

UNIVERSIDADE FEDERAL DE JUIZ DE FORA
PROGRAMA DE PÓS-GRADUAÇÃO EM MODELAGEM
COMPUTACIONAL - PPGMC/UFJF
ENGENHARIA DE SOFTWARE

Eduardo Santos de Oliveira Marques
Gustavo Santos de Oliveira Marques
Sara Crislei de Souza Soares

Projeto de Engenharia de Software: Bomba de Insulina

LISTA DE ILUSTRAÇÕES

Figura 1 – ERF da configuração de Taxa Basal Personalizada	10
Figura 2 – ERF da Calculadora de Bolus Automático	11
Figura 3 – ERF dos Alarmes de níveis de Glicose Fora do Intervalo-alvo	11
Figura 4 – ERF da Conectividade com Monitor Contínuo de Glicose (CGM)	11
Figura 5 – Diagrama de Definição de Blocos da Bomba de Insulina	14
Figura 6 – Diagrama de Blocos SIL	17
Figura 7 – Diagrama de Blocos Interno e Diagrama de Classes do Sistema de Infusão	25
Figura 8 – Diagrama de Blocos Interno e Diagrama de Classes do Sistema de Controle	25
Figura 9 – Diagrama de Blocos Interno e Diagrama de Classes do Sistema de Interface	26
Figura 10 – Diagrama de Blocos Interno e Diagrama de Classes do Sistema de Comunic.	26
Figura 11 – Elementos Utilizados para Construir uma Fault Tree Analysis	27
Figura 12 – Fault Tree Analysis - Administração Incorreta de Insulina	27
Figura 13 – Fault Tree Analysis - Falha no Fornecimento de Insulina	28
Figura 14 – Fault Tree Analysis - Falha no Monitoramento dos Níveis de Glicose . .	28
Figura 15 – Fault Tree Analysis - Falha no Sistema de Alarme	29
Figura 16 – Fault Tree Analysis - Vazamento de Insulina	29
Figura 17 – Fault Tree Analysis - Erros de Configuração do Usuário	30

LISTA DE TABELAS

Tabela 1 – Requisitos Não Funcionais	12
Tabela 2 – Análise de Riscos	16
Tabela 3 – SIL associado aos perigos	18
Tabela 4 – Análise dos Modos de Falha e seus Efeitos - FMEA	31

LISTA DE ABREVIATURAS E SIGLAS

AADL	Architecture Analysis and Design Language
ASIL	Automotive Safety Integrity Level
CIA	Confidentiality, Integrity and Availability
CGM	Continuous Glucose Monitors
CHESS	CHaining Environmental Web ServiceS
DAL	Design Assurance Level
ERF	Especificação de Requisitos Funcionais
FMEA	Failure Modes and Effects Analysis
FDA	Food and Drug Administration
FTA	Fault Tree Analysis
HARA	Hazard Analysis & Risk Assessment
HiP-HOPS	Highly Integrated and Professional Hazard and Operability Study
OSATE	Open Source Architectural Environment Tool
RNF	Especificação de Requisitos Não Funcionais
SIL	Safety Integrity Level
SysML	Systems Modeling Language
UML	Unified Modeling Language

SUMÁRIO

1	DESCRIÇÃO DO PROJETO	5
2	ESCOPO DO SISTEMA	6
2.1	OBJETIVOS	7
2.2	USUÁRIOS	7
2.3	AMBIENTE OPERACIONAL	8
3	CARACTERIZAÇÃO DAS PARTES INTERESSADAS	9
4	ESPECIFICAÇÃO DOS REQUISITOS	10
4.1	FUNCIONAIS	10
4.2	NÃO-FUNCIONAIS	12
4.3	RESTRIÇÕES DO SISTEMA	12
5	PROJETO ARQUITETURAL PRELIMINAR	14
6	ANÁLISE DE RISCO	16
6.1	HAZARD ANALYSIS & RISK ASSESSMENT	16
6.2	ALOCÇÃO DE SIL	17
6.3	THREAT ANALYSIS & RISK ASSESSMENT	19
6.4	ESPECIFICAÇÃO DOS REQUISITOS DE PROCESSO	20
6.4.1	Sistema de Infusão	20
6.4.2	Sistema de Controle	21
6.5	MODELAGEM DE PROCESSO DE SOFTWARE	22
6.5.1	Sistema de Infusão	22
6.5.2	Sistema de Controle	23
7	PROJETO DE SOFTWARE	24
7.1	MODELAGEM LÓGICA DE FALHAS	27
7.1.1	Análise das Árvores de Falhas	27
7.1.2	Análise de Modos de Falha e seus Efeitos - (FMEA)	30
7.2	FERRAMENTAS DE MODEL-BASED SAFETY ANALYSIS	33
8	IMPLEMENTAÇÃO E EXECUÇÃO DO SOFTWARE	34
8.1	ARQUITETURA	36
8.2	FLUXO GERAL	37
9	TESTE DE SOFTWARE	38
9.1	TESTE FUNCIONAL	38
9.2	TESTE ESTRUTURAL	39
9.3	TESTE BASEADO EM DEFEITOS	39
9.4	RESULTADOS DA EXECUÇÃO DOS CASOS DE TESTE	40
10	CONCLUSÃO	41
	REFERÊNCIAS	43

1 DESCRIÇÃO DO PROJETO

O presente trabalho envolve a execução de um projeto de Engenharia de Software de uma Bomba de Infusão de Insulina, com domínio de aplicação em dispositivos médicos. Esse projeto segue as seguintes etapas:

- I Especificação de Requisitos de Software:** Documento de requisitos, projeto arquitetural preliminar, Hazard Analysis & Risk Assessment (HARA), alocação de SILs/DALs/ASILs para mitigar os efeitos de cada hazard, requisitos de segurança de produto e de processo (em termos de objetivos, atividades, guidance e artefatos);
- II Projeto de Software:** Projeto arquitetural detalhado de cada subsistema utilizando o Diagrama de Blocos Interno (Internal Block Diagram) da SysML e Diagramas de Classes da UML para modelagem das estruturas de dados. Modelagem lógica falhas (Failure Logic Modeling) utilizando Fault Tree Analysis (FTA) e Failure Modes and Effects Analysis (FMEA). Ferramentas de Model-Based Safety Analysis como: CHES Framework e Concerto-Failure Logic Analysis, Matlab Simulink e HiP-HOPS ou OSATE-AADL;
- III Implementação e Execução do Software:** Implementação ou geração o código fonte do sistema em C, C++, Ada ou Java e executar a simulação do modelo. Entrega do código fonte da implementação e um relatório com a descrição da arquitetura do sistema e da execução do código;
- IV Teste de Software:** Produção de um relatório com a especificação e resultados da execução de Casos de Teste para uma determinada funcionalidade do sistema projetado aplicando as técnicas de Teste Funcional, Teste Estrutural, i.e., critérios baseados em fluxo de controle e em fluxo de dados, e Teste Baseado em Defeitos.

Na Etapa I, o relatório segue com as seguintes informações: Especificação de requisitos do Sistema, Projeto Arquitetural Preliminar do sistema utilizando o Diagrama de Definição de Blocos (Block Definition Diagram) da SysML, realização de atividades de Hazard Analysis & Risk Assessment (HARA), alocação de SILs/DALs/ASILs para mitigar os efeitos de cada hazard, decomposição SILs/DALs/ASILs alocados aos hazards às falhas de componentes, especificação dos requisitos de segurança (Functional Safety Requirements – negação dos hazards e de falhas de componentes); realização de atividades de Threat Analysis & Risk Assessment para identificar as ameaças de ataques cibernéticos que podem afetar as propriedades de Confidencialidade, Integridade e Disponibilidade (Propriedades CIA) de dados ou do sistema e especificação dos requisitos segurança cibernética; Especificação dos Requisitos de Processo para dois subsistemas de acordo com os SILs/DALs/ASILs e Modelagem de Processo de Software para esses dois subsistemas.

2 ESCOPO DO SISTEMA

A insulina é um hormônio/hormona produzido pelas células beta das ilhotas de Langerhans (localizado no pâncreas). Ela desempenha um papel fundamental no metabolismo do corpo. A sua função principal é regular os níveis de glicose no sangue. A glicose é uma fonte de energia para as células do corpo, atuando como uma chave que permite que a glicose entre nas células, onde pode ser utilizada como energia ou armazenada para uso posterior [1].

Ela é obtida na ingestão de alimentos que contêm carboidratos, tais como pão, arroz, frutas e doces; o sistema digestivo quebra esses carboidratos em glicose, que é absorvida pela corrente sanguínea. Além de regular o metabolismo da glicose, a insulina também desempenha outras funções importantes, como a promoção do armazenamento de gordura, inibição da produção de glicose pelo fígado e estimulação do crescimento celular.

A falta de insulina ou a incapacidade do organismo de usar a insulina de forma eficaz leva a uma condição chamada diabetes. No diabetes tipo 1, o corpo não produz insulina suficiente, enquanto no diabetes tipo 2, o corpo não consegue utilizar a insulina adequadamente. Em ambos os casos, o controle dos níveis de glicose no sangue é comprometido, e o tratamento geralmente envolve a administração de insulina exógena (por injeção ou bomba de infusão) para regular os níveis de açúcar no sangue.

Uma Bomba de Infusão de Insulina é um dispositivo médico usado para administrar insulina de forma contínua e controlada a pacientes com diabetes. Essas bombas são projetadas para liberar doses precisas de insulina ao longo do dia, imitando o processo natural de secreção de insulina pelo pâncreas.

Para garantir a segurança e a confiabilidade do dispositivo, é preciso seguir as diretrizes do padrão IEC 61508 [2], uma norma internacional que especifica os requisitos funcionais e de segurança para sistemas elétricos, eletrônicos e programáveis relacionados à segurança.

Além disso, existe o documento “Infusion Pumps Total Product Life Cycle” [3] produzido pela FDA (Food and Drug Administration) [4], a agência reguladora de medicamentos e alimentos nos Estados Unidos. Ele fornece orientações abrangentes para a fabricação, teste, uso e manutenção de bombas de infusão, incluindo bombas de infusão de insulina. Esse documento aborda o ciclo de vida completo do produto e destaca as diretrizes de segurança e qualidade para esses dispositivos.

2.1 OBJETIVOS

Os principais objetivos do Sistema de uma Bomba de Insulina são:

- **Entrega precisa:** O principal objetivo de uma Bomba de Insulina é fornecer uma dose precisa de insulina para pessoas com diabetes. Isso envolve a administração de doses regulares do hormona de acordo com as necessidades individuais do usuário;
- **Controle do nível de glicose:** O sistema visa manter os níveis de glicose no sangue do usuário dentro de um intervalo saudável. Isso é alcançado ao calcular e ajustar a quantidade de insulina necessária com base em informações como dieta, atividade física, nível de glicose atual e configurações personalizadas;
- **Flexibilidade e conveniência:** A bomba tem como objetivo fornecer flexibilidade aos usuários, permitindo que eles ajustem a administração de insulina de acordo com suas necessidades diárias. Além disso, ela oferece a comodidade de evitar injeções frequentes de insulina, uma vez que o dispositivo é conectado ao corpo do usuário e administra a insulina automaticamente.

2.2 USUÁRIOS

Os possíveis usuários desse sistema podem ser pacientes com os dois tipos de diabetes mencionados anteriormente, sendo eles:

- **Tipo 1:** A bomba de insulina é frequentemente usada por pessoas com diabetes tipo 1, que requerem uma administração regular de insulina para manter os níveis de glicose sob controle. Esses usuários geralmente têm conhecimento sobre diabetes e estão familiarizados com o uso da insulina;
- **Tipo 2:** Em certos casos, pacientes com diabetes tipo 2 que não conseguem controlar adequadamente sua glicose apenas com medicamentos orais podem ser prescritos para usar uma bomba de insulina.

É importante ressaltar que não são todos os casos de pacientes com diabetes do tipo 2 que precisam de uma Bomba de Insulina, apenas em situações em que os medicamentos não são o suficiente. Para o caso do tipo 1, a sua utilização se torna obrigatória.

2.3 AMBIENTE OPERACIONAL

As características do ambiente operacional do sistema são as seguintes:

- **Portabilidade:** As bombas de insulina são dispositivos portáteis e geralmente são usadas no corpo do usuário. Eles são projetados para serem leves e compactos, permitindo que os usuários os levem consigo durante todo o dia;
- **Conectividade sem fio:** Muitas bombas possuem recursos de conectividade sem fio, permitindo que sejam conectadas a outros dispositivos, como monitores contínuos de glicose (CGMs) ou smartphones. Isso facilita o monitoramento contínuo dos níveis de glicose e o ajuste das configurações da bomba;
- **Interface intuitiva:** O sistema possui uma interface fácil de usar, geralmente com botões e uma tela para configurar e ajustar as doses de insulina. As informações exibidas devem ser claras e compreensíveis para o usuário, facilitando o acompanhamento do tratamento;
- **Alarmes e alertas:** O dispositivo pode fornecer alarmes e alertas para notificar o usuário sobre várias condições, como baixo nível de bateria, suspensão da administração de insulina, níveis de glicose fora do intervalo alvo ou necessidade de recarregar ou substituir o reservatório;
- **Segurança e resistência à água:** O sistema da bomba de insulina deve ser resistente à água e projetado para garantir a segurança do usuário. Isso é importante, pois o dispositivo estará em contato com a pele do usuário durante todo o tempo e pode estar exposto a diferentes condições ambientais.

