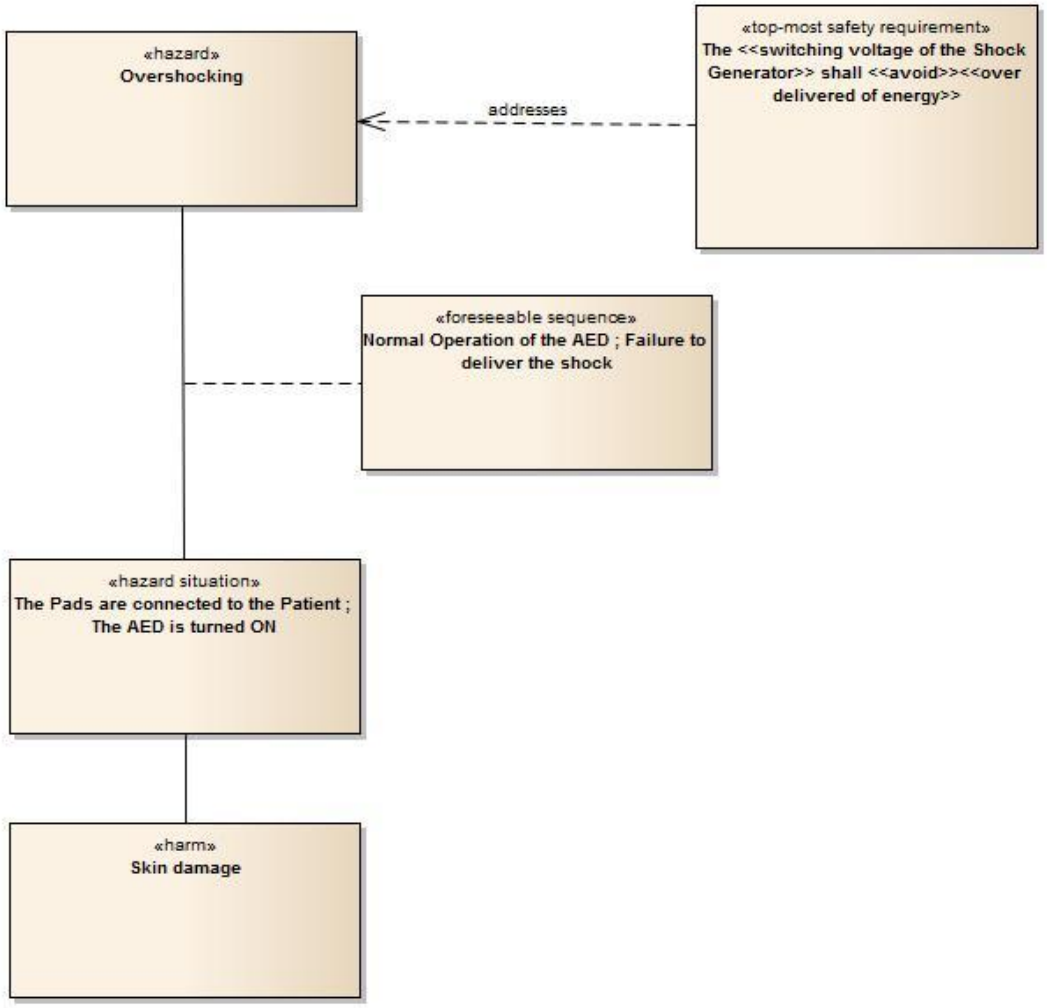
Figura 25 - Possíveis falhas no uso do EAD



Fonte: O autor

Garantir que no chaveamento de tensão em seus semicondutores, o *Shock Generator* não entregará uma corrente elétrica acima do valor previamente especificado, é uma das maneiras de mitigar o hazard *Overshocking*. A Figura 26 representa um diagrama com elementos de análise de riscos, mostrando os possíveis maus usos, situação perigosa e danos causados pelo *Overshocking.*

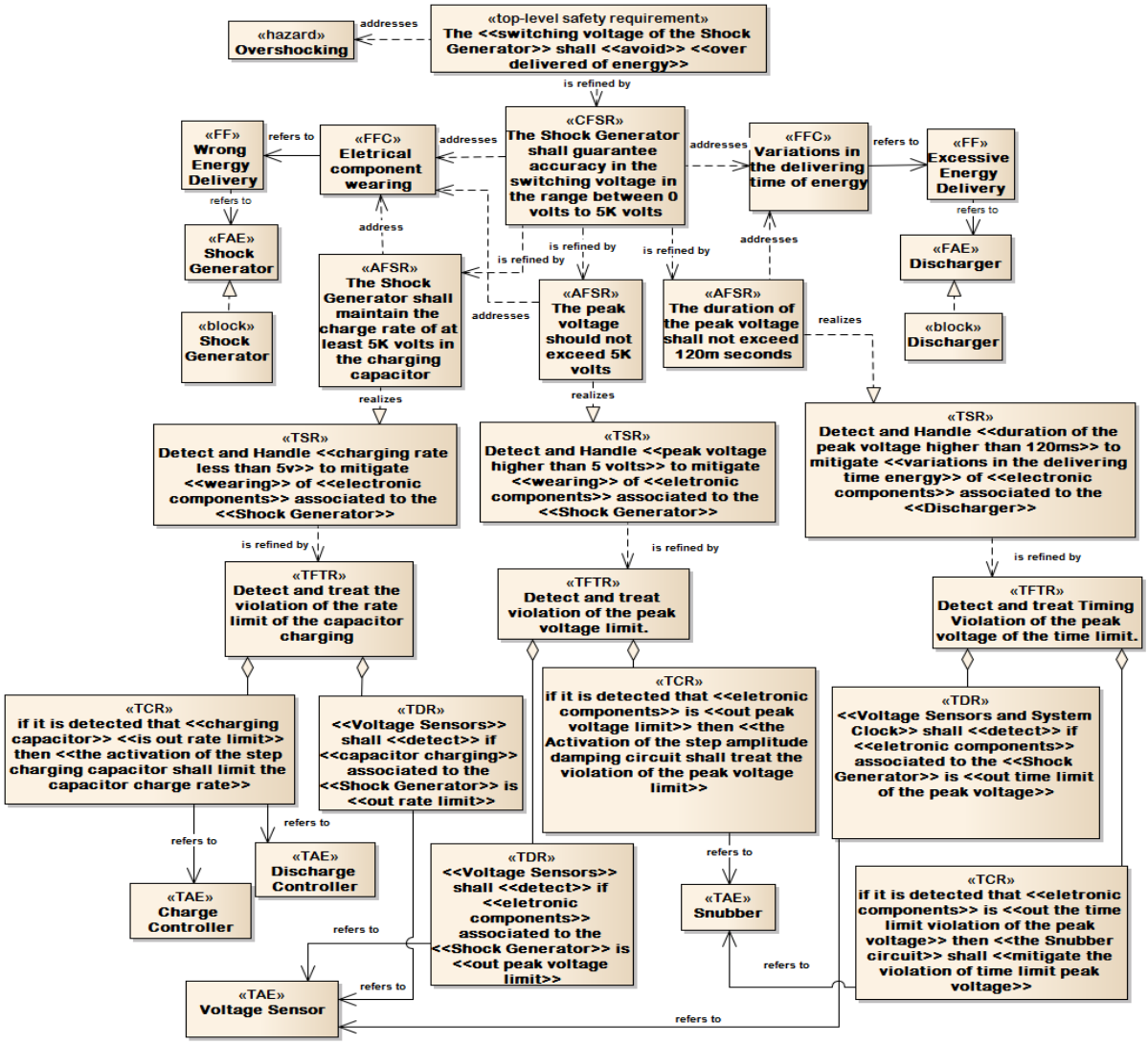
Figura 26 - Diagrama de Análise de Riscos



