UNIVERSIDADE DO VALE DO RIO DOS SINOS - UNISINOS
UNIDADE ACADÊMICA DE GRADUAÇÃO
CURSO DE ENGENHARIA ELETRÔNICA

GUILHERME LUIZ GOTARDO

SEGURANÇA FUNCIONAL APLICADA A CONTROLADORES INDUSTRIAIS PID: Um estudo de caso.

SÃO LEOPOLDO
2022

GUILHERME LUIZ GOTARDO

SEGURANÇA FUNCIONAL APLICADA A CONTROLADORES INDUSTRIAIS PID: Um estudo de caso.

Trabalho de Conclusão de Curso apresentado como requisito parcial para obtenção do título de Bacharel em Engenharia Eletrônica, pelo Curso de Engenharia Eletrônica da Universidade do Vale do Rio dos Sinos (UNISINOS).

Orientador: Prof. Dr. Marques Rodrigo de Figueiredo

São Leopoldo

2022

Dedico esse trabalho à minha mãe, Angela, que me apoiou em toda minha etapa acadêmica.

AGRADECIMENTOS

Deixo aqui meus agradecimentos, primeiramente à minha família, por ter suportado junto comigo o processo de graduação, pois foi uma etapa com muitos desafios e muitas privações, que só poderiam ser apoiados por aqueles que eu mais amo.

Agradeço também pela oportunidade que recebi de estudar na Unisinos, onde foi possível evoluir como pessoa, revolucionar a minha vida profissional e, principalmente, ser o local onde encontrei com uma pessoa fantástica e responsável por mudar completamente minha vida, tendo-a hoje como esposa. Obrigado por tudo, Jaqueline.

Minhas honras ao meu orientador, Prof. Dr. Rodrigo Marques de Figueiredo, que me acompanhou nessa jornada. Muito obrigado pelos conhecimentos compartilhados.

Meu obrigado também ao time da Novus, que me deu todo o suporte para a elaboração desse trabalho, tanto em material como em conhecimento. Quero dizer que vocês me fizeram evoluir muito nesse tempo que trabalhamos juntos.

Por fim, faço um agradecimento aos meus amigos que me acompanharam nessa jornada, pois vocês me ajudaram e muito nesse longo caminho até o final da graduação.

RESUMO

Existe hoje uma demanda para que equipamentos industriais operem de forma segura e tenham certificações apropriadas para isso, tal como a IEC 61508. Esta certificação garante que um equipamento ou sistema eletrônico opere de forma segura e assegura que, em caso de falha, o ambiente e as pessoas envolvidas estejam protegidos e o processo seja colocado em um estado seguro, evitando o máximo possível de danos. O presente trabalho se propõe a criar o protótipo de um controlador de temperatura PID com características de segurança funcional utilizando como base um controlador da empresa Novus Produtos Eletrônicos. Para cada funcionalidade do controlador, foi utilizado um equipamento com as devidas modificações em hardware e software para atender aos requisitos do produto. O trabalho tem seu objetivo validado através de testes realizados em ambiente controlado, simulando um controle de processo resistivo através ferramentas específicas para isso e injetando falhas específicas para validar o comportamento de modo seguro do sistema. Obteve-se os seguintes resultados em todos os testes: o funcionamento contínuo do controle do processo, quando ocorreu a primeira falha e o acionamento da saída de modo seguro, quando aconteceu a segunda falha.

Palavras-chave: segurança funcional; IEC 61508; controlador de temperatura PID; protótipo; sistema eletrônico.