É importante ressaltar que as características e funcionalidades específicas podem variar entre diferentes marcas e modelos de Bombas de Insulina disponíveis no mercado.

3 CARACTERIZAÇÃO DAS PARTES INTERESSADAS

As partes interessadas (usuários e stakeholders) de uma Bomba de Insulina são os seguintes grupos:

1. **Usuários Finais (Pacientes com Diabetes tipo 1 ou 2):** Pessoas que utilizam a bomba de insulina no seu dia a dia para controlar os níveis de glicose no sangue. Eles são os principais beneficiários do sistema e dependem dele para administrar a insulina de forma precisa e conveniente;
2. **Médicos e Especialistas em Diabetes:** Os profissionais de saúde desempenham um papel fundamental na prescrição, acompanhamento e ajuste das configurações da bomba de insulina. Eles são responsáveis por determinar as doses adequadas de insulina, monitorar os resultados e auxiliar os pacientes na gestão do tratamento;
3. **Famíliares e Cuidadores:** Desempenham um papel importante no suporte aos usuários da Bomba de Insulina. Eles podem estar envolvidos no processo de administração da insulina, monitoramento dos níveis de glicose, ajuste das configurações da bomba e fornecimento de apoio emocional;
4. **Fabricantes da Bomba de Insulina:** São os stakeholders responsáveis pelo desenvolvimento, produção e comercialização das bombas de insulina. Elas investem em pesquisa e desenvolvimento, garantindo a segurança e a eficácia do produto, fornecem suporte técnico e atualizações do sistema;
5. **Seguradoras e Sistemas de Saúde:** Empresas que dão suporte e reembolso dos custos associados à Bomba de Insulina. Eles influenciam o acesso dos pacientes ao sistema, estabelecendo políticas de cobertura e critérios de elegibilidade;
6. **Autoridades Reguladoras e Agências de Saúde:** Desempenham um papel fundamental na supervisão e na regulamentação das bombas de insulina. Elas estabelecem diretrizes, normas de segurança e eficácia, e garantem que os dispositivos atendam aos padrões exigidos;
7. **Grupos de Defesa de Pacientes e Associações Médicas:** Associações que representam os interesses dos pacientes com diabetes e profissionais de saúde envolvidos no tratamento da doença. Eles desempenham um papel importante na advocacia, na educação e no apoio aos usuários da bomba de insulina, bem como na promoção de melhores práticas e avanços na área.

É importante considerar que a interação e colaboração entre esses grupos são fundamentais para o desenvolvimento, aprimoramento e utilização efetiva desses sistemas para o tratamento do diabetes.

4 ESPECIFICAÇÃO DOS REQUISITOS

A Especificação dos Requisitos envolve identificar, documentar e descrever de forma clara e precisa os requisitos funcionais e não funcionais de um sistema. Os requisitos são as necessidades, restrições e expectativas que o sistema deve atender para satisfazer os objetivos do projeto. Ela geralmente inclui os seguintes elementos:

1. **Funcionais:** Funcionalidades e capacidades que o sistema deve fornecer. Descrevem o que o sistema deve fazer em termos de entradas, processamento e saídas;
2. **Não Funcionais:** Critérios de qualidade e restrições do sistema que não se relacionam diretamente com funcionalidades específicas, mas com características do sistema como desempenho, segurança, usabilidade, confiabilidade, entre outros;
3. **Restrições do Sistema:** Requisitos que estabelecem restrições ao projeto, como restrições de orçamento, prazos, tecnologias a serem utilizadas ou requisitos legais e regulatórios.

4.1 FUNCIONAIS

As Especificações de Requisitos Funcionais (ERF) foram definidas de acordo com a taxa basal, bolus, níveis de glicose e monitoramento. A taxa basal diz respeito a administração de insulina ao longo do dia; e o bolus é a dose de insulina necessária de acordo com outros fatores.

Figura 1 – ERF da configuração de Taxa Basal Personalizada

Identificador (RF01): Configuração de Taxa Basal Personalizada	
Interessado (s)/Stakeholder (s):	Usuário (Paciente com diabetes)
Pré-condição (ões):	A bomba de insulina está pronta para configuração
Descrição:	O usuário deve ser capaz de configurar taxas basais personalizadas, que são taxas de administração contínua de insulina ao longo do dia, de acordo com as necessidades individuais. O usuário pode definir diferentes taxas basais para períodos específicos, como basal padrão durante a noite e basal reduzida durante o exercício.
Pós-condição (ões):	A bomba de insulina armazena e aplica automaticamente as taxas basais configuradas pelo usuário ao longo do período especificado, garantindo a administração correta e contínua de insulina.

Figura 2 – ERF da Calculadora de Bolus Automático

Identificador (RF02): Calculadora de Bolus Automático	
Interessado (s)/Stakeholder (s):	Usuário (Paciente com diabetes)
Pré-condição (ões):	As configurações de bolus e fatores de correção estão definidos na bomba de insulina.
Descrição:	A bomba de insulina deve fornecer uma calculadora de bolus automático que ajuda o usuário a determinar a dose de insulina necessária com base em fatores como níveis de glicose, quantidade de carboidratos consumidos e fatores de correção. O usuário insere as informações relevantes, e a bomba calcula a dose recomendada.
Pós-condição (ões):	A bomba de insulina exibe a dose de bolus recomendada, permitindo que o usuário confirme e administre a dose correta de insulina para refeições ou correções.

Figura 3 – ERF dos Alarmes de níveis de Glicose Fora do Intervalo-alvo

Identificador (RF03): Alarmes de Níveis de Glicose Fora do Intervalo-alvo	
Interessado (s)/Stakeholder (s):	Usuário (Paciente com diabetes)
Pré-condição (ões):	A bomba de insulina está em uso e os limites do intervalo-alvo de glicose estão definidos.
Descrição:	A bomba de insulina deve monitorar continuamente os níveis de glicose e emitir um alarme quando eles estiverem fora do intervalo-alvo definido pelo usuário. Isso ajuda o usuário a tomar medidas adequadas para corrigir a hiperglicemia ou a hipoglicemia.
Pós-condição (ões):	O usuário é notificado por meio de um alarme sonoro, visual ou vibratório, indicando que os níveis de glicose estão fora do intervalo-alvo e requerem ação imediata.

Figura 4 – ERF da Conectividade com Monitor Contínuo de Glicose (CGM)

Identificador (RF04): Conectividade com Monitor Contínuo de Glicose (CGM)	
Interessado (s)/Stakeholder (s):	A bomba de insulina e o dispositivo CGM estão pareados e conectados.
Pré-condição (ões):	A bomba de insulina e o dispositivo CGM estão pareados e conectados.
Descrição:	A bomba de insulina deve ser capaz de se conectar a um dispositivo de Monitor Contínuo de Glicose (CGM) para receber leituras em tempo real dos níveis de glicose do usuário. Os dados do CGM são usados para ajustar as doses de insulina e auxiliar na tomada de decisões de tratamento.
Pós-condição (ões):	A bomba de insulina exibe as leituras de glicose em tempo real do dispositivo CGM, permitindo ao usuário monitorar e tomar medidas adequadas para manter os níveis de glicose sob controle.

4.2 NÃO-FUNCIONAIS

As Especificações de Requisitos Não Funcionais (RNF) foram definidos considerando as seguintes categorias: confiabilidade, segurança, usabilidade, portabilidade e tecnologia.

Tabela 1 – Requisitos Não Funcionais

Identificador	Descrição	Categoria
RNF01	A bomba de insulina deve ser altamente confiável	Confiabilidade
RNF02	Deve possuir recursos de segurança tais como proteção contra overdose, bloqueio de tela e medidas para prevenir falhas técnicas	Segurança
RNF03	Deve ser fácil de usar mesmo por pacientes com limitações	Usabilidade
RNF04	Preferível que seja portátil e compacta para utilizar no dia a dia	Portabilidade
RNF05	A duração da bateria deve ser o suficiente para atender às necessidades diárias	Confiabilidade
RNF06	Uma bomba resistente à água é desejável para utilização durante o banho	Usabilidade e Confiabilidade
RNF07	Capacidade de comunicação e sincronização de dados com demais sistemas	Tecnologia
RNF08	Manutenção e suporte adequados	Confiabilidade

4.3 RESTRIÇÕES DO SISTEMA

As restrições de sistema para uma Bomba de Insulina podem variar dependendo do projeto específico e dos requisitos do dispositivo, mas no geral elas incluem:

- **Restrições Tecnológicas:** Envolvem requisitos específicos relacionados às tecnologias utilizadas na bomba de insulina, como componentes eletrônicos de baixa potência, sensores de glicose, conectividade sem fio e baterias duradouras;
- **Compatibilidade com Plataformas Operacionais:** É necessário garantir que a bomba seja compatível com determinadas plataformas operacionais, como sistemas operacionais móveis ou sistemas de gerenciamento de dados específicos;
- **Interoperabilidade com Outros Sistemas:** É importante considerar a interoperabilidade do dispositivo com outros sistemas de saúde, como sistemas de monitoramento contínuo de glicose (CGM), aplicativos móveis de monitoramento ou softwares de gerenciamento de dados;

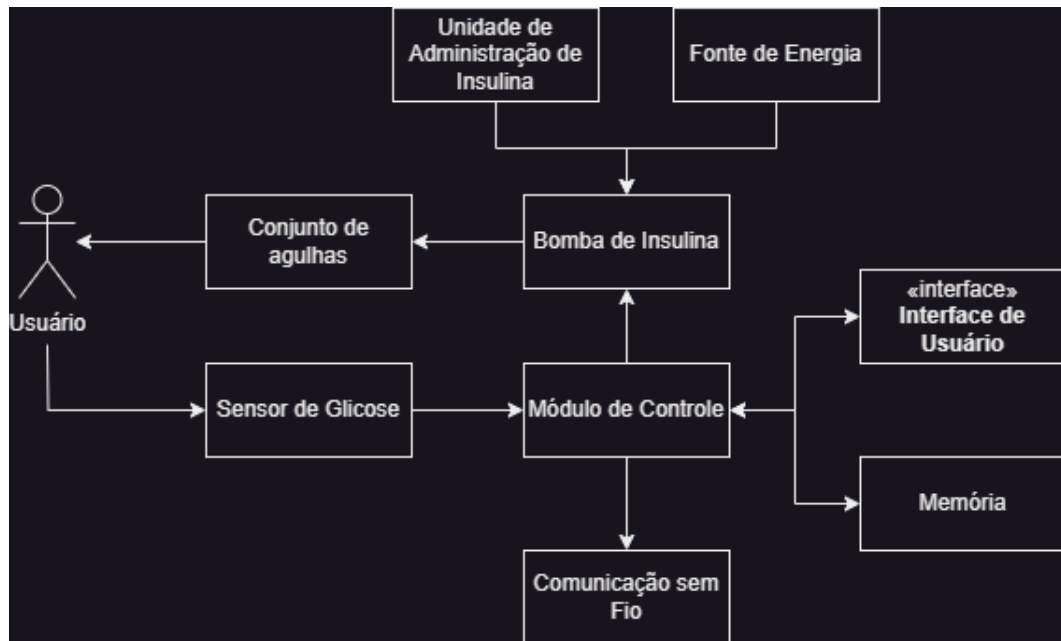
- **Bancos de Dados Legados:** Em alguns casos, pode haver a necessidade de interoperabilidade com bancos de dados legados, como sistemas de registros médicos eletrônicos (EMR) ou sistemas de gerenciamento de pacientes. A Bomba de Insulina pode precisar ser capaz de enviar e receber dados relevantes desses sistemas;
- **Restrições Regulatórias e de Segurança:** O equipamento deve atender a requisitos regulatórios específicos, como padrões de segurança estabelecidos pelas autoridades de saúde competentes. Isso pode incluir conformidade com padrões de segurança e certificações relevantes.

É importante ressaltar que essas são apenas algumas restrições comuns associadas às bombas de insulina, e as restrições específicas podem variar dependendo do projeto, das regulamentações aplicáveis e das necessidades clínicas do paciente.

5 PROJETO ARQUITETURAL PRELIMINAR

Abaixo é apresentado o Projeto Arquitetural Preliminar através do Diagrama de Definição de Blocos (Block Definition Diagram) da SysML, sendo realizado com o auxílio do site <https://app.diagrams.net/> [5].