Fonte: O autor

O *Top-most Safety Requirement* da Figura 27 representa o objetivo principal para esta medida protetiva, decomposta no sentido de detalhar as medidas tomadas em requisitos mais específicos compostos de características próprias.

Figura 27 - Decomposição dos Requisitos de Safety do EAD



Fonte: O autor

A decomposição deste *Top-most safety requirement* se dá basicamente de duas formas, (i) com foco no modulo do *Shock Generator, Atomic Functional Safety Requirement* a esquerda da Figura 27, e (ii) com foco no modulo de descarga, *Atomic Functional Safety Requirement* a direita da mesma figura. Associados a estes requisitos atômicos é possível observar a representação de medidas de controle de falhas, como:

- Indicativos de desgastes de componentes;
- Alertas para manutenção e reparação devem ser emitidos;
- Controle de picos inesperados realizados por circuitos de amortização;

- Evitar que limites de picos de tensões sejam excedidos, gerenciados por outros circuitos.

Por fim, é possível perceber elementos técnicos como sensores e atuadores que trabalham para detectar comportamentos que levem a condições perigosas.

5. METODOLOGIA

Neste capítulo entenderemos o processo metodológico usado nesta pesquisa. Abordaremos o tipo de pesquisa, cenário, tipo de amostragem não probabilística, os critérios de inclusão e exclusão, instrumentos para coleta de dados e os procedimentos e, por fim, a análise e apresentação dos resultados.

5.1. Tipo de pesquisa

Esta é uma pesquisa qualitativa de caráter exploratório e descritivo.

Na tentativa de tornar explícito que problemas como a falta de um planejamento de rastreabilidade e a falta de elementos que aderecem os projetos de dispositivos médicos às normas reguladoras, tornamos essa pesquisa exploratória, aumentando a experiência do investigador e aprofundando o conhecimento, pois, segundo Canzonieri [32] pesquisas deste tipo permitem conhecer mais profundamente fatos e fenômenos relacionados ao tema.

De acordo com Canzonieri [32] uma pesquisa descritiva se dá ao passo que se descrevem algumas características do que é pesquisado, a citar: descrição de um fenômeno. Usando survey, uma técnica padronizada de coleta de dados, torna essa pesquisa descritiva formal, já que registra, observa e avalia o relacionamento entre dados dos fatos ou fenômenos ocorridos [33].

No caso deste trabalho o levantamento dos dados ocorreu no âmbito do NUTES e envolveu o grupo de pessoas dos setores de aprendizado e desenvolvimento de projetos para indústria de dispositivos médicos. Os resultados podem ser conferidos na íntegra no ANEXO A.

5.2. Cenário

O Núcleo de Tecnologias Estratégicas em Saúde (NUTES) foi o ambiente onde aconteceu a pesquisa. Localizado na Universidade Estadual da Paraíba (UEPB), campus I, o NUTES é um centro formador de competências no desenvolvimento de tecnologias para a saúde. Justamente pelo seu caráter formador, as pesquisas tiveram de envolver estudantes e profissionais tanto da área

de computação quanto de engenharia elétrica o que caracterizou a população envolvida nos dados levantados.

6. CONCLUSÃO

Interpretar e alinhar as medidas protetivas a serem desenvolvidas em projetos de alto risco é de fundamental importância para o bem estar dos indivíduos e preservação da vida e a verificação destas medias devem estar presentes em todas as etapas do desenvolvimento, inclusive na de planejamento.

Neste trabalho conseguimos propor uma forma planejamento prático de como alinhar elementos de uma análise de riscos se interligam a elementos que decomposição de requisitos de segurança, partindo de requisitos mais gerais até elementos arquiteturais do sistema. Nos resultados da pesquisa isso se mostrou importante para o trabalho dos profissionais e pesquisadores da área de dispositivos *safety-critical*.

Outro ponto importante foi poder constatar que uma prática de planejamento de rastreabilidade de requisitos é fundamental para a boa construção de projetos de sistemas deste tipo. Para facilitar o uso de um planejamento de rastreabilidade, este trabalho trouxe um protótipo de uma ferramenta que automatiza checagens considerando o relacionamento entre os elementos da decomposição de requisitos. A pesquisa mostra indícios de que os profissionais e pesquisadores precisam de ferramentas deste tipo, agilizando o trabalho dos mesmos e garantindo a conformidade em seus planejamentos.

Não menos importante e considerando a indústria de dispositivos médicos, este trabalhou tentou agregar valores de normas reguladoras na área da saúde brasileira adicionando aos elementos do modelo de rastreabilidade e às checagens feitas pelas ferramentas valores importantes de normas presentes na regulação atual. O que reforçou a utilidade do trabalho foram os resultados da pesquisa onde mostraram que profissionais e pesquisadores dá área procuram considerar o rumo de seus projetos a indicações feitas nas normas.

O protótipo aqui desenvolvido busca diminuir a falta de ferramentas de gerência de rastreabilidades em projetos para dispositivos médicos no mercado, claro, considerando uma ferramenta que atuará na verificação de artefatos de segurança nos projetos e que adicionará valores pertinentes às normas reguladoras em suas checagens.