LISTA DE FIGURAS

LISTA DE FOTOGRAFIAS

LISTA DE GRÁFICOS

LISTA DE QUADROS

LISTA DE TABELAS

LISTA DE SIGLAS

1oo1	*One out of One*
1oo2	*One out of Two*
1oo3	*One out of Three*
2oo3	*Two out of Three*
CE	*Conformité Européenne*
CPU	*Control Process Unit*
E/E/PES	*Electrical/Electronic/Programmable Electronic Safety-related Systems*
IEC	*International Electrotechnical Commission*
NA	Normalmente Aberto
$\mathrm{PDF}_{\mathrm{avg}}$	*Average Probability* of *failure on demand*
PFH	*Average Frequency of Dangerous Failures Per Hour*
PID	Proporcional Integral Derivativo
PV	*Process Variable*
PWM	*Pulse Width Modulation*
SIL	*Safety Integrity Level*
SIS	*Safety Instrumented System*
SP	*Setpoint*
UL	*Underwriters Laboratories*
UNISINOS	Universidade do Vale do Rio dos Sinos

SUMÁRIO

1 INTRODUÇÃO

O uso de controladores de temperatura Proporcional Integral Derivativo (PID) é amplamente difundido nas indústrias que atuam em diferentes processos de fabricação, sejam eles mais simples ou mais complexos. Além disso, empresas que fazem exportação de seus produtos eletrônicos voltados para esta área possuem certificações com foco voltado à proteção do usuário, tal como a certificação *Underwriters Laboratories* (UL) e certificação de Conformidade Europeia, em francês, *Conformité Européenne* (CE), voltado às restrições que um produto eletrônico deve seguir para poder ser vendido na União Europeia.

Até o momento, não há muitas opções de produtos ou equipamentos focados em segurança do processo ou segurança funcional, norma conhecida como Comissão Eletrotécnica Internacional 61508, em inglês, *International Electrotechnical* Commission 61508 (IEC 61508). No Brasil, a primeira solução industrial focada em segurança funcional foi da empresa Altus Sistemas de Automação, que junto à Universidade do Vale do Rio dos Sinos (UNISINOS), criaram uma solução focada neste ramo para atender a uma demanda de mercado vindo do setor de extração de petróleo.

A importância deste tipo de certificação é atender processos que possam vir a causar problemas graves em caso de falha, ou seja, a ideia é que o dispositivo que vai atuar neste processo seja tolerante a falhas e em caso de falha, ele entre em um estado seguro ou se autocorrija, continuando o controle do processo. Isso é necessário em processos que tenham um nível de perigo envolvido como por exemplo nos processos petrolíferos, controle de máquinas, indústria química, todo e qualquer processo que, em caso de perigo, possa levar a prejuízos ambientais, econômicos ou às próprias pessoas, sendo que no pior dos casos, possa levá-las a morte.

Este trabalho tem como objetivo realizar uma prova de conceito através da adaptação de hardware e *firmware* de um controlador de temperatura PID da empresa Novus Produtos Eletrônicos, para avaliar uma possível solução no controle de processos que tenha certificação em segurança funcional com arquitetura 2oo3. O foco do trabalho será onde é a parte crítica do processo que é na medição de temperatura e controle do processo. Já os atuadores e saídas digitais não farão parte do escopo, limitando-se ao uso das saídas originais e não modificada dos controladores.

Este trabalho está estruturado em cinco capítulos. Após a introdução, será apresentada a fundamentação teórica e suas referências. No terceiro capítulo, será demonstrada a metodologia utilizada para o desenvolvimento deste projeto. No quarto capítulo, será exposta a análise dos resultados obtidos nos testes de validação. Por fim, no quinto capítulo estão disponibilizadas as conclusões e juntamente a elas, as sugestões de estudos para trabalhos futuros.

2 FUNDAMENTAÇÃO TEÓRICA

A Novus Produtos Eletrônicos é uma empresa que atua nos segmentos de medição, registro de dados e controle de processos. Seus produtos possuem certificações de compatibilidade eletromagnética (IEC 61326-1: 1997 e IEC 61326-1/A1:1998), segurança (IEC61010-1:1993 e IEC61010-1/A2:1995), CE e UL.

Muitos dos produtos, sejam da linha de controle de processos ou temperatura, já possuem características de segurança, como por exemplo, a saída em modo seguro em caso de falha de sensor (sensor em aberto, por exemplo), levando o controle a um estado definido na configuração deste controlador. Entretanto, não há um produto que possua certificação específica em segurança funcional, tal como a IEC 61508. Deste modo, será apresentado o processo de adaptação do hardware e software de um controlador de temperatura PID para funcionar, de acordo com a norma IEC 61508 de segurança funcional.