Figura 5 – Diagrama de Definição de Blocos da Bomba de Insulina



1. **Unidade de Administração de Insulina:** Representa o subsistema responsável pela administração controlada de insulina. Pode incluir componentes como um motor de bombeamento, câmara de insulina, agulha, sensores de glicose, sistema de controle de fluxo, entre outros;
2. **Fonte de Energia:** Representa o subsistema de energia que fornece energia para a Bomba de Insulina. Pode incluir uma bateria recarregável, circuitos de carregamento, gerenciamento de energia e proteção contra falhas;
3. **Bomba de Insulina:** Representa a própria Bomba de Insulina como um todo, que é o sistema a ser projetado;
4. **Conjunto de Agulhas:** Representa o conjunto de agulhas utilizado na bomba de insulina. O conjunto de agulhas é responsável pela inserção da agulha no corpo do usuário para administrar a insulina. Pode incluir elementos como a agulha propriamente dita, um dispositivo de inserção, um dispositivo de fixação e outras partes relacionadas;

5. **Sensor de Glicose:** Representa o sensor de glicose usado na bomba de insulina. O sensor de glicose é responsável por medir os níveis de glicose no sangue do usuário. Pode ser um sensor contínuo que fornece leituras em tempo real ou um sensor que requer inserções periódicas para medição. O bloco pode incluir componentes como o sensor em si, um dispositivo de monitoramento e outros elementos relacionados;
6. **Módulo de Controle:** Representa o subsistema responsável pelo controle e monitoramento do funcionamento da Bomba de Insulina. Isso pode envolver um microcontrolador ou microprocessador, sensores de pressão, sensores de nível de insulina, algoritmos de controle, entre outros;
7. **Interface de Usuário:** Representa a interface através da qual o usuário interage com a Bomba de Insulina. Isso pode incluir botões, telas, alarmes sonoros e outros elementos de interação;
8. **Memória:** Representa a memória utilizada na bomba de insulina. A memória é responsável por armazenar dados importantes, como configurações do usuário, registros de administração de insulina, leituras de glicose e outros dados relevantes. Pode ser uma memória não volátil que retém informações mesmo quando a energia é desligada. O bloco pode incluir componentes como chips de memória, controladores de memória e interfaces de acesso à memória;
9. **Comunicação sem Fio:** Representa o subsistema responsável pela comunicação da bomba de insulina com outros dispositivos ou sistemas externos, como aplicativos móveis, sistemas de monitoramento contínuo de glicose (CGM) ou sistemas de gerenciamento de dados. Isso pode envolver tecnologias sem fio, como Bluetooth ou Wi-Fi.

Cada bloco desempenha um papel específico na funcionalidade e operação geral do sistema. As relações e conexões existentes entre os blocos formam uma arquitetura completa e coerente, fornecendo comunicações entre o dispositivo como um todo.

6 ANÁLISE DE RISCO

6.1 HAZARD ANALYSIS & RISK ASSESSMENT

A seguir é mostrada a identificação e avaliação de riscos específicos relacionados a Bomba de Insulina. São apresentados os perigos, causas, consequências e medidas de mitigação que poderiam ser considerados durante a análise de risco com base no Diagrama de Definição de Blocos preliminar.

Tabela 2 – Análise de Riscos

Perigo	Causas	Consequências	Mitigação
Administração incorreta de insulina.	Erro de dosagem, falha no reconhecimento da dose programada, erros de calibração do sistema de infusão.	Hipoglicemia grave, hiperglicemia descontrolada, complicações de saúde.	Implementação de verificações duplas de dosagem, alarmes visuais e sonoros de dose incorreta, interface de usuário intuitiva para programação da dose.
Falha no fornecimento de insulina.	Bloqueio na câmara de insulina, falha mecânica no sistema de infusão, falta de energia.	Interrupção na administração de insulina, risco de hiperglicemia descontrolada.	Mecanismos de detecção de bloqueio, alarmes de falha no fornecimento de insulina, bateria de backup ou sistemas de alimentação redundantes.
Falha no monitoramento dos níveis de glicose.	Calibração incorreta do sensor de glicose, falha no sensor de glicose, falta de comunicação com o sistema de monitoramento.	Administração incorreta de insulina, falta de informação sobre os níveis de glicose.	Calibração regular do sensor de glicose, alarmes de falha de comunicação, sistema de monitoramento de backup.
Falha no sistema de alarme.	Falha no sensor de glicose, falha no sistema de comunicação, defeito no sistema de alarme	Ausência de alertas para níveis de glicose anormais, falha em notificar o usuário sobre condições críticas	Testes regulares do sistema de alarme, redundância nos sistemas de notificação, mecanismos de feedback do usuário.
Vazamento de insulina.	Falha na vedação do sistema de infusão, falha no controle de pressão, dano físico à câmara de insulina.	Perda de insulina, contaminação do ambiente, risco de infecção.	Materiais de vedação de qualidade, testes de vazamento, alarmes de detecção de vazamento, fácil acesso à limpeza e manutenção.
Erros de configuração do usuário.	Interface de usuário confusa, falta de orientação adequada, inserção incorreta de parâmetros	Administração incorreta de insulina, desequilíbrio dos níveis de glicose.	Interface de usuário intuitiva e amigável, instruções claras e orientações para configuração, verificações de validação dos parâmetros inseridos.

6.2 ALOCAÇÃO DE SIL

Para realizar a alocação de SIL (Nível de Integridade de Segurança - Safety Integrity Level), é necessário considerar a gravidade das consequências associadas a cada perigo identificado. Essa alocação é feita com o auxílio de uma tabela que indica a severidade das consequências e a sua probabilidade, mostrada na Figura abaixo.

Figura 6 – Diagrama de Blocos SIL

	Severity of Consequence				
Likelihood	Catastrophic (5)	Critical (4)	Marginal (3)	Minor (2)	Negligible (1)
Frequent (5)	-	-	-	SIL4	SIL3
Probable (4)	-	-	SIL4	SIL 3	SIL2
Occasional (3)	-	SIL4	SIL 3	SIL 2	SIL1
Remote (2)	SIL 4	SIL 3	SIL 2	SIL 1	-
Improbable (1)	SIL 3	SIL2	SIL 1	-	-

Considerando ordenando os perigos definidos na Tabela 2, a alocação do SIL para cada caso fica da seguinte forma:

1. Administração incorreta de insulina:

- a) **Probabilidade:** Improvável a Remota (falha no sistema);
- b) **Consequência:** Crítica (hipoglicemia grave, hiperglicemia descontrolada);
- c) **Alocação:** SIL 3 ou inferior;

2. Falha no fornecimento de insulina:

- a) **Probabilidade:** Improvável a Remota (falha no sistema);
- b) **Consequência:** Marginal a Crítica (interrupção na administração de insulina);
- c) **Alocação:** SIL 3 ou inferior;

3. Falha no monitoramento dos níveis de glicose:

- a) **Probabilidade:** Improvável a Remota (falha no sistema);
- b) **Consequência:** Marginal (administração incorreta, falta de informação);
- c) **Alocação:** SIL 2 ou superior (dependendo do erro na administração);

4. Falha no sistema de alarme:

- a) **Probabilidade:** Improvável a Remota (falha no sistema);
- b) **Consequência:** Insignificante a Menor (ausência de alertas para anomalias);
- c) **Alocação:** SIL 1 ou insignificante (dependendo da análise de risco detalhada);

5. Vazamento de insulina:

- a) **Probabilidade:** Remota a Ocasional (falha no sistema, erro do usuário);
- b) **Consequência:** Marginal (perda de insulina, contaminação, risco de infecção);
- c) **Alocação:** SIL 3 ou inferior (dependendo da análise de risco detalhada);

6. Erros de configuração do usuário:

- a) **Probabilidade:** Remota a Ocasional (erro do usuário);
- b) **Consequência:** Marginal a Crítico (administração incorreta, desequilíbrio);
- c) **Alocação:** SIL 4 ou inferior (dependendo do usuário em questão);

Tabela 3 – SIL associado aos perigos

Perigo	Probabilidade	Consequência	SIL
1	2	4	SIL 3
2	2	4	SIL 3
3	2	3	SIL 2
4	2	2	SIL 1
5	3	3	SIL 3
6	3	4	SIL 4

Essas são apenas sugestões gerais de alocação de SIL com base nos exemplos fornecidos. É importante ressaltar que a alocação de SIL adequada requer uma análise mais detalhada. Recomenda-se envolver especialistas em segurança funcional e seguir as normas e regulamentações relevantes (como a IEC 61508 mencionada anteriormente) para uma alocação de SIL precisa e confiável.

6.3 THREAT ANALYSIS & RISK ASSESSMENT

Ao realizar uma análise de ameaças (Threat Analysis) e avaliação de riscos (Risk Assessment) para identificar ameaças de ataques cibernéticos à Bomba de Insulina, é necessário considerar as propriedades de Confidencialidade, Integridade e Disponibilidade (CIA) dos dados e do sistema. Abaixo seguem as ameaças cibernéticas e suas potenciais consequências para a Bomba de Insulina.

- **Ataque de negação de serviço (DoS):** Interrupção da disponibilidade da bomba de insulina, impossibilitando a administração adequada de insulina;
- **Interceptação de comunicações:** Comprometimento da confidencialidade dos dados transmitidos entre a Bomba de Insulina e outros sistemas, resultando na exposição de informações sensíveis, como dados do usuário ou configurações de dosagem;
- **Manipulação de dados:** Modificação não autorizada de dados na bomba, levando a uma administração incorreta de insulina e desequilíbrio nos níveis de glicose;
- **Injeção de código malicioso:** Execução de código malicioso no dispositivo, podendo resultar em comportamento indesejado, acesso não autorizado a informações ou manipulação dos processos internos;
- **Exploração de vulnerabilidades:** Aproveitamento de falhas de segurança conhecidas ou desconhecidas na Bomba de Insulina para ganhar acesso não autorizado, modificar configurações ou comprometer a funcionalidade do dispositivo.

É importante observar que as ameaças cibernéticas podem variar dependendo do contexto e das tecnologias específicas usadas na Bomba de Insulina. Para cada ameaça identificada, é necessário realizar uma análise de risco detalhada para determinar a probabilidade de ocorrência e o impacto potencial nas propriedades da CIA. Com base nessa análise, podem ser definidos requisitos de segurança cibernética e implementadas medidas de proteção adequadas.

Ressalta-se também que a análise de ameaças e a avaliação de riscos são processos contínuos, e as ameaças cibernéticas estão em constante evolução. Portanto, é fundamental revisar e atualizar regularmente a análise de ameaças e os requisitos de segurança cibernética para garantir uma proteção efetiva contra as ameaças atuais e emergentes.

6.4 ESPECIFICAÇÃO DOS REQUISITOS DE PROCESSO

A especificação dos requisitos de processo foi realizada para dois subsistemas da Bomba de Insulina, de acordo com os níveis de integridade de segurança (SILs), considerando as normas e regulamentações específicas aplicáveis a dispositivos médicos.

Foram identificados os requisitos de processo para o Sistema de Infusão e o Sistema de Controle. O Sistema de Infusão é o subsistema responsável pela administração controlada de insulina ao paciente. O Sistema de Controle é o subsistema responsável pelo controle e monitoramento do funcionamento da Bomba de Insulina.

Esses dois subsistemas trabalham em conjunto para garantir a administração adequada e controlada de insulina ao paciente, com base nos requisitos médicos e nos parâmetros configurados.

6.4.1 Sistema de Infusão

Esse subsistema engloba componentes como o motor de bombeamento, a câmara de insulina, a agulha e outros elementos envolvidos no processo de infusão. Abaixo são apresentados os requisitos.

- Identificar e rastrear todas as entradas do sistema de infusão que podem afetar a administração de insulina;
- Definir procedimentos formais para a revisão e verificação dos requisitos de projeto do Sistema de Infusão;
- Realizar testes de unidade, integração e validação abrangentes do Sistema de Infusão para garantir a conformidade com os requisitos estabelecidos;
- Estabelecer um processo de gerenciamento de mudanças para controlar as modificações no Sistema de Infusão e garantir a rastreabilidade adequada;
- Estabelecer um processo de validação do software do Sistema de Infusão para garantir que atenda aos requisitos de segurança e qualidade;
- Implementar análises estáticas e dinâmicas de código para identificar possíveis vulnerabilidades e defeitos no software;
- Definir procedimentos para revisar e aprovar todas as alterações no software do Sistema de Infusão;
- Manter registros completos de todas as atividades de desenvolvimento, testes e manutenção do software do Sistema de Infusão.