Para finalizar, devemos considerar que este trabalho trouxe, também, formas de tentar adicionar agilidade no processo de desenvolvimento de projetos de

sistemas críticos, tentando aproximar, principalmente os desenvolvedores de softwares, a realidades mais atuais na prática do desenvolvimento.

REFERÊNCIAS

[1] B. H. Brown, R. H. Smallwood, D. C. Barber, P. V. Lawford, and D. R. Hose, *Medical Physics and Biomedical Engineering*. New York: Taylor & Francis Group, 1999.

[2] Clifton A Ericson II, *Hazard Analysis Techniques for System Safety*. Fredericksburg, Virginia: Wiley-Interscience, 2005.

[3] Paulo E. S. Barbosa et al., "Towards Medical Device Behavioural Validation Using Petri Nets," in *IEEE International Symposium on Computer-Based Medical Systems - CBMS 2013*, Porto, 2013.

[4] David A. Vogel, *Medical device software verification, validation and compliance*. Norwood, MA: Artech House, 2011.

[5] ISO 14971, ISO 14971 - Medical Devices - Application of risk management to medical devices, 2007.

[6] Guilherme Mauro Germoglio Barbosa, *Um Livro-texto para o Ensino de Projeto de Arquitetura de Software*. Campina Grande, Paraíba, Brasil: UFCG, 2009.

[7] P. Mäder, P. L. Jones, Y. Zhang, and J. Cleland-Huang, "Strategic traceability for safety-critical projects," *IEEE Software Vol. 30*, pp. 58-66, May 2013.

[8] Jane Huang, Orlena Gotel, and Andrea Zisman, *Software and Systems Traceability*. London: Springer, 2012.

[9] Pablo Oliveira Antonino and Mario Trapp, "Improving consistency checks between safety concepts and view based architecture design," *Probabilistic Safety Assessment and Management*, Dec. 2014.

[10] International Organization for Standardization, ISO/DIS 26262 - Road Vehicles – Functional Safety, 2011.

[11] J. Cleland-Huang, O. C. Z. Gotel, J. Huffman Hayes, Patrick Mäder, and A. Zisman, "Software traceability: Trends and future directions," *Proceedings of the on Future of Software Engineering,* pp. 55-69, 2014.

[12] IEC, IEC 62304 - Medeical Device Software - Software Life Cycle Process, 2006.

[13] Pablo Oliveira Antonino, Thorsten Keuler, Nicolas Germann, and Brian Cronauer, "A Non-invasive Approach to Trace Architecture Design, Requirements Specification and Agile Artifacts," *Software Engineering Conference (ASWEC)*, pp. 220-229, Apr. 2014.

[14] Timothy Patrick Kelly, Arguing Safety - A Systematic Approach to Managing Safety Cases, 1998.

[15] Klaus Pohl and Chris Rupp, *Requirements Engineering Fundamentals*. Sebastopol, CA: O'Reilly, 2011.

[16] D Domis, M Forster, S Kemmann, and M Trapp, "Safety Concept Trees," *Reliability and Maintainability Symposium*, pp. 212-217, Jan 2009.

[17] Ibrahim Habli, Ireri Ibarra, Roger Rivett, and Tim Kelly, Model-Based Assurance for Justifying Automotive Functional Safety, 2010.

[18] John Birch et al., "Safety Cases and Their Role in ISO 26262 Functional Safety Assessment," in *Computer Safety, Reliability, and Security*. Toulouse, France: Springer, 2013, pp. 154-165.

[19] Ewen Denney and Ganesh Pai, "A Formal Basis for Safety Case Patterns," in *Computer Safety, Reliability, and Security*. Toulouse, France: Springer, 2013, pp. 21-32.

[20] RTCA, DO-178C/ED-12C - Software Considerations in Airborne Systems and Equipment Certification, 2011.

[21] Patrick Mäder, O. Gotel, and I. Philippow, "Getting back to basics: Promoting the use of a traceability information model in practice," *Proceedings of the 2009 ICSE Workshop on Traceability in Emerging Forms of Software Engineering*, pp. 21-25, 2009.

[22] AAMI - Association for the Advancement of Medical Instrumentation, "TIR 80002-1:2009 - Medical Device Software - Part 1: Guidance on the Application of ISO 14971 to Medical Device Software," Arlington, VA, 2009.

[23] Michael R. Lyu, *Software Fault Tolerance*. Chichester, UK: John Wiley and Sons Ltd, 1995.

[24] Laura L. Pullum, *Software Fault Tolerance - Techniques and Implementation*. Norwood, MA: Artech house, 2001.

[25] Sparxsystems. (2015, Oct.) Sparx Systems. [Online]. www.sparxsystems.com.au

[26] David Sean Avis, IIBA UK Business Analysis Survey 2012 - Top Line Results, 2012.

[27] Sparx Systems. (2015, Oct.) International Electrotechnical Commission moves Common Information Model to Sparx Systems Enterprise Architect. [Online]. http://www.sparxsystems.com.au/press/articles/iec.html

[28] Paulo Barbosa et al., "RAwTIM - Uma ferramenta para rastreabilidade da informação em análises de riscos," *Brazilian Conference on Software: Theory and Practice - Tools Section*, Sep. 2015.

[29] Carlos Fornazier et al. (2011, Março) Anvisa - Boletim Informativo de Tecnovigilância. [Online]. http://www.anvisa.gov.br/boletim_tecno/boletim_tecno_fev2011/PDF/matriz_desfibri_que_temos04fev2011.pdf

[30] Clean Medical. (2015, Março) www.cleanmedical.com.br. [Online]. www.cleanmedical.com.br/dea.php

[31] NUTES. (06, Março) nutes.uepb.edu.br. [Online]. nutes.uepb.edu.br

[32] A. M. Canzonieri, *Metodologia qualitativa na saúde*, 1st ed. Petrópolis, RJ, Brasil: Vozes, 2010.

[33] C. Wohlin et al., *Experimentation in Software Engineering*.: Springer Science & Business Media, 2012.

[34] Tânia Modesto Veludo de Oliveira. (2001, Sep.) Amostragem não Probabilística: Adequação de Situações para uso e Limitações de amostras por Conveniência, Julgamento e Quotas. [Online]. http://www.fecap.br/adm_online/art23/tania2.htm

[35] Carlos Ochoa. (2015, Oct.) Blog da Netquest. [Online]. http://www.netquest.com/blog/br/amostra-conveniencia/

[36] Balasubramaniam Ramesh and Matthias Jarke, "Toward Reference Models for Requirements Traceability," *IEEE Transactions on Software Engineering*, pp. 58-93, Jan 2001.