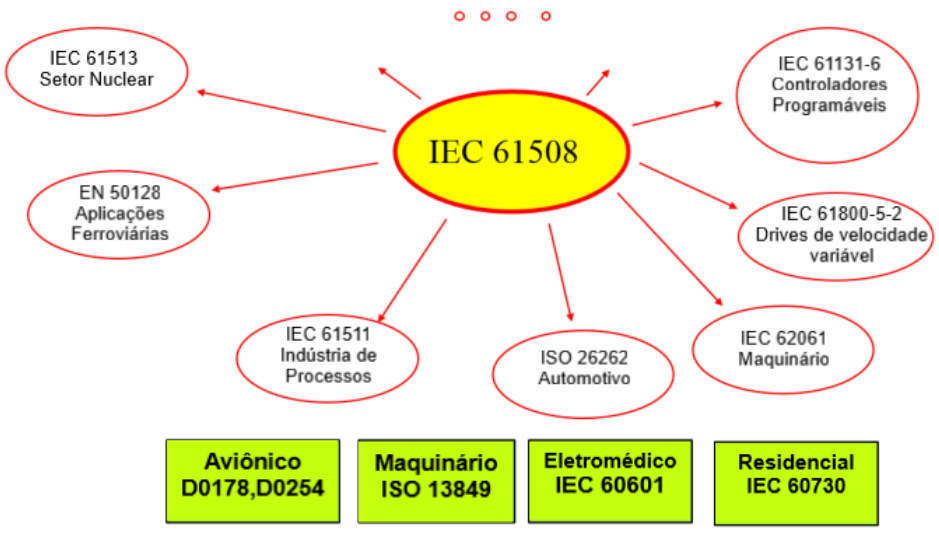
Nos subcapítulos a seguir serão trabalhados os tópicos de interesse deste trabalho, bem como aqueles que são base para seu bom entendimento. Será iniciado com um subcapítulo explicando a filosofia da norma IEC 61508 de forma resumida e, nos subcapítulos seguintes, serão abordados conceitos, tratamento e diagnóstico das falhas. Também serão tratados assuntos como o controle de processos industrial e os elementos que atuam e manipulam tais processos.

2.1 IEC 61508

A norma IEC 61508 tem a proposta de trazer padrões para o desenvolvimento de sistemas instrumentados de segurança, em inglês *safety instrumented system* (SIS), que possuem componentes elétricos e/ou eletrônicos e/ou sistemas eletrônicos programáveis relacionados à segurança, em inglês *Electrical/Electronic/Programmable Electronic Safety-related Systems* (E/E/PES), que serão aplicados para o controle de processos de alto risco e para que possam oferecer grande perigo para as pessoas ou ambiente ao redor em caso de falha (IEC). Julsereewon (2018) diz que o objetivo principal da segurança funcional é prover garantias de que o SIS funcionará corretamente para a redução de risco necessária para manter ou atingir um estado seguro para um processo industrial, ao detectar uma condição potencial de processo em perigo.

Deste modo, é preciso que o dispositivo que vai atuar no processo seja tolerante a falhas, ou seja, em caso de falha, ele entre em um estado seguro ou se autocorrija daquela falha e continue o controle do processo. Meany (2017) fala que o tempo para sair de um estado inseguro e chegar em um estado seguro é crítico devido às possíveis consequências físicas para as pessoas que estão ao redor. Portanto, uma das grandes importâncias do SIS é a velocidade de atuação ao identificar um estado inseguro e levar ao estado seguro. Moraes, Weber et al. (2018) dizem que, em vários setores da indústria, tais como extração de óleo, produção de energia e controle de máquinas são baseados na norma IEC 61508, fazendo-se necessário, nestes casos, a adequação necessária em processos que, em caso de perigo, possam levar a prejuízos ambientais, econômicos ou às próprias pessoas (e no pior dos casos, levá-las à morte). A partir da norma IEC 61508, também deriva sua base a outras normas de segurança para diferentes áreas de atuação, como por exemplo, para a indústria de processos (IEC 61511), para o setor nuclear (IEC 61513), aplicações ferroviárias (EN 50128), o setor automotivo (ISO 26262) entre outros, como mostra a Figura 1.