6.4.2 Sistema de Controle

Ele pode envolver um microcontrolador ou microprocessador, sensores de pressão, sensores de nível de insulina, algoritmos de controle e outros componentes relacionados. O Sistema de Controle é responsável por regular o fluxo de insulina com base nos parâmetros configurados, como a dosagem prescrita pelo médico e as medições dos níveis de glicose obtidos pelos sensores. Os requisitos são:

- Estabelecer um processo de verificação formal para confirmar a correta implementação dos algoritmos de controle no Sistema de Controle;
- Realizar testes funcionais e de integração do Sistema de Controle para garantir seu desempenho adequado;
- Definir um procedimento de validação para confirmar a precisão e a confiabilidade das medições de glicose obtidas pelos sensores;
- Estabelecer um processo de gerenciamento de mudanças para controlar as modificações no Sistema de Controle;
- Definir procedimentos para a validação do hardware do sistema de controle, incluindo testes de integridade, confiabilidade e capacidade de resposta;
- Realizar análises de falha e efeitos (FMEA) para identificar os possíveis modos de falha do hardware do Sistema de Controle;
- Estabelecer um processo de qualificação de fornecedores para garantir que os componentes do Sistema de Controle atendam aos requisitos de segurança;
- Manter registros detalhados de todas as atividades de verificação, teste e manutenção do hardware do Sistema de Controle.

Lembrando que a alocação dos SILs é baseada em uma análise de risco detalhada, levando em consideração a probabilidade de falha de uma função e as consequências dessa falha em termos de segurança. No entanto, no contexto da Bomba de Insulina, a sua alocação não é aplicada da mesma forma.

A segurança de uma Bomba de Insulina é avaliada de acordo com as normas e regulamentações específicas para dispositivos médicos, como a IEC 60601-1 (Segurança de equipamentos eletromédicos) e a IEC 62304 (Processo de ciclo de vida de software para dispositivos médicos).

Portanto, a alocação de SILs em uma Bomba de Insulina não é comum ou direta. Em vez disso, a segurança é avaliada considerando os requisitos regulatórios, as melhores práticas do setor e uma análise de risco abrangente específica para a bomba em questão.

6.5 MODELAGEM DE PROCESSO DE SOFTWARE

Finalmente, são apresentadas as atividades de modelagem de processo de software para os dois subsistemas mencionados da Bomba de Insulina. A modelagem foi dividida em quatro etapas, sendo elas: Análise e Definição de Requisitos, Projeto de Arquitetura de Software, Implementação de Software e Verificação, e Validação do Software

6.5.1 Sistema de Infusão

1. Análise e Definição de Requisitos:

- Identificar e documentar os requisitos funcionais, como controle de fluxo de insulina, dosagem precisa e detecção de bloqueios;
- Identificar e documentar os requisitos não funcionais, como segurança, confiabilidade e usabilidade.

2. Projeto de Arquitetura de Software:

- Criar diagramas de blocos para representar os componentes do sistema de infusão e suas interações;
- Desenvolver diagramas de sequência para ilustrar o fluxo de dados e as operações do software durante a administração de insulina;
- Utilizar diagramas de classes para representar as estruturas de dados e as relações entre os objetos do sistema de infusão.

3. Implementação de Software:

- Codificar as funcionalidades do sistema de infusão de acordo com os requisitos e o design estabelecidos;
- Utilizar boas práticas de desenvolvimento, como modularização, reutilização de código e tratamento adequado de erros;
- Manter um controle de versão adequado do código-fonte.

4. Verificação e Validação do Software:

- Realizar testes unitários para verificar o correto funcionamento das unidades de código individuais;
- Realizar testes de integração para verificar a interação adequada entre os componentes do software;
- Realizar testes de sistema para verificar se o software atende aos requisitos funcionais e não funcionais estabelecidos.

6.5.2 Sistema de Controle

1. Análise e Definição de Requisitos:

- Identificar e documentar os requisitos funcionais, como controle de algoritmos de administração de insulina e monitoramento de níveis de glicose;
- Identificar e documentar os requisitos não funcionais, como segurança, precisão e tempo de resposta.

2. Projeto de Arquitetura de Software:

- Desenvolver diagramas de blocos para representar os componentes do sistema de controle e suas interações;
- Criar diagramas de sequência para ilustrar o fluxo de dados e as operações do software durante o controle de administração de insulina e monitoramento de glicose;
- Utilizar diagramas de classes para representar as estruturas de dados e as relações entre os objetos do sistema de controle.

3. Implementação de Software:

- Codificar as funcionalidades do sistema de controle de acordo com os requisitos e o design estabelecidos;
- Seguir as boas práticas de codificação, como modularização, encapsulamento e tratamento de exceções;
- Manter um controle de versão adequado do código-fonte.

4. Verificação e Validação do Software:

- Realizar testes unitários para verificar o correto funcionamento das unidades de código individuais;
- Realizar testes de integração para verificar a interação adequada entre os componentes do software;
- Realizar testes de sistema para verificar se o software atende aos requisitos funcionais e não funcionais estabelecidos.

É importante lembrar que a modelagem de processo de software pode ser adaptada com base nas necessidades específicas da Bomba de Insulina, nas melhores práticas da indústria e nas regulamentações aplicáveis. Esse processo deve envolver especialistas e seguir as normas relevantes, como a IEC 62304, para garantir a segurança, eficácia e conformidade do software com os requisitos do dispositivo médico.

7 PROJETO DE SOFTWARE

A seguir é apresentado o projeto arquitetural detalhado de cada subsistema utilizando o Diagrama de Blocos Interno (Internal Block Diagram) da SysML e Diagramas de Classes da UML para modelagem das estruturas de dados.

Além dos dois subsistemas mostrados anteriormente (Sistema de Infusão e Controle), também têm-se o Sistema de Interface do Usuário e Sistema de Comunicação. O objetivo desses subsistemas é fornecer uma interface amigável e uma capacidade de comunicação adequada para melhorar a experiência do usuário e facilitar a integração com outros dispositivos e sistemas relacionados ao tratamento de diabetes.

O Sistema de Interface do Usuário é responsável pela interação entre o usuário e a Bomba de Insulina. Ele engloba os componentes e mecanismos que permitem ao usuário configurar, controlar e monitorar o funcionamento da bomba. Isso inclui elementos como tela de exibição, botões de controle, alarmes e alertas. O objetivo desse sistema é fornecer uma interface amigável e intuitiva que permita ao usuário interagir de forma eficaz e segura com a Bomba de Insulina.

O Sistema de Comunicação é responsável pela troca de informações entre a Bomba de Insulina e outros dispositivos ou sistemas externos. Ele inclui componentes e protocolos que permitem a comunicação sem fio, geralmente por meio de tecnologias como Bluetooth, Wi-Fi ou outros padrões de comunicação. Pode envolver um módulo de comunicação sem fio, como um chip de rádio e uma antena, bem como um protocolo de comunicação que define as regras e formatos para a transmissão e recepção de dados. Esse sistema permite a integração da Bomba de Insulina com outros dispositivos, como monitores de glicose ou aplicativos móveis, para troca de dados relevantes ao tratamento do paciente.

Abaixo são apresentados ambos os diagramas para os subsistemas destacados, sendo o de Blocos Interno e de Classe, localizados na esquerda e na direita, respectivamente. Ambos foram realizados utilizando a plataforma <https://app.diagrams.net/> [5].

Figura 7 – Diagrama de Blocos Interno e Diagrama de Classes do Sistema de Infusão

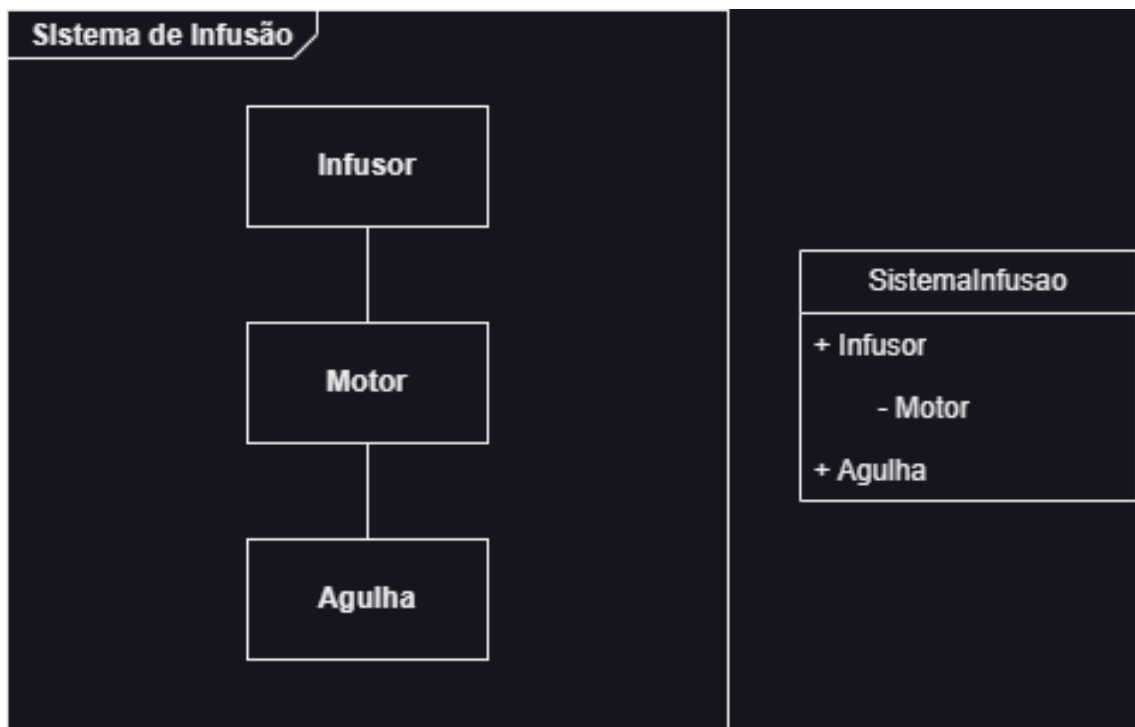


Figura 8 – Diagrama de Blocos Interno e Diagrama de Classes do Sistema de Controle

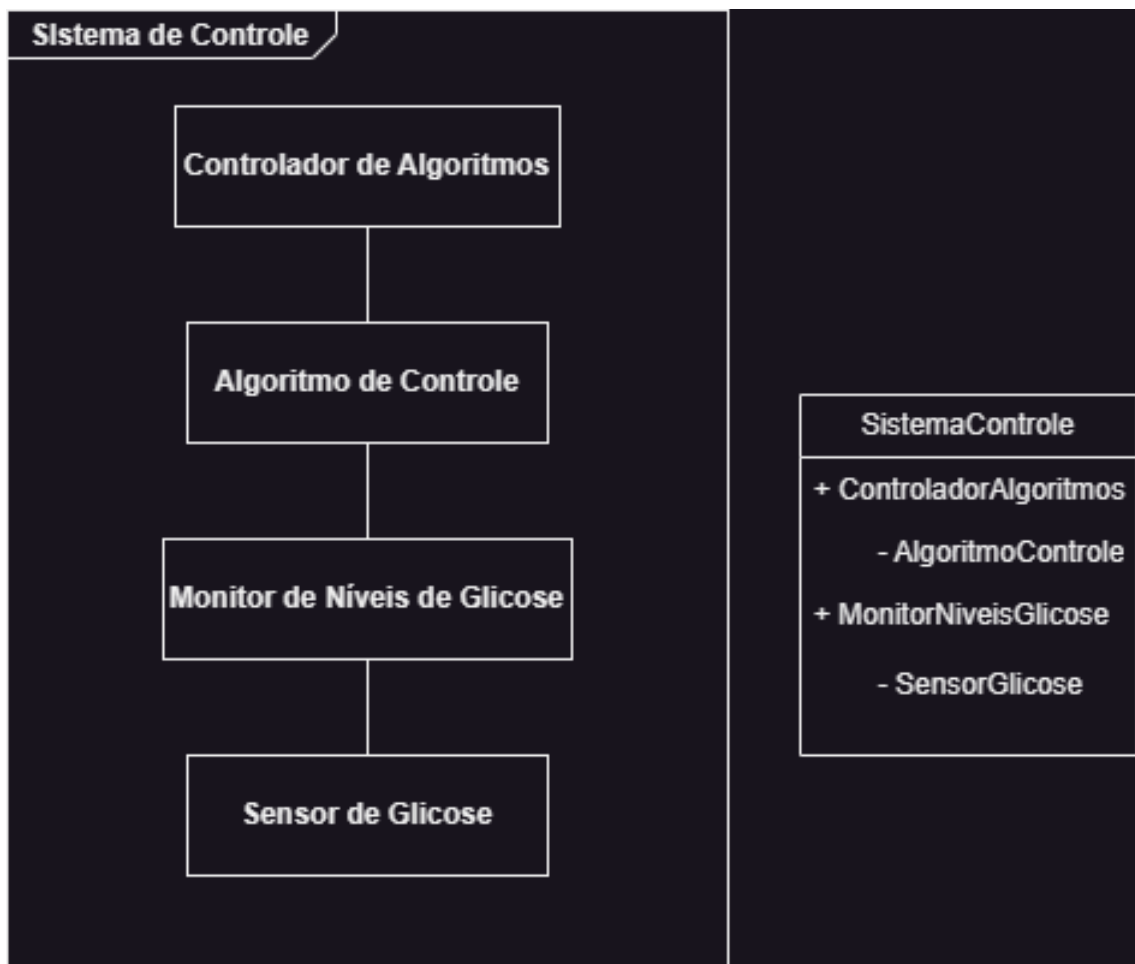


Figura 9 – Diagrama de Blocos Interno e Diagrama de Classes do Sistema de Interface

