**Safety ArtISt – Método para a Garantia de Segurança Crítica (Safety) de Sistemas com Inteligência Artificial: Desenvolvimento e Análise de Estudos de Caso**

**Relatório Técnico de Pesquisa**

**<TÍTULO DO RELATÓRIO>: Modelo de Relatório Técnico para Estudos de Caso do Projeto de Pesquisa “Safety ArtISt: Um Método para a Garantia de Segurança Crítica de Sistemas com Inteligência Artificial”**

Autor(es): Antonio Vieira da Silva Neto

Revisor: Antonio Vieira da Silva Neto

Revisão **1** – **28/03/2022**

<TÍTULO DO RELATÓRIO>: Modelo de Relatório Técnico para Estudos de Caso do Projeto de Pesquisa “Safety ArtISt: Um Método para a Garantia de Segurança Crítica de Sistemas com Inteligência Artificial”

[1 Introdução 4](#_Toc99390718)

[1.1 Siglas e Abreviações 4](#_Toc99390719)

[2 Descrição do Sistema do Estudo de Caso 5](#_Toc99390720)

[3 Primeira iteração do Método Safety ArtISt 6](#_Toc99390721)

[3.1 Etapa 1: Especificação de Requisitos e Definição Preliminar da Arquitetura 6](#_Toc99390722)

[3.2 Etapa 2: Seleção e Análise de Bases de Dados de Entrada 6](#_Toc99390723)

[3.3 Etapa 3: Projeto Preliminar da IA 7](#_Toc99390724)

[3.4 Etapa 4: Projeto dos Modelos Base da IA 7](#_Toc99390725)

[3.5 Etapa 5: Treinamento e V&V Preliminar da IA 8](#_Toc99390726)

[3.6 Etapa 6: V&V Avançada da IA 8](#_Toc99390727)

[3.7 Etapa 7: Monitoramento durante Operação e Manutenção 9](#_Toc99390728)

[3.8 Conclusões da Iteração 9](#_Toc99390729)

[4 Enésima iteração do Método Safety ArtISt 10](#_Toc99390730)

[4.1 Etapa 1: Especificação de Requisitos e Definição Preliminar da Arquitetura 10](#_Toc99390731)

[4.2 Etapa 2: Seleção e Análise de Bases de Dados de Entrada 10](#_Toc99390732)

[4.3 Etapa 3: Projeto Preliminar da IA 11](#_Toc99390733)

[4.4 Etapa 4: Projeto dos Modelos Base da IA 11](#_Toc99390734)

[4.5 Etapa 5: Treinamento e V&V Preliminar da IA 12](#_Toc99390735)

[4.6 Etapa 6: V&V Avançada da IA 12](#_Toc99390736)

[4.7 Etapa 7: Monitoramento durante Operação e Manutenção 13](#_Toc99390737)

[4.8 Conclusões da Iteração 13](#_Toc99390738)

[5 Conclusões 14](#_Toc99390739)

[6 Referências Bibliográficas 15](#_Toc99390740)

**CONTROLE DE REVISÕES DO RELATÓRIO**

| **Revisão** | **Data** | **Autor da Revisão** | **Descrição da Revisão** |
| --- | --- | --- | --- |
| 1 | 28/03/2022 | Antonio V. da S. Neto | Versão inicial de modelo para a documentação técnica dos estudos de caso do projeto de pesquisa Safety ArISt |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Introdução

O objetivo desta seção do documento é apresentar uma breve descrição do estudo de caso e da estratégia utilizada para realizá-lo, desde a especificação inicial de requisitos até as etapas de operação e manutenção do protótipo correlato. Deve-se descrever que todo o ciclo de vida do estudo de caso foi realizado aplicando-se o método Safety ArtISt (*Artificial Intelligence Structure*).

Dica geral: recomendado utilizar o software Mendeley para controle e citação de referências no texto. Utilizar padrão ABNT para as citações.

## Siglas e Abreviações

As siglas e abreviações utilizadas na elaboração deste documento são apresentadas a seguir.

<Instrução: uma sigla por linha da tabela, ordenando em ordem alfabética. Sempre que uma sigla aparecer no texto, deve ser definida por extenso na primeira ocorrência, apenas.>

|  |  |
| --- | --- |
| **ArtISt** | *Artificial Intelligence Structure* |

# Descrição do Sistema do Estudo de Caso

O objetivo desta seção é apresentar uma descrição de alto nível do sistema que pertence ao escopo do estudo de caso. Os seguintes tópicos devem ser, minimamente, abordados ao longo deste capítulo:

* Descrição das principais funções do sistema;
* Diagrama da arquitetura de alto nível do sistema;
* Descrição dos principais blocos que compõem o sistema.