Figura 1 – Certificação IEC 61508 e suas derivações



Fonte: Adaptado de Meany (2017, p. 20).

O subcapítulo 2.1.1 descreve sobre conceitos importantes para o entendimento da norma IEC 61508, a seguir.

2.1.1 Defeito, Falha e Erro

É caracterizado um defeito quando um circuito não possui um funcionamento correto daquilo que foi projetado para realizar. Podem ter três origens diferentes: defeito físico, defeito de projeto e defeito de utilização (Balen & Lubaszewski, 2014). O defeito físico é relacionado a uma imperfeição física presente em um circuito. Pode ser referente ao material da qual, por exemplo, um circuito integrado foi produzido (imperfeições não desejadas na estrutura do material semicondutor) ou na etapa de fabricação (ausência de contatos, *pads* ou vias, componentes com tolerância maior que o limite) (Balen & Lubaszewski, 2014).

Defeito de projeto é relacionado ao projeto do circuito/dispositivo que não pode ser verificado antes da fabricação, causando, por exemplo, defeitos elétricos no sistema. Já o defeito de utilização está relacionado com a má utilização do circuito ou uso em condições inapropriadas, como por exemplo, utilizar em ambientes com temperaturas não adequadas ao dispositivo e/ou ambientes hostis (ruídos, radioatividade). A falha é caracterizada por um defeito interno. Ela só é visível ao fazer testes lógicos no circuito observando sua resposta. São exemplos de falha o curto-circuito ou circuito aberto em pinos de entrada ou saídas do circuito e só serão identificadas ao fazer testes correspondentes a esses pinos. Por último, o erro é a manifestação externa de uma falha (2014), ou seja, ao ocorrer uma falha no circuito, a resposta na saída é o erro identificado (Balen & Lubaszewski, 2014). No próximo subcapítulo, serão vistos os principais indicadores utilizados pela norma IEC 61508 para medir a probabilidade de falha de um sistema.

2.1.2 Indicadores de medição da falha

São definidos no capítulo 3.5.16 da IEC 61508-4 2010 três modos de operação de um E/E/PES:

a) *Low demand mode*, que traduzida para o português é modo de baixa demanda, a operação em modo seguro é performada apenas em demanda e sua frequência não é maior que uma vez ao ano.
b) *High demand mode*, que traduzida para o português é modo de alta demanda a operação em modo seguro também é performada apena sob demanda e sua frequência é mais que uma vez por ano;

c) *Continuous mode*, que traduzida para o português é modo continuo a função segura faz parte da operação normal.

A forma em que pode ser medida a eficácia da função segura de um E/E/PES é através de indicadores chamados:

a) *Average Probability* of *failure on demand* $\left(\mathrm{PDF}_{\mathrm{avg}}\right)$ – Probabilidade média de falha sob demanda.
b) *Average Frequency of Dangerous Failures Per Hour* (PFH) – Frequência média de falhas perigosas por hora.

Torres (2020) diz que um E/E/PES operando em *low demand mode*, utiliza $\mathrm{PDF}_{\mathrm{avg}}$ como um indicador apropriado para confiabilidade. Isto se deve ao fato de que em *low demand mode*, a probabilidade de falha ser menor do que em high/continuous mode.

No subcapítulo 2.1.3 será visto como os indicadores de falha são aplicados para decidir o nível de segurança de um E/E/PES.