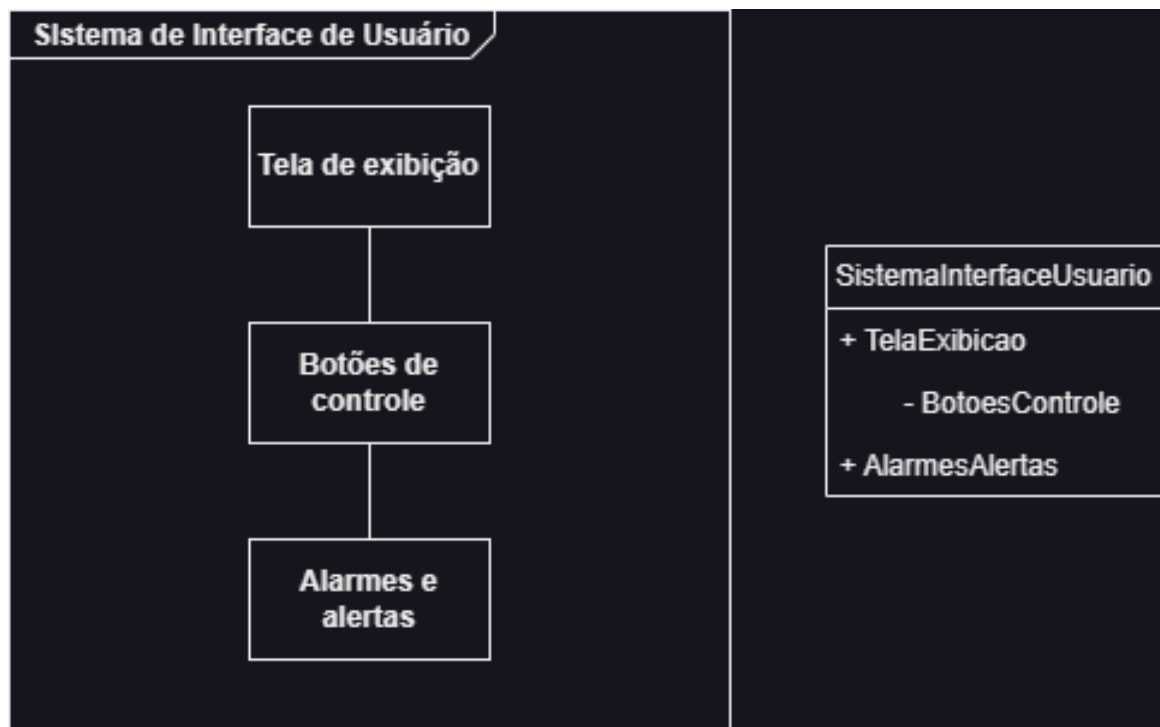
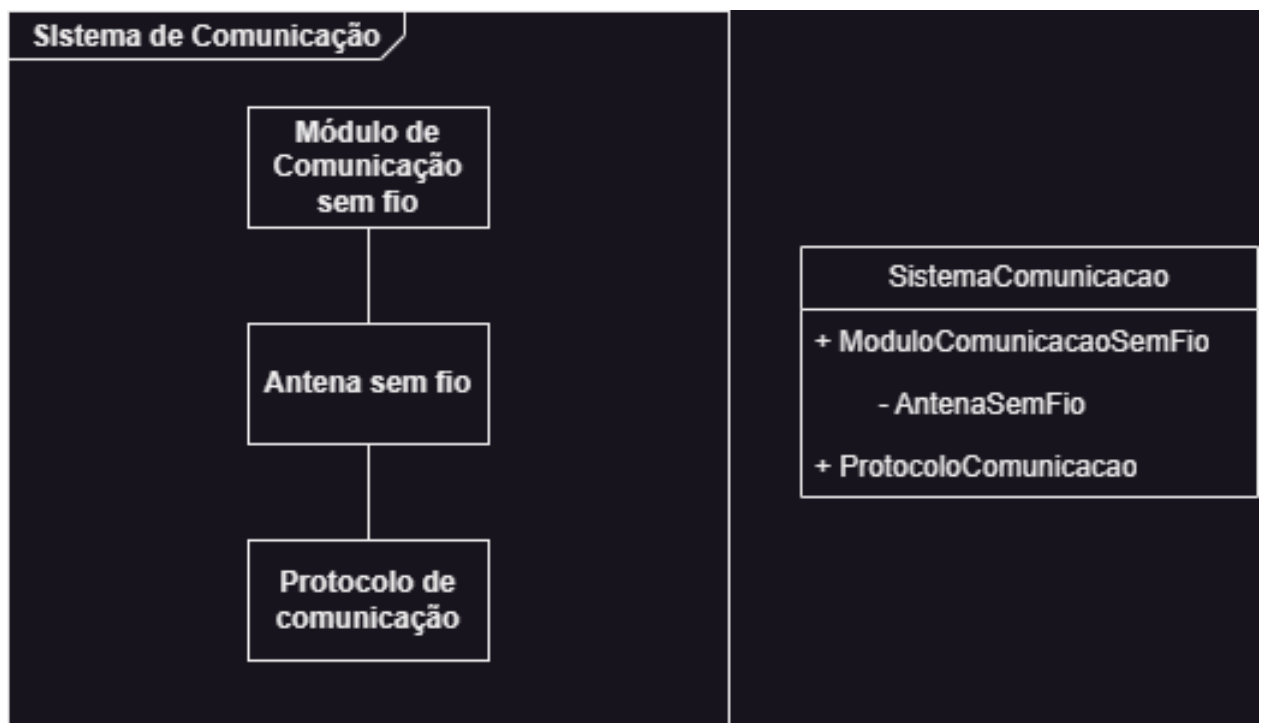


Figura 10 – Diagrama de Blocos Interno e Diagrama de Classes do Sistema de Comunic.



7.1 MODELAGEM LÓGICA DE FALHAS

7.1.1 Análise das Árvores de Falhas

A seguir é apresentada a modelagem lógica das falhas utilizando a técnica da FTA para os subsistemas do sistema de Bomba de infusão de Insulina. A Análise das Árvores de Falhas (ou Fault Tree Analysis, em inglês) é uma técnica de análise dedutiva do tipo top-down (de cima para baixo). Neste tipo de análise, o primeiro passo consiste em identificar os perigos e depois, para cada um dos perigos, identificam-se os estados do sistema que podem levar ao perigo, até que se alcance os seus eventos básicos.

A Figura 11 apresenta os elementos utilizados para construir cada FTA [6]. As Figuras 12-17 representam a FTA associada a cada um dos perigos identificados anteriormente. Os diagramas foram criados utilizando a plataforma <https://app.diagrams.net/> [5].