# Primeira iteração do Método Safety ArtISt

O objetivo desta seção é apresentar os resultados da primeira iteração do método Safety ArtISt, evidenciando as decisões e os resultados de cada uma de suas etapas, atividades e subatividades.

## Etapa 1: Especificação de Requisitos e Definição Preliminar da Arquitetura

Nesta seção, devem ser apresentadas as seguintes características sobre a aplicação da etapa 1 do método Safety ArtISt:

* Detalhar restrições iniciais ao projeto (exemplo: deve ser feito para FPGA, deve ser feito em C/C++, etc.);
* Para cada atividade / subatividade:
  + Avaliar se é aplicável ao desenvolvimento e justificar a decisão;
  + Descrever quais os resultados obtidos e justifica-los.
* Ao final:
  + Detalhar os requisitos funcionais e não funcionais (especialmente de segurança) do sistema;
  + Detalhar a arquitetura preliminar do sistema.

## Etapa 2: Seleção e Análise de Bases de Dados de Entrada

Nesta seção, devem ser apresentadas as seguintes características sobre a aplicação da etapa 2 do método Safety ArtISt:

* Detalhar quais dados foram selecionados para o projeto, de onde foram obtidos e, se foram gerados especificamente para o estudo de caso, descrever como essa geração foi realizada;
* Para cada atividade / subatividade:
  + Avaliar se é aplicável ao desenvolvimento e justificar a decisão;
  + Descrever quais os resultados obtidos e justifica-los.
* Ao final:
  + Detalhar as bases de dados geradas ao final da etapa 2, incluindo sua estrutura e os testes estatísticos realizados para argumentar que tratam-se de versão apropriada para o seguimento do projeto;
  + Rastrear os resultados obtidos nos requisitos de segurança da etapa 1;

## Etapa 3: Projeto Preliminar da IA

Nesta seção, devem ser apresentadas as seguintes características sobre a aplicação da etapa 3 do método Safety ArtISt:

* Para cada atividade / subatividade:
  + Avaliar se é aplicável ao desenvolvimento e justificar a decisão;
  + Descrever quais os resultados obtidos e justifica-los.
* Detalhar os blocos funcionais da arquitetura, com seus respectivos componentes básicos de HW e SW. O detalhamento deve prever diagramas de arquitetura e descrições dos blocos e de suas interfaces;
* Detalhar as ferramentas que serão empregadas no projeto e, quando necessário, as configurações que serão adotadas;
* Detalhar e justificar as características de tolerância a falhas previstas no projeto, identificando o porquê de cada mecanismo e como eles se relacionam com os requisitos de segurança do sistema.
* Rastrear os resultados obtidos nos requisitos de segurança da etapa 1.

## Etapa 4: Projeto dos Modelos Base da IA

Nesta seção, devem ser apresentadas as seguintes características sobre a aplicação da etapa 4 do método Safety ArtISt:

* Para cada atividade / subatividade:
  + Avaliar se é aplicável ao desenvolvimento e justificar a decisão;
  + Descrever quais os resultados obtidos e justifica-los.
* Detalhar quais modelos base de bibliotecas de terceiros serão reaproveitados e quais serão desenvolvidos especificamente para o estudo de caso, justificando com base nas decisões globais da etapa 3;
* Detalhar as características dos modelos base, como elas foram escolhidas e por que foram selecionadas;
* Rastrear os resultados obtidos nos requisitos de segurança da etapa 1.

## Etapa 5: Treinamento e V&V Preliminar da IA

Nesta seção, devem ser apresentadas as seguintes características sobre a aplicação da etapa 5 do método Safety ArtISt:

* Para cada atividade / subatividade:
  + Avaliar se é aplicável ao desenvolvimento e justificar a decisão;
  + Descrever quais os resultados obtidos e justifica-los.
* Detalhar como foi realizado o treinamento dos modelos de aprendizado supervisionado;
* Detalhar os resultados de cada atividade / subatividade de V&V, identificando os problemas de segurança e categorizando-os como “verdadeiro positivo”, “falso positivo” e “falso negativo” (se introduzido deliberadamente pelo projetista);
* Se houver pelo menos um “verdadeiro positivo”, identificar causa raiz e iniciar nova iteração a partir da etapa da causa raiz da etapa mais inicial do projeto;
* Rastrear os resultados obtidos nos requisitos de segurança da etapa 5.