2.1.3 Nível de Integridade de Segurança

A definição de integridade de segurança, segundo a norma IEC 61508 2010, em inglês *Safety Integrity*, é a probabilidade de um sistema relacionado à segurança performar satisfatoriamente as funções seguras necessárias sobre todas as condições estabelecidas. Sendo assim, um dispositivo pode ter classificações sobre a função de segurança em que ele atuará, de acordo com os riscos envolvidos no processo. Surge então, os níveis associados a cada uma dessas funções de segurança, chamado *Safety Integrity Level*.

O nível de integridade de segurança (em inglês *Safety Integrity Level* – SIL) é definido como uma medida da confiabilidade esperada de um sistema para executar sua função segura (Torres, 2020). Trata-se de uma medida que representa a redução de riscos de uma função segura, de modo que, quanto maior o nível, mais rigorosas devem ser as especificações do projeto. Esses níveis são tabelados pela IEC 61508 2010 e variam conforme o nível de segurança exigido pelo processo em que o dispositivo E/E/PES irá atuar. As Tabelas 1 e 2 mostram os níveis de segurança para cada aplicação exigida.

Tabela 1 - Probabilidade média de falha sob demanda

Nível SIL	$\mathrm{PDF}_{\mathrm{avg}}$	Eficácia Necessária
4	$\geq 10^{-5}$ a $< 10^{-4}$	99,99% a 99,999%
3	$\geq 10^{-4}$ a $< 10^{-3}$	99,9% a 99,99%
2	$\geq 10^{-3}$ a $< 10^{-2}$	99% a 99,9%
1	$\geq 10^{-2}$ a $< 10^{-1}$	90% a 99 %

Fonte: Adaptado de IEC 61508 – 6 (2010).

Tabela 2 - Frequência média de falhas perigosas por hora

Nível SIL	PFH	Eficácia Necessária
4	$\geq 10^{-5}$ a $< 10^{-4}$	99,99% a 99,999%
3	$\geq 10^{-4}$ a $< 10^{-3}$	99,9% a 99,99%
2	$\geq 10^{-3}$ a $< 10^{-2}$	99% a 99,9%
1	$\geq 10^{-2}$ a $< 10^{-1}$	90% a 99 %

Fonte: Adaptado de IEC 61508 – 6 (2010).

Quanto mais riscos estiverem envolvendo o processo, maior o SIL associado, isso vale tanto para processos que envolvam *low demand*, nesse caso utilizando o parâmetro $\mathrm{PDF}_{\mathrm{avg}}$, quanto para *continuous/high demand*, utilizando PHF.

Além disso, a norma não especifica o SIL, pois isso depende do tipo de aplicação do sistema E/E/PES. A norma nesse caso sugere a consulta aos órgãos/comitês adequados para que se busquem as especificidades necessárias para o produto.

Para atingir os níveis necessários de SIL, algumas técnicas são empregadas para avaliar a probabilidade de falhas no hardware do sistema. Essas técnicas serão apresentadas e exemplificadas na seção 2.2 deste trabalho.

2.2 Arquiteturas de tolerância a falha

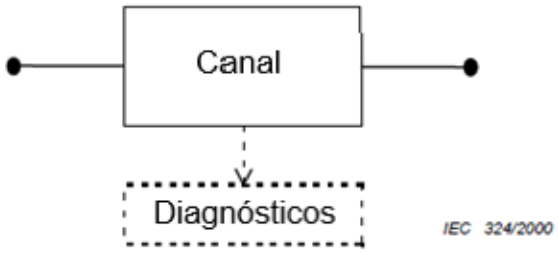
São descritos na norma IEC 61508 2010 algumas técnicas de tolerância a falha em hardware que devem ser escolhidas adequadamente para atingir o objetivo de deixar aquela parte do sistema com maior confiabilidade. Torres (2020) fala que a IEC 61508, IEC 61551 e ISA TR 84.00.02 recomendam diferentes métodos analíticos para quantificar a probabilidade de falha e o SIL necessário. Cada arquitetura possui um equacionamento da sua taxa de falha perigosa, sendo elementos importantes na hora de definir o nível SIL do sistema.