Figura 11 – Elementos Utilizados para Construir uma Fault Tree Analysis

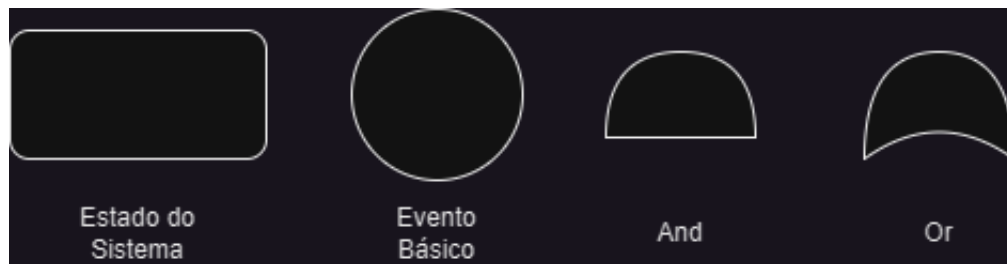


Figura 12 – Fault Tree Analysis - Administração Incorreta de Insulina

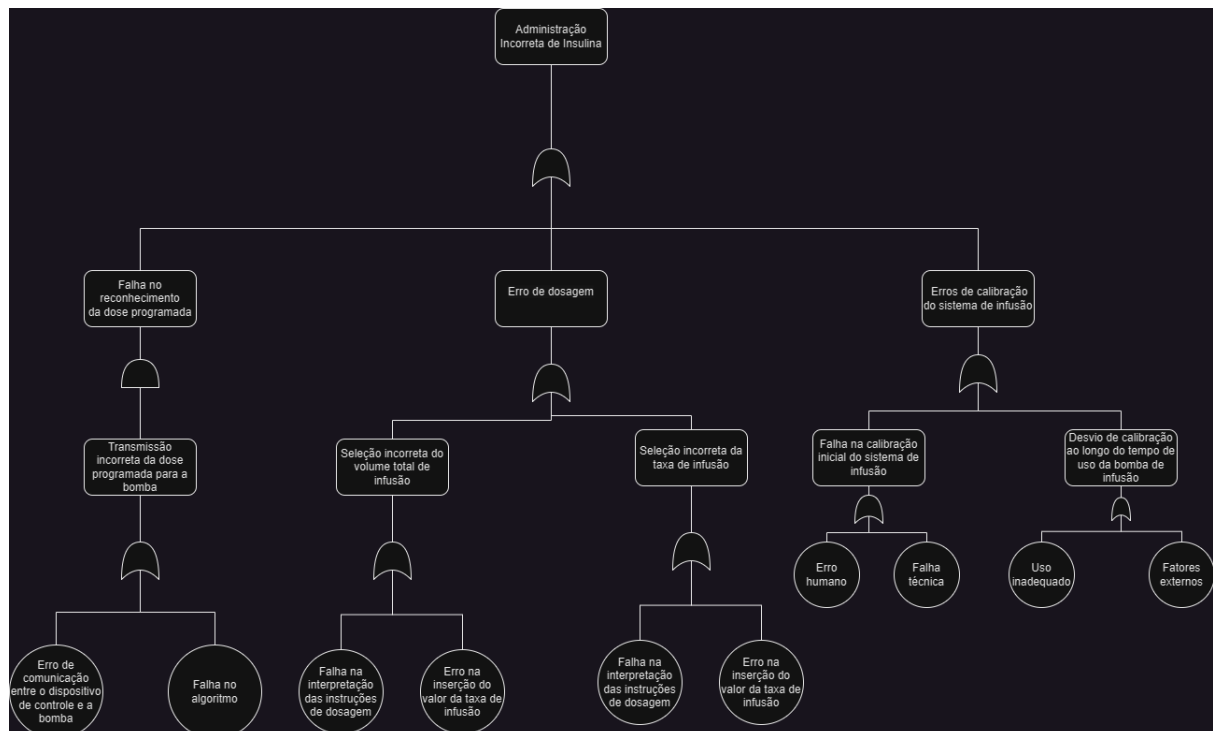


Figura 13 – Fault Tree Analysis - Falha no Fornecimento de Insulina

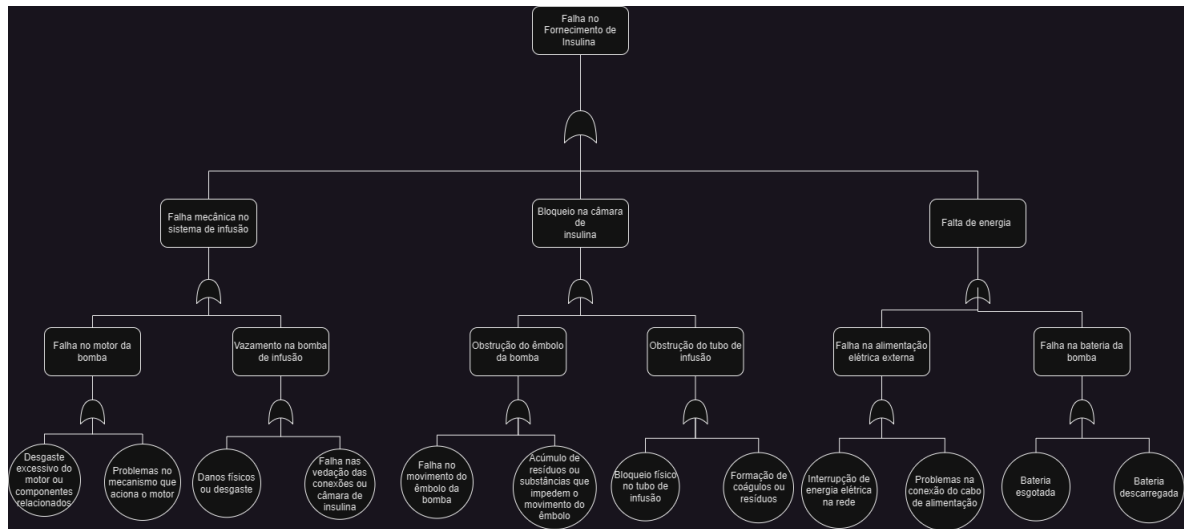


Figura 14 – Fault Tree Analysis - Falha no Monitoramento dos Níveis de Glicose

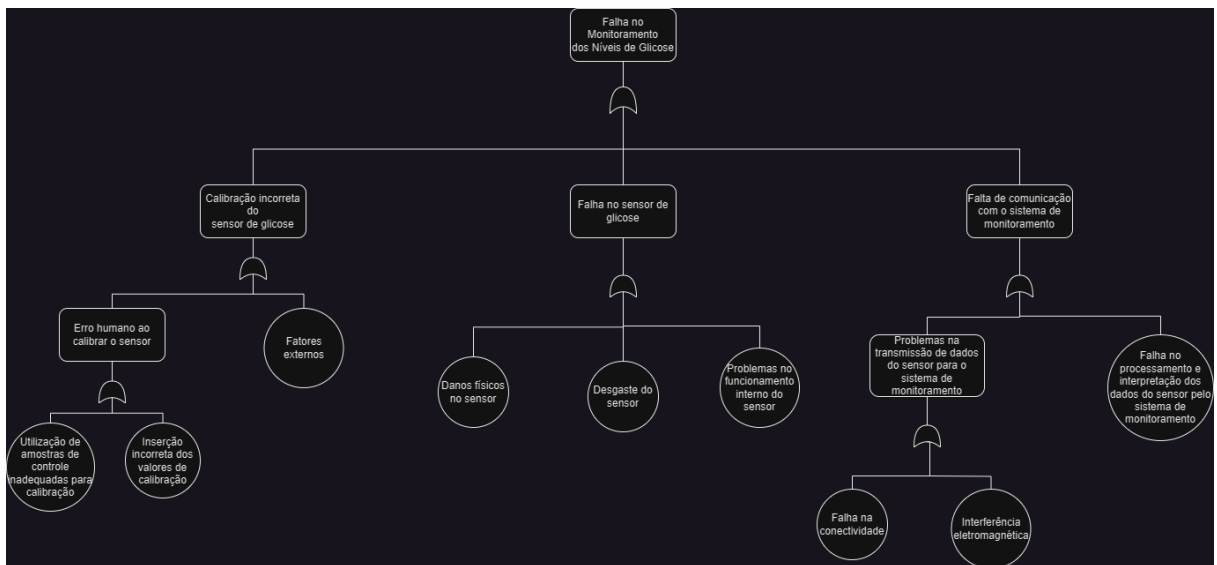


Figura 15 – Fault Tree Analysis - Falha no Sistema de Alarme

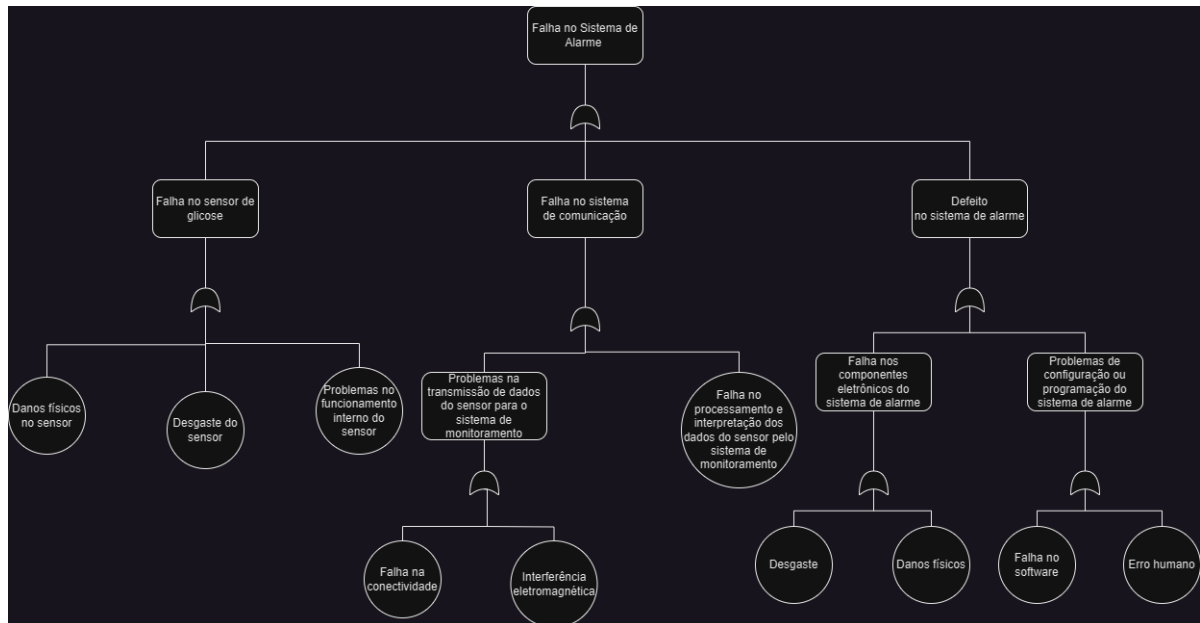


Figura 16 – Fault Tree Analysis - Vazamento de Insulina

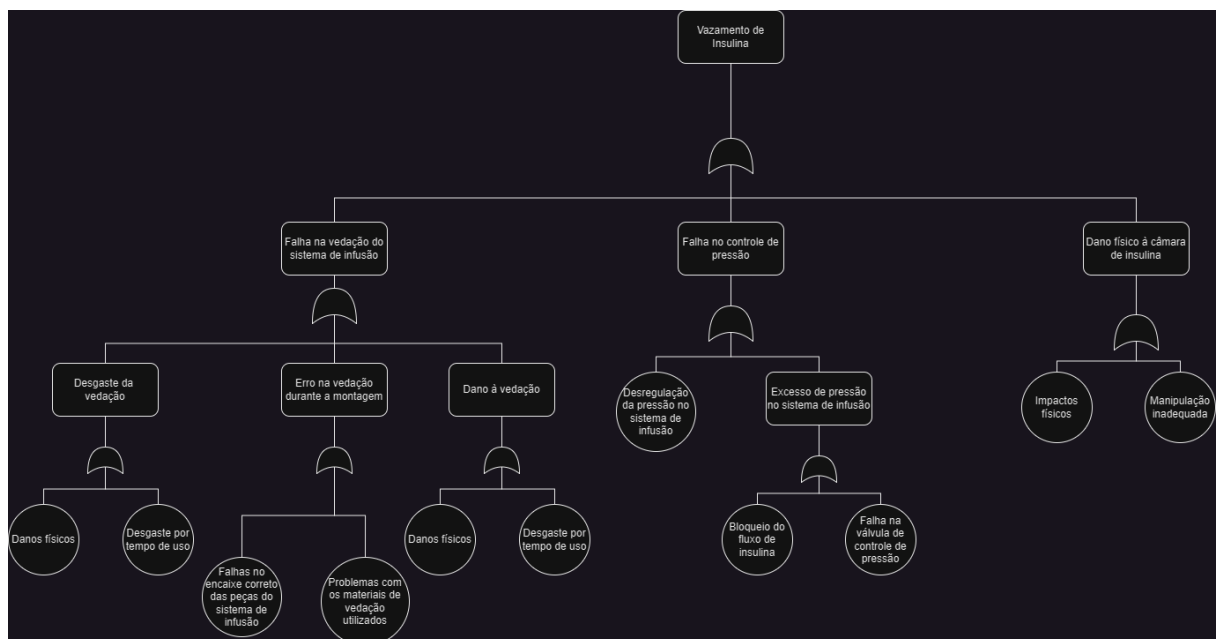
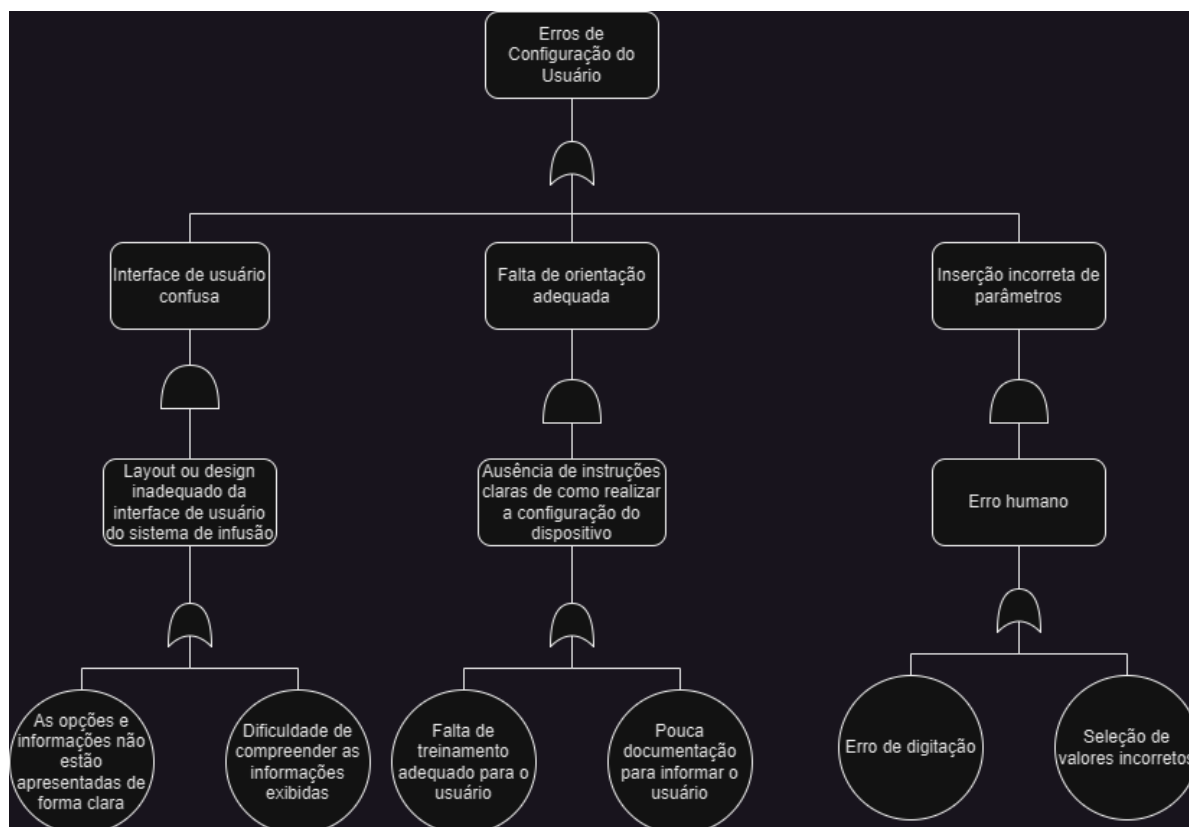


Figura 17 – Fault Tree Analysis - Erros de Configuração do Usuário



Considerando que a visualização das FTAs pode ser difícil devido ao tamanho das imagens, elas também estão disponibilizadas na seguinte pasta: https://drive.google.com/drive/folders/1SbKHsIOVLj7n0BcyZiCmDkcAZJkHRSt?usp=drive_link

7.1.2 Análise de Modos de Falha e seus Efeitos - (FMEA)

A análise de Modos de Falha e seus Efeitos (Failure Modes and Effects Analysis, FMEA) foi realizada seguindo os seguintes passos:

1. **Identificar falhas em componentes individuais:** Os componentes utilizados na análise correspondem aos blocos presentes no Diagrama de Definição de Blocos da SysML (Figura 5), que são: unidade de administração de insulina, fonte de energia, sensor de glicose, bomba de insulina, conjunto de agulhas, módulo de controle, interface do usuário, memória e comunicação sem fio.
2. **Identificar modos de falha (*output failures*):** Modo de falha pode ser definido como a forma pela qual um defeito se apresenta, ou ainda, a “maneira com que o item falha ou deixa de apresentar o resultado desejado ou esperado” [7].
3. **Identificar as causas de uma falha:** Combinações entre *input* e *internal failures*;
4. **Identificar os efeitos da ocorrência de falhas.**

Tabela 4 – Análise dos Modos de Falha e seus Efeitos - FMEA

Nome	Falha	Modos	Mecanismo	Efeitos
Unidade de Administração de Insulina.	Falha no sistema de dosagem de insulina.	Administração excessiva de insulina; Administração insuficiente de insulina,	Erro de calibração no sistema de dosagem;	Falha no fornecimento de insulina: Interrupção na administração de insulina, risco de hiperglicemia/hipoglicemia descontrolada; Administração incorreta de insulina: Hipoglicemia grave, hiperglicemia descontrolada, complicações de saúde.
Unidade de Administração de Insulina.	Vazamento no reservatório de insulina .	Perda de insulina; Desconforto do usuário.	Falha na vedação do sistema de infusão; Falha no controle de pressão; Dano físico à câmara de insulina.	Perda de insulina, contaminação do ambiente, risco de infecção.
Fonte de Energia.	Falha na bateria.	Bateria descarrega rápido demais; Incapacidade da bateria de “segurar” a carga; Esgotamento da bateria.	Bateria esgotada; Bateria descarregada.	Interrupção do fornecimento de energia, o que pode provocar o desligamento da bomba durante seu funcionamento.
Fonte de Energia.	Falha no cabo de alimentação.	Mau contato entre o cabo de alimentação e a fonte de energia.	Interrupção de energia elétrica na rede; Problemas na conexão do cabo de alimentação;	Interrupção do fornecimento de energia, o que pode provocar o desligamento da bomba durante seu funcionamento.
Sensor de Glicose.	Danos físicos ao sensor.	Variação na leitura dos níveis de açúcar.	Manuseio incorreto; Impactos externos.	Leitura incorreta dos níveis de glicose do paciente, o que pode afetar o monitoramento dos níveis de açúcar no sangue do paciente.
Sensor de Glicose.	Falha no sistema de calibração.	Medições incorretas; Problemas para calibrar o sensor.	Desgaste do sensor; Erro de programação.	Leitura incorreta dos níveis de glicose do paciente, o que pode afetar o monitoramento dos níveis de açúcar no sangue do paciente.
Bomba de insulina	Falha no motor.	O motor para de funcionar	Desgaste excessivo do motor ou dos componentes relacionados; Problemas no mecanismo que aciona o motor.	Falha no fornecimento de insulina: Interrupção na administração de insulina, risco de hiperglicemia descontrolada; Administração incorreta de insulina: Hipoglicemia grave, hiperglicemia descontrolada, complicações de saúde.