APENDICÊ

APÊNDICE A – DISCUSSÃO DOS RESULTADOS OBTIDOS NO QUESTIONÁRIO SOBRE PRÁTICA DE DECOMPOSIÇÃO DE REQUISITOS DE SAFETY COM ANALISE DE RISCOS PARA INDÚSTRIA DE DISPOSITIVOS MÉDICOS

UNIVERSIDADE ESTADUAL DA PARAÍBA
CENTRO DE CIÊNCIAS EXATAS E DA TERRA - CCT
PROGRAMA DE PÓS GRADUAÇÃO EM CIÊNCIA E TECNOLOGIA EM SAÚDE – PPCTS

Usando uma técnica de amostragem não probabilística, adotamos para esta pesquisa uma abordagem chamada de amostragem por conveniência. Este tipo de abordagem se dá quando não é possível ter acesso a todos os indivíduos que formariam a população desejada, conhecido como marco amostral, os indivíduos são selecionados simplesmente por que estavam acessíveis não sendo escolhidos por meios estatísticos [34].

Apesar de parecer uma abordagem em que os dados podem não refletir a realidade, estudiosos da área apontam que este tipo de seleção não irá inserir nenhum viés em quando considerado a população total e os resultados podem ser uma imagem bastante próxima do real, o diferencial, neste caso, é que o leitor terá de confiar nos critérios de seleção do pesquisador, visto que, o mesmo não pode por algum motivo aplicar ferramentas estatísticas como margem de erro e níveis de confiança [35].

Foram inclusos nesta coleta de dados estudantes, pesquisadores e engenheiros egressos dos cursos de computação da Universidade Estadual da Paraíba - UEPB e de computação e engenharia elétrica da Universidade Federal de Campina Grande que já tinham alguma experiência em pesquisas nas áreas de com desenvolvimento de sistemas *safety-critical* com ênfase em dispositivos médicos realizados no Núcleo de Tecnologias Estratégicas em Saúde – NUTES. Ainda no âmbito do NUTES foram inclusos também profissionais da área de computação e engenharia elétrica que também participaram dos mesmos tipos de projetos. Adicionado a estes contamos com colaboradores atuantes na área de projetos em sistemas *safety-critical* do instituto espanhol, Tecnalia. Um total de 22 participantes e todos responderam as questões presentes no formulário do Apêndice B.

Foram excluídos destas pesquisas os indivíduos que não tinham quaisquer conhecimentos prático ou teórico acerca dos tópicos tratados nesta pesquisa e que

não colaboraram com as pesquisas realizadas no NUTES na área de desenvolvimento de software ou hardware para indústria médica entre os anos de 2012 e 2015.

Utilizamos para coleta de dados a ferramenta do Google Docs, criando um formulário o qual foi enviado para todas os indivíduos que estavam disponíveis e que se encaixavam dentro dos critérios de seleção estipulados na seção 5.4. Este formulário (Apêndice A), constituía 9 perguntas relacionadas a importância de gerenciamento planejado de rastreabilidade na decomposição de requisitos de safety até elementos arquiteturais do sistema, além disso perguntas relacionadas à importância de se ter uma ferramenta que pudesse ser usada no auxilio a este gerenciamento e algumas perguntas que envolviam a importância de elementos de normas reguladores na decomposição de tais requisitos.

Este formulário foi enviado via e-mail e juntamente com uma explicação detalhada do que se tratava a pesquisa.

Este procedimento se caracterizou, também, por não ter sido uma aplicação controlada, ou seja, o pesquisador não estava junto aos respondentes no momento da aplicação do formulário. Isentando-o de qualquer tentativa de manipular a pesquisa inserindo algum viés do pesquisador.

A distribuição destes perfis no conjunto de respondentes pode ser vista na Tabela 1 onde temos os totais de 12 estudantes de computação ou engenharia elétrica com uma porcentagem de 54,5%, profissionais de computação eram 9 o equivalente 40,9% e 1 engenheiro eletricista que representou 4,5% do total. Não observamos nenhum respondente que tivesse outro perfil além dos três supracitados.

Tabela 1 - População da pesquisa

População da pesquisa		
Perfil do entrevistado	**Quantidade**	**%**
Estudante de Computação/Engenharia Elétrica	12	54.5
Profissional de Computação	9	40.9
Engenheiro Eletricista	1	4.5
Outro	0	0

Fonte: O autor

Observando as respostas à questão 1 que tratava da importância de uma análise prévia de riscos no apoio a tomada de decisões arquiteturais de um sistema para indústria médica, obtivemos o seguinte resultado que pode ser visto na Tabela 2, apenas foram obtidas as respostas ‘Essencial e Relevante’, onde 95,5% dos respondentes disseram ser essencial a análise prévia de riscos e 4,5% consideraram relevante. Para estudantes de computação ou engenharia elétrica todos (100%) consideraram ‘Essencial’ e a mesma resposta foi obtida de 88,9% dos profissionais de computação respondentes e 100% dos engenheiros eletricistas. Para 11,1% dos profissionais de computação essa analise prévia é ‘Relevante’.

Tabela 2 – Questão 1: Como você avalia o uso da análise prévia de riscos no apoio a tomada de decisões arquiteturais de um sistema para dispositivos médicos?

RESPOSTA	TOTAL (%)	% POR PERFIL		
		ESTUDANTE COMPUTAÇÃO OU ELETRICA	PROFISSIONAL DE COMPUTAÇÃO	ENGENHEIRO ELETRICISTA
Essencial	95,5	100,0	88,9	100,0
Relevante	4,5	0,0	11,1	0,0
TOTAL	**100,0**	**100,0**	**100,0**	**100,0**

Fonte: O autor

Na questão 2, que tem seus resultados mostrados na Tabela 3, a ideia foi levantar informações sobre a necessidade de apresentar elementos de normas reguladoras na documentação arquitetural dos dispositivos médicos. Onde apenas respostas como: ‘Necessário’ e ‘Boa prática’ foram obtidos, onde 72,7% dos respondentes disseram que acham necessários a presença de elementos de normas reguladoras em documentação arquitetural para o tipo de sistema aqui tratado e 27,3% consideraram que ter essa informação é uma ‘Boa prática’ não tendo caráter mandatório. Destes, 66,7% dos estudantes de computação ou engenharia elétrica responderam achar ‘Necessário’ e 33,3% ‘Boa prática’, profissionais de computação consideraram em 77,8% ‘Necessário’ e 22,2% ‘Boa prática’ e para os engenheiros eletricistas 100% consideraram ‘Necessário’.