As arquiteturas citadas serão usadas para a operação em baixa demanda (*Low Demand Mode*) devido à especificação do trabalho.

2.2.1 Arquitetura 1oo1

Essa arquitetura 1 *out of* 1 (1oo1) é a mais simples, que consiste em apenas um canal/caminho e qualquer falha ocorrida leva o sistema a executar sua função segura. A figura 2 mostra o diagrama de blocos da arquitetura 1oo1.

Figura 2 - Diagrama de blocos da arquitetura 1oo1



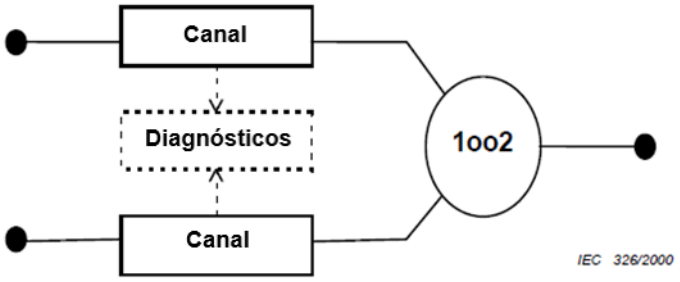
Fonte: Adaptado de IEC 61508-6 (2010).

Os próximos subcapítulos apresentam arquiteturas redundantes com sistemas de votação na saída.

2.2.2 Arquitetura 1oo2

A arquitetura 1 *out of* 2 (1oo2) se trata de dois canais que estão conectados em paralelo, e só vão executar a função de segurança se qualquer um deles estiver em estado de falhas perigosas. A figura 3 mostra o diagrama de blocos da arquitetura 1oo2.

Figura 3 - Diagrama de blocos da arquitetura 1oo2



Fonte: Adaptado de IEC 61508-6 (2010).

As equações para a taxa de falhas perigosas por hora, em inglês *dangerous failure rate (per hour)*, do canal são compostas da soma de duas componentes: a taxa de falhas não detectadas por hora, em inglês *undetected dangerous failure rate (per hour)*, e a taxa de falhas detectadas por hora, em inglês *detected dangerous failure rate (per hour)*. A equação é representada então por:

$$\lambda_D = \lambda_{DU} + \lambda_{DD} \quad (1)$$

Onde λ_D, λ_{DU} e λ_{DD} são respectivamente a taxa de falhas perigosas por hora, a taxa de falhas não detectadas por hora e a taxa de falhas detectadas por hora.

Aplicações que necessitem de apenas uma redundância sem um sistema de votação majoritária utiliza esse tipo de arquitetura, por exemplo, uso de dois sensores (IEC 61508-6, 2010).

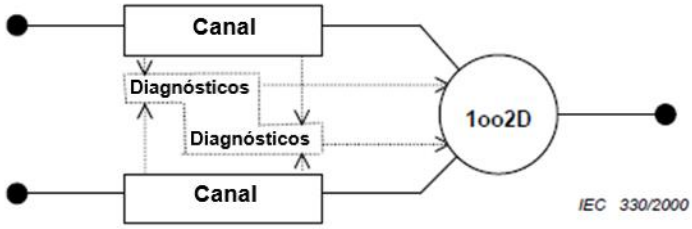
O subcapitulo 2.2.2 irá falar sobre arquitetura com estrutura de diagnóstico.

2.2.3 Arquitetura 1oo2D

A arquitetura *1 out of 2 Diagnostics* (1oo2D), mostrada na Figura 4, se trata da mesma estrutura 1oo2 com uma estrutura de diagnóstico a mais. Esta estrutura executa testes e caso encontre falha em um dos canais, a saída é adaptada para que siga o mesmo resultado da saída do outro canal que não está com falha. Se houver

falha em ambos os canais, ou uma discrepância que não permita a alocação da saída do canal com falha para seguir a saída do canal sem falha, o sistema então executa a função segura. A figura 4 mostra o diagrama de blocos da arquitetura 1oo2D.