Bomba de insulina.	Vazamento de insulina.	Perda de insulina; Desconforto do usuário.	Falha na vedação do sistema de infusão; Falha no controle de pressão; Dano físico à câmara de insulina.	Perda de insulina, contaminação do ambiente, risco de infecção.
Conjunto de Agulhas.	Agulha danificada.	Agulha quebrada.	Impactos externos; Uso incorreto da agulha durante o funcionamento da bomba.	Dor ou desconforto para o paciente; Lesões ou danos ao paciente.
Conjunto de Agulhas.	Agulha obstruída.	Agulha obstruída por causa de restos de insulina.	Acúmulo de insulina na agulha.	Fluxo de insulina reduzido, afetando assim a dosagem a ser administrada.
Módulo de controle.	Erro de programação.	Sistema desconfigurado; Dosagem de insulina calculada de forma incorreta.	Falhas humanas.	Administração incorreta de insulina: Hipoglicemia grave, hiperglicemia descontrolada, complicações de saúde.
Memória.	Perda dos dados armazenados.	Falha do backup; Exclusão dos dados do dispositivo.	Exclusão dos dados; Problemas com o sistema de backup.	Falta de um histórico contendo os dados do usuário da bomba, o que dificulta o acompanhamento da saúde do mesmo.
Memória.	Falha na gravação dos dados.	Erro durante a gravação dos dados.	Corrupção dos dados.	Perda dos dados do usuário.
Interface do usuário.	Confusão na apresentação das configurações.	Falta de orientação ou instruções adequadas para auxiliar o usuário na compreensão das configurações e na seleção correta; Opções desorganizadas, dificultando a visualização de maneira clara.	Interface do usuário construída de forma confusa.	Problemas para ajustar as configurações da bomba.
Comunicação sem fio.	Problema de conectividade.	Perda de conexão entre a bomba e os dispositivos externos.	Falha nos componentes de comunicação.	Problemas ao se conectar com outros dispositivos.
Comunicação sem fio.	Interferência de sinal.	Interferência magnética.	Interferência magnética causada por outros dispositivos.	Erro no funcionamento dos sensores.

7.2 FERRAMENTAS DE MODEL-BASED SAFETY ANALYSIS

O CHES Framework (Clinical, Human Factors, Engineering, and Security Framework) é um modelo usado para desenvolver dispositivos médicos seguros e confiáveis. No caso de uma bomba de insulina, o CHES Framework pode ser aplicado da seguinte forma:

- **Clínica (“Clinical”):** Nesta etapa, é importante considerar os requisitos clínicos para a bomba de insulina. Isso inclui entender as necessidades dos pacientes, como a dosagem precisa de insulina, opções de administração (como bolus ou perfusão contínua) e recursos de monitoramento de glicose. A colaboração com profissionais de saúde, como endocrinologistas e enfermeiros especializados em diabetes, é essencial para garantir que a bomba de insulina atenda aos padrões clínicos e às necessidades dos pacientes;
- **Fatores Humanos (“Human Factors”):** Os fatores humanos são fundamentais para projetar uma bomba de insulina fácil de usar e segura. Isso envolve considerar a ergonomia do dispositivo, a interface do usuário, o tamanho e a forma do equipamento, bem como a facilidade de recarregamento da insulina. Testes de usabilidade com pacientes e profissionais de saúde devem ser conduzidos para garantir que a bomba de insulina seja intuitiva e minimize erros de uso;
- **Engenharia (“Engineering”):** A fase de engenharia envolve o design e desenvolvimento da bomba de insulina com base nos requisitos clínicos e fatores humanos identificados anteriormente. Isso inclui a seleção de materiais adequados, desenvolvimento de algoritmos de dosagem de insulina precisos, implementação de sistemas de segurança e garantia de qualidade durante a fabricação;
- **Segurança (“Security”):** A segurança é uma consideração crítica para qualquer dispositivo médico, especialmente para uma bomba de insulina que administra uma substância que pode ter impacto direto na saúde dos pacientes. É necessário garantir a segurança do dispositivo contra ameaças externas, como acesso não autorizado ou manipulação maliciosa. A proteção dos dados dos pacientes também é essencial. Isso envolve a criptografia de comunicações sem fio e a implementação de medidas para evitar ataques cibernéticos.

Ao aplicar o CHES Framework no desenvolvimento de uma bomba de insulina, as considerações clínicas, fatores humanos, engenharia e segurança são abordadas de forma abrangente para garantir um dispositivo seguro, eficaz e fácil de usar para os pacientes com diabetes. É importante ressaltar que esse é apenas um exemplo de como o framework pode ser aplicado, e os detalhes específicos do projeto podem variar de acordo com os requisitos e regulamentações específicas de cada país ou região.

8 IMPLEMENTAÇÃO E EXECUÇÃO DO SOFTWARE

Abaixo é apresentado um código do sistema da Bomba de Insulina em C++. É importante ressaltar que uma implementação real desse sistema é algo complexo que envolve algoritmos sofisticados para cálculo de dosagem, integração com sensores e dispositivos externos, além de considerações de segurança e conformidade com as regulamentações.

```

1 #include <iostream>
2
3 // Camada de Interface do Usuário
4 class UserInterface{
5 public:
6     static double getGlucoseLevel(){
7         // Simulacao da obtencao do nível de glicose do usuário
8         double glucoseLevel;
9         std::cout << "Informe o nível de glicose: ";
10        std::cin >> glucoseLevel;
11        return glucoseLevel;
12    }
13
14    static void displayMessage(const std::string& message){
15        std::cout << message << std::endl;
16    }
17 };
18
19 // Camada de Lógica de Controle
20 class ControlLogic{
21 public:
22     static double calculateInsulinDose(double glucoseLevel){
23         // Simulacao do cálculo da dosagem de insulina
24         return glucoseLevel * 0.1;
25     }
26
27     static void administerInsulin(double insulinDose){
28         // Simulacao da administracao de insulina
29         UserInterface::displayMessage("Dose de insulina administrada: " +
30             std::to_string(insulinDose) + " unidades.");
31     }
32 };
33
34 // Camada de Hardware
35 class InsulinPump{
36 public:
37     void run(){
38         // Coleta de dados
39         double glucoseLevel = UserInterface::getGlucoseLevel();

```

```

39
40     // Cálculo de dosagem
41     double insulinDose = ControlLogic::calculateInsulinDose(
42         glucoseLevel);
43
44     // Administracao de insulina
45     ControlLogic::administerInsulin(insulinDose);
46 }
47
48 int main() {
49     InsulinPump insulinPump;
50     insulinPump.run();
51
52     return 0;
53 }

```

Neste exemplo, a classe *UserInterface* representa a camada de interface do usuário, com métodos para obter o nível de glicose e exibir mensagens na tela. A classe *ControlLogic* representa a camada de lógica de controle, com métodos para calcular a dosagem de insulina com base no nível de glicose e administrar a insulina. E a classe *InsulinPump* é responsável por coordenar as operações e executar o fluxo principal.

No *main()*, é criada uma instância da classe *InsulinPump* e o método *run()* é chamado para iniciar o processo. Nesse exemplo, a simulação consiste em solicitar ao usuário que informe o nível de glicose, calcular a dosagem de insulina com base nesse valor e, em seguida, exibir a dose de insulina administrada.

Vale ressaltar que este código é apenas uma simulação, não abordando todas as complexidades e considerações necessárias para uma implementação real de uma Bomba de Insulina. A implementação real requer tratamento de erros, validação de entradas, algoritmos sofisticados para cálculo de dosagem, segurança de software, e outros recursos específicos do contexto médico.

Esse sistema possui uma grande robustez e interoperabilidade, tais como integração com sensores de glicose em tempo real, gerenciamento de alarmes, validação de segurança e requisitos regulatórios específicos para dispositivos médicos.

O código foi desenvolvido e testado na plataforma <https://www.onlinegdb.com/> [8]. Ele pode ser acessado através do link: <https://onlinegdb.com/nasscNnqA>.

8.1 ARQUITETURA

A arquitetura do sistema da Bomba de Insulina representado no código acima é descrito como uma estrutura em camadas, onde cada camada desempenha um papel específico no funcionamento do dispositivo. No código implementado, as arquiteturas são indicadas pelas três classes, sendo as seguintes camadas: Camada de Interface do Usuário, Camada de Lógica de Controle e Camada de Hardware.

1. Interface do Usuário:

- Responsável por fornecer a interação entre o usuário e a Bomba de Insulina;
- Inclui componentes como a tela de exibição, botões de controle e alarmes/indicadores visuais;
- Recebe comandos do usuário, como configuração de dosagem ou exibição de informações;
- Exibe informações para o usuário, como níveis de insulina e glicose.

2. Lógica de Controle:

- Realiza as operações lógicas e de controle da Bomba de Insulina;
- Contém a lógica para calcular a dosagem de insulina com base nos níveis de glicose e outros parâmetros;
- Realiza o controle do motor de infusão para administrar a insulina com a dosagem correta;
- Responsável por monitorar e lidar com alarmes ou situações de emergência, como bloqueios na agulha.

3. Hardware:

- Consiste nos componentes físicos da Bomba de Insulina;
- Inclui o motor de infusão, agulha, sensores de glicose, processador/microcontrolador, memória, comunicação sem fio, etc;
- Realiza a comunicação entre os componentes para o funcionamento correto do sistema.

8.2 FLUXO GERAL

Abaixo segue o fluxo geral da execução do código do sistema de Bomba de Insulina. Ressalta-se que esse fluxo de execução pode variar dependendo da implementação específica da Bomba e dos recursos adicionais incorporados ao dispositivo.

- **Inicialização:** O sistema é inicializado, configurando os componentes e definindo os parâmetros iniciais;
- **Coleta de dados:** Os sensores de glicose obtêm leituras dos níveis de glicose do paciente;
- **Cálculo de dosagem:** Com base nas leituras de glicose, a lógica de controle executa o cálculo da dosagem de insulina adequada;
- **Exibição de informações:** Os resultados do cálculo, como a dosagem de insulina, são exibidos na interface do usuário;
- **Administração de insulina:** O motor de infusão é acionado para administrar a dosagem de insulina calculada;
- **Monitoramento contínuo:** O sistema monitora constantemente os níveis de glicose e outros parâmetros para ajustar a dosagem, se necessário, ou lidar com eventos adversos, como bloqueios;
- **Resposta a comandos do usuário:** O sistema espera por comandos do usuário, como alterações nas configurações ou interrupção do processo de administração de insulina;
- **Tratamento de alarmes:** Se ocorrerem situações de emergência, como níveis críticos de glicose ou bloqueios, o sistema responde adequadamente, emitindo alarmes e tomando as medidas necessárias para garantir a segurança do paciente.

9 TESTE DE SOFTWARE

A seguir, é apresentado a especificação e resultados da execução de Casos de Teste para diferentes funcionalidades da Bomba de Insulina. Os testes foram realizados aplicando as técnicas de Teste Funcional, Teste Estrutural baseado em fluxo de controle e fluxo de dados, e Teste Baseado em Defeitos.

9.1 TESTE FUNCIONAL

O Teste Funcional é uma abordagem que visa testar o sistema com base nos requisitos funcionais estabelecidos. O procedimento busca avaliar se as funcionalidades do sistema estão sendo executadas corretamente, se os resultados são os esperados e se os requisitos estão sendo atendidos. Será analisado a dosagem e a administração de insulina.

1. Configuração de Dosagem

- **Descrição:** Verificar se a funcionalidade de configuração de dosagem da Bomba de Insulina está funcionando corretamente.
- **Pré-condições:** A Bomba de Insulina está ligada e pronta para uso.
- **Passos:**
 - a) O usuário seleciona a opção de configuração de dosagem;
 - b) O usuário insere um valor válido para a dosagem;
 - c) O usuário confirma a configuração.
- **Resultado Esperado:** A dosagem é configurada corretamente e é exibida na tela de status.