Tabela 3 – Questão 2: No tocante certificação de dispositivos médicos diante agências reguladoras como você avalia necessidade de apresentar elementos das normas reguladoras na documentação arquitetural de dispositivo médico?

RESPOSTA	TOTAL (%)	% POR PERFIL

		ESTUDANTE COMPUTAÇÃO OU ELETRICA	PROFISSIONAL DE COMPUTAÇÃO	ENGENHEIRO ELETRICISTA
Necessário	72,7	66,7	77,8	100,0
Boa prática	27,3	33,3	22,2	0,0
TOTAL	**100,0**	**100,0**	**100,0**	**100,0**

Fonte: O Autor

Considerando que ao entender essencial o uso da analise previa de riscos para o apoio tomada de decisões arquiteturais, preocupação presente na questão 1 espera-se que uma forte tendência a que estas pessoas considerem elementos de análise de riscos necessário no tocante a documentação que será apresentada a órgãos reguladores, presentes na questão 2.

O resultado obtido verificado na Tabela 4 foi que 100% dos que consideram analise de riscos relevante consideram, também, necessário que elementos oriundos desta analise sejam descritos na documentação que remetem a itens de regulação. Já para aqueles que tentem essencial a analise de riscos 71,4% acham que é necessário a descrição destes na documentação e 28,6% consideram uma boa prática.

Assim, podemos constatar que a tendência de que projetistas entendem que analise de riscos pode contribuir inserindo fortes valores à documentação que poderá ser avaliada por órgãos reguladores é forte e que esta pratica é bastante presente no âmbito do desenvolvimento.

Tabela 4 - Relacionamento entre Q1 e Q2 – Elementos de analise de riscos e seus valores presentes em documentação arquitetural

RESPOSTA PARA QUESTÃO 2	RESPOSTAS PARA QUESTÃO 1	
	Relevante	Essencial
Necessário	100%	71,4%
Boa prática	0%	28,6%
TOTAL	**100%**	**100%**

Fonte: O Autor

Sobre a questão 3, a ideia foi buscar informações sobre como o projetista entende a necessidade de ter um modelo de decomposição de requisitos onde este auxiliaria na manutenção da rastreabilidade, considerando uma ênfase nos requisitos de safety e elementos arquiteturais do sistema. Na Tabela 5 conseguimos

verificar que para 63,6% dos respondentes este modelo é ‘Necessário’ e 36,4% considera ‘Boa prática’, nenhuma outra resposta foi obtida além destas duas citadas. Observamos também que entre os estudantes de computação e engenharia elétrica 66,7% consideraram ser ‘Necessário’ e 33,3% ‘Boa prática’ para profissionais de computação obtivemos 55,6% dizendo que é ‘Necessário’ e ’44,4’ que consideram ‘Boa prática’, para 100% dos engenheiros eletricistas esse modelo é ‘Necessário’.

Tabela 5 – Questão 3: Como você entende a necessidade de ter um modelo para guiar o planejamento de rastreabilidade entre requisitos de safety decompostos e elementos arquiteturais do sistema?

RESPOSTA	TOTAL (%)	% POR PERFIL		
		ESTUDANTE COMPUTAÇÃO OU ELETRICA	PROFISSIONAL DE COMPUTAÇÃO	ENGENHEIRO ELETRICISTA
Necessário	63,6	66,7	55,6	100,0
Boa prática	36,4	33,3	44,4	0,0
TOTAL (%)	**100,0**	**100,0**	**100,0**	**100,0**

Fonte: O autor

Como discutido em capítulos anteriores e chegando à conclusão de que garantir a boa manutenção da rastreabilidade pode agregar valores de medidas protetivas à documentação passível de verificação por parte de órgãos regulamentadores, procuramos relacionar a questão 2, no tocante a documentação e questão 3 no tocante a manutenção de rastreabilidade. Como vimos na Tabela 6.

Para àqueles que entendem ser uma boa prática a inclusão de valores de medidas protetivas na documentação 50% responderam que é necessário que exista um planejamento de rastreabilidade e os outros 50% consideram uma boa prática, em ambos os casos o indicio é de a apresentação um planejamento de rastreabilidade na documentação fortalece aspectos de regulação, isto se fortalece quando observamos que para aqueles que 68,8% entendem necessário a inclusão de valores de medidas protetivas na documentação também acreditam que a inserção de um planejamento de rastreabilidade se faz necessário, e não menos importe 31,2% consideram uma boa prática.

Tabela 6 - Relacionamento entre Q2 e Q3 – Planejamento de rastreabilidade em documentação como valor de descrição de medida protetiva.

RESPOSTAS PARA QUESTÃO 3	RESPOSTAS PARA QUESTÃO 2	
	Boa prática	Necessário
Necessário	50,0	68,8
Boa prática	50,0	31,2
TOTAL	**100,0**	**100,0**

Fonte: O autor

No intuito de entender o raciocínio dos respondentes sobre a utilidade que teria uma ferramenta que pudesse de forma automatizada guiar o projetista na manutenção e criação de rastreabilidade de requisitos em projetos para sistemas *safety-critical* garantindo checagens de validação entre relacionamentos e atributos de elementos obtivemos da questão 4 o quadro representado na Tabela 7, onde apenas as respostas ‘Útil’ e ‘O uso deveria ser mandatório’ foram percebidas sendo que 77,3% do total disseram que seria ‘Útil’ e para ‘O uso deveria ser mandatórios’ foram 22,7%. Entre os estudantes de computação ou engenharia elétrica tivemos 66,7% dizendo que é ‘Útil’ e 33,3% considerando mandatório o uso, para os profissionais de computação tivemos 88,9% entendendo como útil e 11,1% entendendo como mandatório e 100% dos engenheiros eletricistas consideraram “´Útil”.

Tabela 7 – Questão 4: O quão útil seria para você ter uma ferramenta que, de forma automatizada, lhe guiasse na manutenção e na gerência da rastreabilidade entre: os elementos da análise de riscos, os requisitos de safety decompostos e os elementos arquiteturais do sistema?

RESPOSTA	TOTAL (%)	% POR PERFIL		
		ESTUDANTE COMPUTAÇÃO OU ELETRICA	PROFISSIONAL DE COMPUTAÇÃO	ENGENHEIRO ELETRICISTA
Útil	77,3	66,7	88,9	100,0
O uso deveria ser mandatório	22,7	33,3	11,1	0,0
TOTAL (%)	**100,0**	**100,0**	**100,0**	**100,0**

Fonte: O autor

Seguir um planejamento de rastreabilidade à risca pode ser uma tarefa árdua como visto em capítulos anteriores, partindo deste entendimento tentamos entender entre o público respondente a necessidade de se ter uma ferramenta para fortalecer

o uso da prática de planejamento de rastreabilidade. Estes dados são apresentados na Tabela 8.