## Etapa 6: V&V Avançada da IA

Esta seção é aplicável apenas se a etapa 5 da iteração não tiver nenhum problema “verdadeiro positivo” ou “falso negativo”. Devem ser apresentadas as seguintes características sobre a aplicação da etapa 6 do método Safety ArtISt:

* Para cada atividade / subatividade:
  + Avaliar se é aplicável ao desenvolvimento e justificar a decisão;
  + Descrever quais os resultados obtidos e justifica-los.
* Detalhar os resultados de cada atividade / subatividade de V&V, identificando os problemas de segurança e categorizando-os como “verdadeiro positivo”, “falso positivo” e “falso negativo” (se introduzido deliberadamente pelo projetista);
* Se houver pelo menos um “verdadeiro positivo”, identificar causa raiz e iniciar nova iteração a partir da etapa da causa raiz da etapa mais inicial do projeto;
* Rastrear os resultados obtidos nos requisitos de segurança da etapa 6.

## Etapa 7: Monitoramento durante Operação e Manutenção

Esta seção é aplicável apenas se a etapa 6 da iteração não tiver nenhum problema “verdadeiro positivo” ou “falso negativo”. Devem ser apresentadas as seguintes características sobre a aplicação da etapa 6 do método Safety ArtISt:

* Definir qual a estratégia de prototipação do sistema para operação e manutenção;
* Para cada atividade / subatividade:
  + Avaliar se é aplicável ao desenvolvimento e justificar a decisão;
  + Descrever quais os resultados obtidos e justifica-los.
* Detalhar os resultados de cada atividade, com as respectivas reentrâncias em etapas pregressas durante a operação ou em eventuais manutenções;
* Rastrear os resultados obtidos nos requisitos de segurança da etapa 7.

## Conclusões da Iteração

Apresentar um breve resumo dos principais resultados da iteração (projeto, problemas de segurança e potenciais correções).

# Enésima iteração do Método Safety ArtISt

Esta seção deve ser instanciada tantas vezes quanto necessário sempre que as etapas 5 ou 6 da iteração anterior permitirem identificar problemas de segurança das categorias “verdadeiro positivo” ou “falso negativo”. A seção deve ser iniciada a partir da etapa do método Safety ArtISt rastreada na causa mais pregressa dos problemas constatados.

O objetivo desta seção é apresentar os resultados da enésima iteração do método Safety ArtISt, evidenciando as decisões e os resultados de cada uma de suas etapas, atividades e subatividades.

## Etapa 1: Especificação de Requisitos e Definição Preliminar da Arquitetura

Nesta seção, devem ser apresentadas as seguintes características sobre a aplicação da etapa 1 do método Safety ArtISt:

* Detalhar restrições iniciais ao projeto (exemplo: deve ser feito para FPGA, deve ser feito em C/C++, etc.);
* Para cada atividade / subatividade:
  + Avaliar se é aplicável ao desenvolvimento e justificar a decisão;
  + Descrever quais os resultados obtidos e justifica-los.
* Ao final:
  + Detalhar os requisitos funcionais e não funcionais (especialmente de segurança) do sistema;
  + Detalhar a arquitetura preliminar do sistema.

## Etapa 2: Seleção e Análise de Bases de Dados de Entrada

Nesta seção, devem ser apresentadas as seguintes características sobre a aplicação da etapa 2 do método Safety ArtISt:

* Detalhar quais dados foram selecionados para o projeto, de onde foram obtidos e, se foram gerados especificamente para o estudo de caso, descrever como essa geração foi realizada;
* Para cada atividade / subatividade:
  + Avaliar se é aplicável ao desenvolvimento e justificar a decisão;
  + Descrever quais os resultados obtidos e justifica-los.
* Ao final:
  + Detalhar as bases de dados geradas ao final da etapa 2, incluindo sua estrutura e os testes estatísticos realizados para argumentar que tratam-se de versão apropriada para o seguimento do projeto;
  + Rastrear os resultados obtidos nos requisitos de segurança da etapa 1;

## Etapa 3: Projeto Preliminar da IA

Nesta seção, devem ser apresentadas as seguintes características sobre a aplicação da etapa 3 do método Safety ArtISt:

* Para cada atividade / subatividade:
  + Avaliar se é aplicável ao desenvolvimento e justificar a decisão;
  + Descrever quais os resultados obtidos e justifica-los.
* Detalhar os blocos funcionais da arquitetura, com seus respectivos componentes básicos de HW e SW. O detalhamento deve prever diagramas de arquitetura e descrições dos blocos e de suas interfaces;
* Detalhar as ferramentas que serão empregadas no projeto e, quando necessário, as configurações que serão adotadas;
* Detalhar e justificar as características de tolerância a falhas previstas no projeto, identificando o porquê de cada mecanismo e como eles se relacionam com os requisitos de segurança do sistema.
* Rastrear os resultados obtidos nos requisitos de segurança da etapa 1.