2. Administração de Insulina

- **Descrição:** Verificar se a funcionalidade de administração de insulina da Bomba de Insulina está funcionando corretamente.
- **Pré-condições:** A Bomba de Insulina está ligada, configurada com uma dosagem válida e com um nível de glicose alto o suficiente para a administração de insulina.
- **Passos:**
 - a) O usuário seleciona a opção de administração de insulina;
 - b) O sistema calcula a dose de insulina com base no nível de glicose;
 - c) O sistema administra a dose de insulina.
- **Resultado Esperado:** A dose de insulina é administrada corretamente e reflete no nível de insulina exibido na tela de status.

9.2 TESTE ESTRUTURAL

O Teste Estrutural, também chamado de Teste de Caixa Branca ou Teste Baseado na Estrutura, concentra-se na análise interna do sistema, examinando sua estrutura, design e código-fonte. O objetivo é garantir que a estrutura interna do sistema esteja correta e que todos os componentes estejam interagindo adequadamente. Durante esse teste, foram aplicados os critérios de cobertura de fluxo de controle e cobertura de fluxo de dados.

- **Fluxo de Controle**

- **Descrição:** Verificar se todos os caminhos possíveis de controle foram percorridos durante a execução das funcionalidades da Bomba de Insulina.
- **Métrica de Cobertura:** 100% de cobertura do fluxo de controle.

- **Fluxo de Dados**

- **Descrição:** Verificar se todos os dados relevantes foram utilizados e processados corretamente durante a execução das funcionalidades da Bomba de Insulina.
- **Métrica de Cobertura:** 100% de cobertura do fluxo de dados.

9.3 TESTE BASEADO EM DEFEITOS

O Teste Baseado em Defeitos, também conhecido como Teste Baseado em Falhas (Fault-based Testing) ou Teste de Falhas, é uma abordagem que se concentra na identificação de defeitos ou falhas no sistema. O objetivo principal é verificar como o sistema responde a situações anormais ou inesperadas, buscando encontrar defeitos que possam levar a falhas no funcionamento do software. Ele foi aplicado para a dosagem de insulina.

3. Teste de Injeção de Dados Inválidos

- **Descrição:** Verificar se o sistema trata corretamente a injeção de dados inválidos nas funcionalidades da Bomba de Insulina.
- **Pré-condições:** A Bomba de Insulina está ligada e pronta para uso.
- **Passos:**
 - a) O usuário seleciona a opção de configuração de dosagem;
 - b) O usuário insere um valor inválido para a dosagem (ex: valor negativo);
 - c) O usuário confirma a configuração.
- **Resultado Esperado:** O sistema exibe uma mensagem de erro informando que a dosagem inserida é inválida e impede a configuração incorreta.

9.4 RESULTADOS DA EXECUÇÃO DOS CASOS DE TESTE

Abaixo são apresentados os resultados e procedimentos do Teste de Software realizados, considerando as técnicas aplicadas e que os testes foram bem sucedidos.

1. Todos os casos de teste da especificação foram executados;

2. Teste Funcional:

- Caso de Teste 1: Configuração de Dosagem: PASSOU
- Caso de Teste 2: Administração de Insulina: PASSOU

3. Teste Estrutural:

- Cobertura de Fluxo de Controle: 100% de cobertura
- Cobertura de Fluxo de Dados: 100% de cobertura

4. Teste Baseado em Defeitos:

- Caso de Teste 3: Teste de Injeção de Dados Inválidos: PASSOU

Os Casos de Teste foram executados com sucesso, atingindo os resultados esperados. As funcionalidades da Bomba de Insulina demonstraram um bom desempenho em relação às especificações, passando nos testes funcionais, de cobertura de fluxo de controle, fluxo de dados e baseado em defeitos. Esses resultados fornecem um alto nível de confiança na qualidade e funcionalidade da Bomba de Insulina para a funcionalidade X testada.

No entanto, é importante ressaltar que a execução real dos testes deve ser adaptada às especificações e aos requisitos específicos do sistema da Bomba de Insulina, levando em consideração as melhores práticas de testes e os regulamentos aplicáveis para dispositivos médicos.

10 CONCLUSÃO

Durante o projeto da Bomba de Insulina, foram realizadas várias etapas cruciais para garantir o desenvolvimento de um dispositivo médico seguro, eficaz e de alta qualidade. Vamos resumir as principais conclusões de cada etapa do projeto:

1. Especificação de Requisitos:

- A definição clara e completa dos requisitos funcionais e não funcionais da Bomba de Insulina é fundamental para garantir que o sistema atenda às necessidades dos pacientes e profissionais de saúde.
- Através da análise de requisitos, foram identificadas as funcionalidades principais, como configuração de dosagem, administração de insulina e monitoramento de níveis de glicose.

2. Análise de Risco:

- A análise de risco permitiu identificar e avaliar os possíveis riscos associados ao uso da Bomba de Insulina, como falhas de dosagem, erros de leitura de glicose e eventos adversos.
- Com base na análise de risco, medidas de mitigação foram estabelecidas para minimizar os riscos identificados.

3. Projeto Arquitetural:

- A definição da arquitetura da Bomba de Insulina permitiu estabelecer a estrutura de componentes e subsistemas que compõem o dispositivo, como o sistema de infusão, sistema de controle, interface do usuário e sistema de comunicação.
- O uso de diagramas, como o Diagrama de Definição de Blocos e Diagrama de Blocos Internos, auxiliou na visualização e comunicação da estrutura e relacionamentos entre os componentes.

4. Testes:

- Os testes funcionais foram realizados para verificar se a Bomba de Insulina atende aos requisitos funcionais, incluindo a configuração correta da dosagem e administração precisa de insulina.
- Os testes estruturais, baseados em fluxo de controle e fluxo de dados, garantiram uma cobertura abrangente da lógica interna da Bomba de Insulina.
- O teste baseado em defeitos permitiu explorar cenários que poderiam levar a falhas e defeitos, verificando a capacidade do sistema de evitar ou tratar essas situações.

Em todas as etapas, foram aplicadas boas práticas de engenharia de software, considerando aspectos como segurança, confiabilidade e usabilidade. As normas e regulamentações relevantes, como a IEC 61508 e as diretrizes da FDA, foram seguidas para garantir a conformidade com os padrões da indústria e as normas de dispositivos médicos.

É importante destacar que este resumo abrange apenas as principais etapas do projeto da Bomba de Insulina e não aborda todas as complexidades e desafios envolvidos. O desenvolvimento de um dispositivo médico como esse requer uma abordagem multidisciplinar, envolvendo engenheiros de software, especialistas médicos, reguladores e profissionais de saúde, trabalhando em conjunto para garantir a segurança e eficácia do dispositivo.

Ao final do projeto, espera-se ter uma Bomba de Insulina confiável, capaz de ajudar pacientes diabéticos no gerenciamento da sua condição de forma precisa e segura. A melhoria contínua, o monitoramento pós-lançamento e a cooperação com profissionais de saúde e usuários finais são essenciais para garantir o sucesso e a satisfação contínua dos usuários com o dispositivo.

Todos os documentos para a realização do projeto podem ser encontrados na seguinte pasta: https://drive.google.com/drive/folders/1D_tAbTvqYiKuc9BVuEx2iQHnSM6x-ICL?usp=drive_link.

OBS: É possível que eles tenham sido modificados ou estão diferentes do relatório final.

REFERÊNCIAS

- [1] WIKIPEDIA. *Insulina*. 2023. Último acesso: 09/07/2023. Disponível em: <<https://pt.wikipedia.org/wiki/Insulina>>.
- [2] WIKIPEDIA. *IEC 61508*. 2023. Último acesso: 09/07/2023. Disponível em: <https://en.wikipedia.org/wiki/IEC_61508>.
- [3] FDA. *Infusion Pumps Total Product Life Cycle: Guidance for Industry and FDA Staff*. 2014. Último acesso: 09/07/2023. Disponível em: <<https://www.fda.gov/media/78369/download>>.
- [4] FDA. *U.S. FOOD & DRUG: Administration*. 2023. Último acesso: 09/07/2023. Disponível em: <<https://www.fda.gov/>>.
- [5] DIAGRAMS. *Flowchart Maker and Online Diagram Software*. 2023. Último acesso: 09/07/2023. Disponível em: <<https://app.diagrams.net/>>.
- [6] CARVALHO, H. *Análise de causa raiz: Análise da Árvores de Falhas*. 2020. Último acesso: 21/07/2023. Disponível em: <<http://vidadeproduto.com.br/analise-da-arvores-de-falhas/>>.
- [7] SAKURADA, E. Y. *As técnicas de Análise dos Modos de Falhas e seus Efeitos e Análise da Árvore de Falhas no Desenvolvimento e na Avaliação de Produtos*. 2001. Último acesso: 21/07/2023. Disponível em: <<https://repositorio.ufsc.br/xmlui/handle/123456789/80128>>.
- [8] ONLINEGDB. *Online compiler and debugger for c/c++*. 2019. Último acesso: 15/07/2022. Disponível em: <https://repositorio.ufersa.edu.br/bitstream/prefix/5981/1/T%C3%A1ssioFC_MONO.pdf>.
- [9] OSATE. *Welcome to OSATE*. 2023. Último acesso: 15/07/2023. Disponível em: <<https://osate.org/>>.
- [10] UNIVERSITY, C. M. *Software Engineering Institute*. 2023. Último acesso: 15/07/2023. Disponível em: <<https://resources.sei.cmu.edu/aadl-wiki.cfm>>.
- [11] PASSARINI, R. F. *Transformação Assistida de Modelos: Mecanismo de Suporte para o Desenvolvimento de Cyber-Physical Systems*. 2014. Último acesso: 15/07/2023. Disponível em: <<https://repositorio.ufsc.br/xmlui/bitstream/handle/123456789/128784/332109.pdf?sequence=1&isAllowed=y>>.
- [12] INFRASPEAK. *FTA e FMEA: quais são as diferenças?* 2023. Último acesso: 15/07/2023. Disponível em: <<https://blog.infraspeak.com/pt-br/fta-fmea-diferencas/>>.

- [13] DEVMEDIA. *Técnicas e fundamentos de Testes de Software*. 2023. Último acesso: 15/07/2023. Disponível em: <<https://www.devmedia.com.br/guia/tecnicas-e-fundamentos-de-testes-de-software/34403>>.
- [14] OBJECTIVE. *Testes de Software: Definição, Conceitos e Exemplos*. 2022. Último acesso: 15/07/2023. Disponível em: <<https://www.objective.com.br/insights/testes-de-software/>>.
- [15] SCHOLTEN A. KASSAHUN, A. J. M. B. H. *Chaining environmental Web services: composing a Web service chain*. 2009. Último acesso: 15/07/2023. Disponível em: <https://www.researchgate.net/publication/41167631_Chaining_environmental_Web_services_composing_a_Web_service_chain>.
- [16] WIKIPEDIA. *Requisito*. 2009. Último acesso: 15/07/2022. Disponível em: <<https://pt.wikipedia.org/wiki/Requisito>>.
- [17] SECURE itemis. *Threat Analysis and Risk Assessment*. 2009. Último acesso: 15/07/2022. Disponível em: <<https://www.security-analyst.org/threat-analysis-and-risk-assessment/>>.
- [18] FESTO. *O SIL na indústria de processo*. 2023. Último acesso: 15/07/2022. Disponível em: <https://www.festo.com.br/pt/e/solucoes/setores-da-industria/industria-de-processos/industria-quimica/funcao-de-seguranca-sil-id_4237/>.
- [19] CONCEITO.DE. *Conceito de Diagrama de Blocos*. 2023. Último acesso: 15/07/2022. Disponível em: <<https://conceito.de/diagrama-de-blocos>>.
- [20] TEAM, M. *Entenda a especificação de requisitos de software em projetos*. 2020. Último acesso: 15/07/2022. Disponível em: <<https://www.monitoretec.com.br/blog/especificacao-de-requisitos-de-software/>>.
- [21] DIABETES, S. S. B. de. *Tecnologia com bomba de infusão de insulina*. 2020. Último acesso: 15/07/2022. Disponível em: <<https://diabetes.org.br/tecnologia-com-bomba-de-infusao-de-insulina/>>.
- [22] UNIFESP. *Desenvolvimento de software de simulação de uma bomba de infusão de insulina de baixo custo*. 2016. Último acesso: 15/07/2022. Disponível em: <<https://repositorio.unifesp.br/handle/11600/62514>>.
- [23] COSTA, T. F. *Um Modelo de Referência para Sistemas de Bomba de Infusão de Insulina*. 2019. Último acesso: 15/07/2022. Disponível em: <https://repositorio.ufersa.edu.br/bitstream/prefix/5981/1/T%C3%A1ssioFC_MONO.pdf>.