Para aqueles que acreditam que o uso de um planejamento de rastreabilidade é uma boa prática 100% disseram que seria útil de ter uma ferramenta para ajudar nesta manutençãoo da rastreabilidade e 64,3% que entende que a prática de planejamento é necessária acharam que seria útil ter uma ferramenta para auxilia-los e 35,7% entendem que o uso desta ferramenta é mandatório se você considera necessário o planejamento da rastreabilidade.

Tabela 8 - Relacionamento entre Q3 e Q4 – Considerando o uso de uma ferramenta para auxiliar no planejamento da rastreabilidade quando boa prática ou necessário.

RESPOSTAS PARA QUESTÃO 4	**RESPOSTAS PARA QUESTÃO 3**	
	Boa prática	**Necessário**
Útil	100,0	64,3
O uso deveria ser mandatório	0,0	35,7
TOTAL (%)	**100,0**	**100,0**

Fonte: O autor

Uma das preocupações, também relacionadas a uma ferramenta que automatize a verificação de elementos de uma decomposição de requisitos, foi entender se ter parâmetros previstos pelas normas reguladoras, como, por exemplo, *Software Safety Class* sendo indicados e verificados por essa por uma ferramenta teria alguma utilidade, visto que, esses elementos serviram para compor dados em uma futura documentação.

Segundo o público envolvido na pesquisa, 72,7% entendem ser ‘Útil’ que valores necessários a compor uma documentação sejam gerenciados pela ferramenta e 27,3% acham que deveria ser ‘Mandatório’ o uso de ferramentas com essa característica. Destes, 58,3% eram estudantes de computação ou engenharia elétrica respondendo ser ‘Útil’ e 41,7% entenderam ser ‘mandatório’. No perfil de profissionais de computação, 88,9% acham ‘Útil’ e 11,1% acham que deveria ser ‘Mandatório’. Para os engenheiros eletricistas 100% consideraram ‘Útil’, estes dados estão descritos na Tabela 9.

Tabela 9 – Questão 5: O quão útil para você seria usar uma ferramenta que lhe guiasse no tocante a definição e manutenção de parâmetros dos elementos (por exemplo, Software Safety Class) de um projeto, parâmetros esses exigidos por normas técnicas reguladoras na indústria de dispositivos médicos?

RESPOSTA	TOTAL (%)	% POR PERFIL		
		ESTUDANTE COMPUTAÇÃO OU ELETRICA	PROFISSIONAL DE COMPUTAÇÃO	ENGENHEIRO ELETRICISTA
Útil	72,7	58,3	88,9	100,0
O uso deveria ser mandatório	27,3	41,7	11,1	0,0
TOTAL (%)	**100,0**	**100,0**	**100,0**	**100,0**

Fonte: O autor

Voltando à discussão sobre a importância de uma ferramenta no intuito de seguir o planejamento de rastreabilidade e agora adicionando características a essas ferramentas de valores explícitos em normas reguladoras tentamos entender como os respondentes buscam ferramentas que detenham essa característica.

Na Tabela 10 observamos que para os respondentes que entendem o planejamento de rastreabilidade como uma boa prática 66,7% gostariam de uma ferramenta com característica de verificar valores explícitos oriundos de normas reguladoras e 33,3% que esta deveria ser uma característica mandatória. Entre os que entendem o planejamento como necessário apenas 25% gostariam que ferramentas de auxilio ao planejamento de rastreabilidade tivessem estes valores de forma mandatória e 75% achariam útil.

Tabela 10 - Relacionamento entre Q2 e Q5 – Importância da inserção de valores explícitos em norma reguladores em ferramentas de auxilio ao planejamento de rastreabilidade

RESPOSTAS PARA QUESTÃO 5	RESPOSTAS PARA QUESTÃO 2	
	Boa prática	Necessário
Útil	66,7	75,0
O uso deveria ser mandatório	33,3	25,0
TOTAL (%)	**100,0**	**100,0**

Fonte: O autor

Considerando aquele que realmente consideram o **uso** de uma ferramenta de auxilio importante tentando na Tabela 11 entender o quão os respondentes esperam que estas ferramentas verifiquem valores explícitos de normas reguladoras.

Para aqueles que consideram uma boa prática os usos de ferramentas 100% entendem ser útil a verificação de valores explícitos em normas e apar àqueles que acham necessário o uso de ferramentas 57,1% desejam ter esses valores

verificados por elas e 42,9% acham que é mandatório que ferramentas desse tipo tenham essa característica.

Estes dados reforçam que as ferramentas de auxilio a manutenção de rastreabilidade devem estar atualizadas com elementos de normas reguladoras, o que, no final, agregará valor as documentações que podem ser geradas, também, através dessas ferramentas.

Tabela 11 – Relacionamento entre Q3 e Q5 – Comportamento dos que consideram o uso de ferramentas importante entendem que estas devem ter valores de normas reguladoras

RESPOSTAS PARA QUESTÃO 5	**RESPOSTAS PARA QUESTÃO 3**	
	Boa prática	**Necessário**
Útil	100,0	57,1
O uso deveria ser mandatório	0,0	42,9
TOTAL (%)	**100,0**	**100,0**

Fonte: O autor

Considerando que alguns dos pontos previstos em de normas reguladoras para indústria médica que considera avaliar minuciosamente projetos de sistemas para dispositivos médicos, pois os mesmos pode trazer falhar que refletirão no projeto final e na tentativa de mitigar falhas inerentes ao projeto uma das abordagens é criar uma forma gerencial planejada de gerencia de rastreabilidade, tentamos entender na questão 6 a preocupação dos indivíduos envolvidos na pesquisa com esse tipo de requisito.

As respostas obtidas, organizadas na Tabela 12, foram que 50% entendem como ‘Mandatório’, 45,5% como importante e 4,5% acham pouco importante. Entre os estudantes de computação e engenharia elétrica em 58,3% consideram e 41,7% consideram importante, nenhum deles considerou uma prática pouco importante. Já para os engenheiros eletricistas 100% disseram ser uma prática pouco importante. Já para profissionais de computação 44,4% acham uma prática mandatória e 55,6% consideram importante.