## Etapa 4: Projeto dos Modelos Base da IA

Nesta seção, devem ser apresentadas as seguintes características sobre a aplicação da etapa 4 do método Safety ArtISt:

* Para cada atividade / subatividade:
  + Avaliar se é aplicável ao desenvolvimento e justificar a decisão;
  + Descrever quais os resultados obtidos e justifica-los.
* Detalhar quais modelos base de bibliotecas de terceiros serão reaproveitados e quais serão desenvolvidos especificamente para o estudo de caso, justificando com base nas decisões globais da etapa 3;
* Detalhar as características dos modelos base, como elas foram escolhidas e por que foram selecionadas;
* Rastrear os resultados obtidos nos requisitos de segurança da etapa 1.

## Etapa 5: Treinamento e V&V Preliminar da IA

Nesta seção, devem ser apresentadas as seguintes características sobre a aplicação da etapa 5 do método Safety ArtISt:

* Para cada atividade / subatividade:
  + Avaliar se é aplicável ao desenvolvimento e justificar a decisão;
  + Descrever quais os resultados obtidos e justifica-los.
* Detalhar como foi realizado o treinamento dos modelos de aprendizado supervisionado;
* Detalhar os resultados de cada atividade / subatividade de V&V, identificando os problemas de segurança e categorizando-os como “verdadeiro positivo”, “falso positivo” e “falso negativo” (se introduzido deliberadamente pelo projetista);
* Se houver pelo menos um “verdadeiro positivo”, identificar causa raiz e iniciar nova iteração a partir da etapa da causa raiz da etapa mais inicial do projeto;
* Rastrear os resultados obtidos nos requisitos de segurança da etapa 5.

## Etapa 6: V&V Avançada da IA

Esta seção é aplicável apenas se a etapa 5 da iteração não tiver nenhum problema “verdadeiro positivo” ou “falso negativo”. Devem ser apresentadas as seguintes características sobre a aplicação da etapa 6 do método Safety ArtISt:

* Para cada atividade / subatividade:
  + Avaliar se é aplicável ao desenvolvimento e justificar a decisão;
  + Descrever quais os resultados obtidos e justifica-los.
* Detalhar os resultados de cada atividade / subatividade de V&V, identificando os problemas de segurança e categorizando-os como “verdadeiro positivo”, “falso positivo” e “falso negativo” (se introduzido deliberadamente pelo projetista);
* Se houver pelo menos um “verdadeiro positivo”, identificar causa raiz e iniciar nova iteração a partir da etapa da causa raiz da etapa mais inicial do projeto;
* Rastrear os resultados obtidos nos requisitos de segurança da etapa 6.

## Etapa 7: Monitoramento durante Operação e Manutenção

Esta seção é aplicável apenas se a etapa 6 da iteração não tiver nenhum problema “verdadeiro positivo” ou “falso negativo”. Devem ser apresentadas as seguintes características sobre a aplicação da etapa 6 do método Safety ArtISt:

* Definir qual a estratégia de prototipação do sistema para operação e manutenção;
* Para cada atividade / subatividade:
  + Avaliar se é aplicável ao desenvolvimento e justificar a decisão;
  + Descrever quais os resultados obtidos e justifica-los.
* Detalhar os resultados de cada atividade, com as respectivas reentrâncias em etapas pregressas durante a operação ou em eventuais manutenções;
* Rastrear os resultados obtidos nos requisitos de segurança da etapa 7.

## Conclusões da Iteração

Apresentar um breve resumo dos principais resultados da iteração (projeto, problemas de segurança e potenciais correções).

# Conclusões

O objetivo desta seção é apresentar as conclusões do estudo de caso, contemplando minimamente os seguintes aspectos:

* Arquitetura e técnicas de tolerância a falhas envolvendo IA;
* Resultado global do estudo de caso (sistema “seguro” ou com problemas insolúveis);
* Velocidade de convergência para uma solução aceitável (em função do número de iterações do método) ou para problema insolúvel;
* Eficácia da etapa 5 em filtrar antecipadamente problemas da etapa 6. É possível antecipá-los, ou há mais chance de “exclusão mútua” entre ambas?;
* Principais problemas, desafios e resultados positivos encontrados durante o estudo de caso;
* Potenciais alterações e ajustes ao método Safety ArtISt para contornar os problemas e desafios verificados.

# Referências Bibliográficas

Inserir lista de referências aqui.

Dica global: utilizar software Mendeley e padrão ABNT.