Tabela 12 – Questão 6: Como você avalia a importância de usar uma abordagem de gerenciamento de rastreabilidade planejada na diminuição de problemas com manutenção de design de projetos para indústria médica?

RESPOSTA	**TOTAL (%)**	**% POR PERFIL**		
		ESTUDANTE COMPUTAÇÃO OU ELETRICA	**PROFISSIONAL DE COMPUTÇÃO**	**ENGENHEIRO ELETRICISTA**
Mandatório	50,0	58,3	44,4	0,0
Importante	45,5	41,7	55,6	0,0
Um pouco importante	4,5	0,0	0,0	100,0

TOTAL (%)	**100,0**	**100,0**	**100,0**	**100,0**

Fonte: O autor

A diferença entre as questões 6 e 7 esta relacionada a diminuição de custos, na questão 7 o aspecto de planejar a rastreabilidade e evitar problemas no desenvolvimento do produto podem diminuir custos e isto foi considerado por 63,6% dos entrevistados como uma prática importante, foi mandatório para 31,8% e pouco importante para 4,5%.

Conferindo os dados na Tabela 13, temos que de acordo com os estudantes de computação entrevistados, 58,3% consideram importante o planejamento para diminuição de custos, 41,7% acham mandatório. Para os engenheiros eletricistas entrevistados todos (100%) consideram importante e entre os profissionais de computação 11,1% acham pouco importante, 22,2% mandatório e 66,7% dizem ser um fator importante na redução de custos.

Tabela 13 – Questão 7: Como você avalia a importância de usar uma abordagem de gerenciamento de rastreabilidade planejada na diminuição de custos no desenvolvimento de projeto para a indústria médica?

RESPOSTA	**TOTAL (%)**	**% POR PERFIL**		
		ESTUDANTE COMPUTAÇÃO OU ELETRICA	**PROFISSIONAL DE COMPUTÇÃO**	**ENGENHEIRO ELETRICISTA**
Importante	63,6	58,3	66,7	100,0
Mandatório	31,8	41,7	22,2	0,0
Um pouco importante	4,5	0,0	11,1	0,0
TOTAL (%)	**100,0**	**100,0**	**100,0**	**100,0**

Fonte: O autor

As praticas de planejamento de rastreabilidade também agregam valor à manutenção dos projetos de sistemas *safety-critical* uma relação entre as questões 6 e 7 tenta mostrar como se comportou os indivíduos envolvidos na pesquisa em uma relação de diminuição de falhas na manutenção de projetos e custos de manutenção dos mesmos. Podemos observar esse comportamento na Tabela 14.

Para os que entendem que é mandatório a abordagem de uma rastreabilidade planejada na tentativa de mitigar erros de manutenção, 45,5% acreditam que é importante na tentativa de diminuir custos com manutenção e 54,5% entendem que é mandatório.

Para os que entendem que é importante ter uma técnica como esta para auxiliar na manutenção, 80% acreditam, também, ser é importante para diminuição de custos, 10% acham que seria mandatório e os outros 10% que é pouco importante, ou seja, que não contribuiria com diminuição de custos na manutenção dos projetos.

Por fim, para àqueles que acham que um abordagem de planejamento de rastreabilidade é pouco importante, encontramos uma pequena contradição, pois 100% disseram que essa abordagem pode importante para diminuição nos custos.

Tabela 14 – Relacionamento entre Q6 e Q7 – Importância de técnicas de planejamento de rastreabilidade na diminuição de custos com manutenção de projeto

RESPOSTAS PARA QUESTÃO 7	RESPOSTAS PARA QUESTÃO 6		
	Mandatório	Importante	Pouco importante
Importante	45,5	80,0	100,0
Mandatório	54,5	10,0	0,0
Um pouco importante	0,0	10,0	0,0
TOTAL (%)	**100,0**	**100,0**	**100,0**

Fonte: O autor

Após levantar pontos a respeito de pontos mais conceituais, na questão 8 foi direcionado a entender quais dos indivíduos de fato usam ferramentas no modelagem de desenvolvimento de projetos. Do total 45,5% dizem sempre usar, 36,4% entender que o uso apenas é útil em caso de projetos grande e os 18,1% restantes usam apenas às vezes.

Entre os estudantes de computação e engenharia elétrica que estiveram envolvidos em projetos de pesquisa recentes na área da indústria médica 41,7% disseram sempre usar ferramentas de modelagem, 33,3% entenderam ser útil apenas em projetos grandes e 25% só usam às vezes. No perfil de profissionais de computação 44,4% sempre usam ou entendem útil apenas em projetos grandes e 11,2% usam apenas às vezes. Todos (100%) engenheiros eletricistas disseram usar, podemos observar esses valores organizados na Tabela 15.

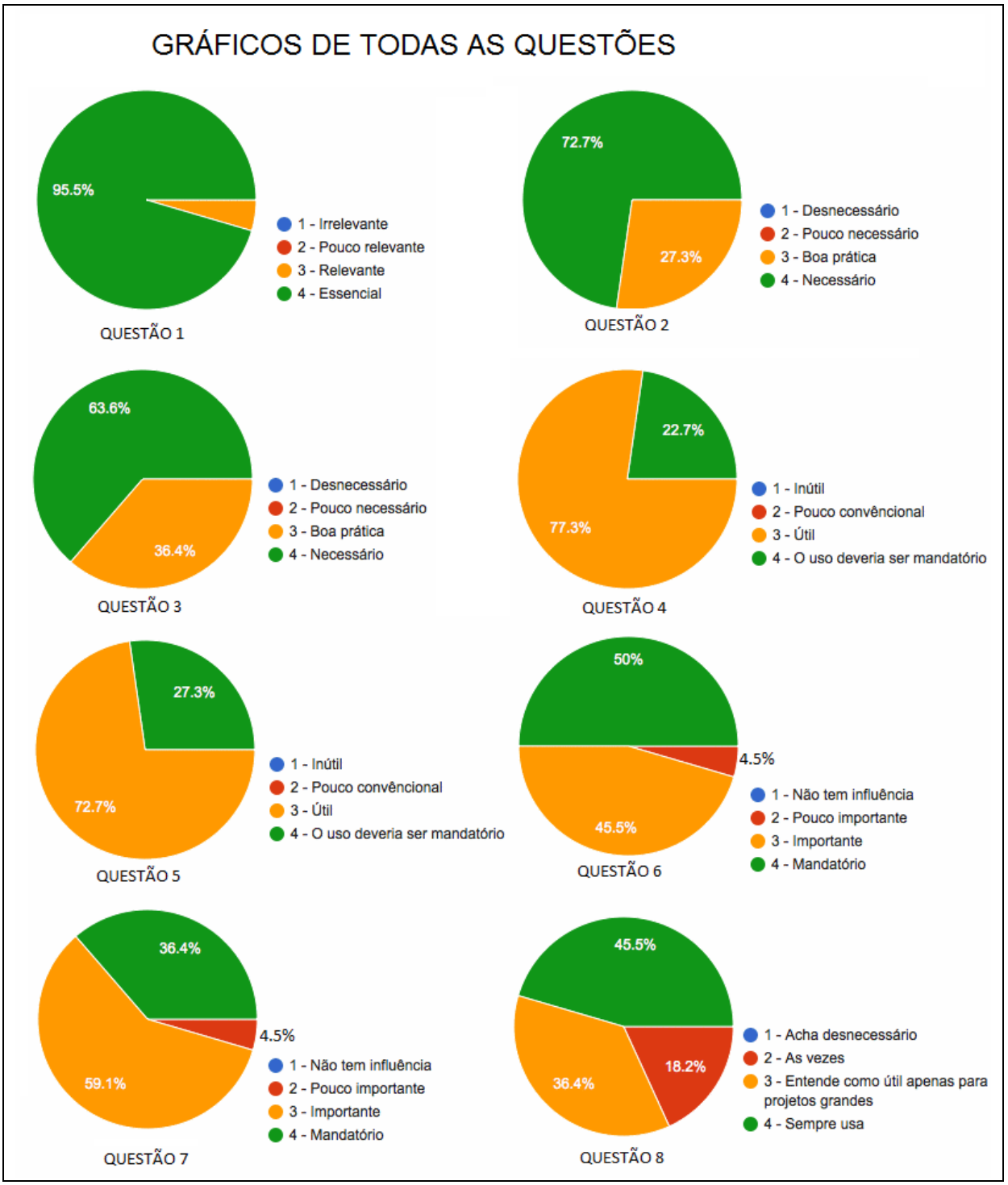
Tabela 15 – Questão 8: Você costuma usar alguma ferramenta de modelagem no desenvolvimento de projetos?

RESPOSTA	TOTAL (%)	% POR PERFIL		
		ESTUDANTE COMPUTAÇÃO OU ELETRICA	PROFISSIONAL DE COMPUTÇÃO	ENGENHEIRO ELETRICISTA
Sempre usa	45,5	41,7	44,4	100,0
Entende como útil apenas para projetos grandes	36,4	33,3	44,4	0,0
As vezes	18,1	25,0	11,2	0,0
TOTAL (%)	**100,0**	**100,0**	**100,0**	**100,0**

Fonte: O autor

A seguir na Figura 1 podemos verificar como se comportaram de forma geral todas respostas por questão. Nota-se que a grande maioria das respostas mostra a importância da necessidade de modelos de planejamento de rastreabilidade e de ferramentas para auxilio no gerenciamento da mesma, adicionando necessidade de análise de riscos em projetos desse segmento.

Figura 1 - Gráficos de todas as questões



Fonte: O autor

APÊNDICE B – QUESTIONÁRIO SOBRE PRATICA DE DECOMPOSIÇÃO DE REQUISITOS DE SAFETY COM ANALISE DE RISCOS PARA INDÚSTRIA DE DISPOSITIVOS MÉDICOS

UNIVERSIDADE ESTADUAL DA PARAÍBA

CENTRO DE CIÊNCIAS EXATAS E DA TERRA - CCT

PROGRAMA DE PÓS GRADUAÇÃO EM CIÊNCIA E TECNOLOGIA EM SAÚDE – PPCTS

A. Você é um?

( ) Estudante de computação/engenharia elétrica ( ) Profissional de computação

( ) Engenheiro Eletricista ( ) Other:

1. Como você avalia o uso da análise prévia de riscos no apoio a tomada de decisões arquiteturais de um sistema para dispositivos médicos?

( ) 1 - Irrelevante

( ) 2 - Pouco relevante

( ) 3 - Relevante

( ) 4 - Essencial

2. No tocante certificação de dispositivos médicos diante agências reguladoras, como você avalia necessidade de apresentar elementos das normas reguladoras na documentação arquitetural de dispositivo médico?

( ) 1 - Desnecessário

( ) 2 - Pouco necessário

( ) 3 - Boa prática

( ) 4 - Necessário

3. Como você entende a necessidade de ter um modelo para guiar o planejamento de rastreabilidade entre requisitos de safety decompostos e elementos arquiteturais do sistema?

( ) 1 - Desnecessário

( ) 2 - Pouco necessário

( ) 3 - Boa prática

( ) 4 - Necessário

4 - O quão útil seria para você ter uma ferramenta que, de forma automatizada, lhe guiasse na manutenção e na gerência da rastreabilidade entre: os elementos da análise de riscos, os requisitos de safety decompostos e os elementos arquiteturais do sistema?

( ) 1 - Inútil

( ) 2 - Pouco convêncional

( ) 3 - Útil

( ) 4 - O uso deveria ser mandatório

5 - O quão útil para você seria usar uma ferramenta que lhe guiasse no tocante a definição e manutenção de parâmetros dos elementos (por exemplo, Software Safety Class) de um projeto, parâmetros esses exigidos por normas técnicas reguladoras na indústria de dispositivos médicos?

( ) 1 - Inútil

( ) 2 - Pouco convêncional

( ) 3 - Útil

( ) 4 - O uso deveria ser mandatório

6 - Como você avalia a importância de usar uma abordagem de gerenciamento de rastreabilidade planejada na diminuição de problemas com manutenção de design de projetos para indústria médica ?

( ) 1 - Não tem influência

( ) 2 - Pouco importante

( ) 3 - Importante

( ) 4 - Mandatório

7 - Como você avalia a importância de usar uma abordagem de gerenciamento de rastreabilidade planejada na diminuição de custos no desenvolvimento de projeto para a indústria médica?

( ) 1 - Não tem influência

( ) 2 - Pouco importante

( ) 3 - Importante

( ) 4 - Mandatório

8 - Você costuma usar alguma ferramenta de modelagem no desenvolvimento de projetos? Em caso de nunca ter desenvolvido nenhum projeto na prática considere seus conhecimentos teóricos.

( ) 1 - Acha desnecessário

( ) 2 - As vezes

( ) 3 - Entende como útil apenas para projetos grandes

( ) 4 - Sempre usa