Figura 4 - Diagrama de blocos da arquitetura 1oo2D



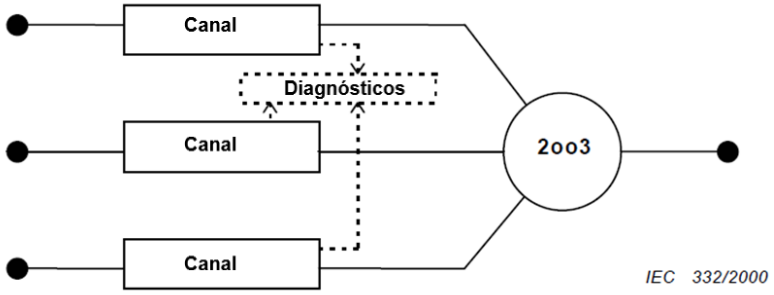
Fonte: Adaptado de IEC 61508-6 (2010).

O subcapítulo 2.2.3 irá falar sobre a arquitetura do tipo votação majoritária.

2.2.4 Arquitetura 2oo3

Esse tipo de arquitetura *2 out of 3* (2oo3) ou *1 out of 3* (1oo3) se trata de três canais (cada qual representa um sistema) que estão conectados em paralelo, e operam sob forma de votação majoritária para decidir o estado da saída. A diferença fundamental entre as arquiteturas 2oo3 e 1oo3 está na execução da função segura. A arquitetura 2oo3 executa a função segura quando quaisquer dos dois canais estão em falha, ao passo que a arquitetura 1oo3 considera executar a função segura quando apenas um canal está em estado de falha. A figura 5 mostra a arquitetura 2oo3.

Figura 5 - Diagrama de blocos da arquitetura 2oo3



Fonte: Adaptado de IEC 61508-6 (2010).

A utilização deste sistema pode ser exemplificada com três módulos redundantes de saída digital que votam em qual deve ser o estado do atuador do processo. Em caso de falha de um, o próximo assume o papel do defeituoso, fazendo com que o sistema não pare de funcionar.

A seção 2.3 abordará sobre o assunto de controle de processos industriais.

2.3 Controle de Processos Industriais

Para explicar o controle de processos, é necessário primeiro defini-lo. Segundo Franchi (2011, p. 18), o processo é:

> Um termo utilizado para descrever os métodos de mudança ou refinamento de matérias-primas para obter produtos finais. Essas matérias-primas, que podem ser liquidas, gasosas, solidas ou uma mistura entre fases, durante o processo, são transferidas medidas, misturadas, aquecidas, resfriadas, filtradas, armazenadas ou tratadas de uma determinada forma para desenvolver o produto final.
> Nas indústrias de processos podem ser incluídas aquelas de óleo e gás, bebidas e alimentos, farmacêuticas, açúcar e álcool, entre outras.

Um processo pode ser representado por um bloco, conforme a Figura 6, que possui uma entrada (matéria-prima), um modificador dessa entrada (sistema de controle) e uma saída obtida (produto final). Por fim, o sistema de controle é o meio pelo qual se faz o controle das saídas de um processo com um determinado desempenho através de uma entrada especificada (NISE, 2017).

Figura 6 - Descrição simplificada de um processo genérico

Fonte: Adaptado de Nise (2017).

Exemplos de processos incluem processos de refinaria de óleo, aquecimento de caldeiras, processos de fornalha de craqueamento para quebra de óleo cru, trocadores de calor entre outros. Dentre inúmeros processos, alguns devem ter um maior cuidado na implementação do controle devido ao seu grau de risco de acidentes. Torres (2020) cita alguns exemplos de processos que causaram acidentes e fatalidades devido a falhas em sistemas de segurança críticos:

a) acidente com queda do *Boing* 737 Max-8, em março de 2019 no leste da África;
b) derramamento de óleo da *Deepwater Horizon*, em abril de 2010 no golfo do México
c) explosão e incêndio na refinaria BP Texas City, em março de 2005 no estado do Texas, Estados Unidos da América (EUA);
d) explosão e incêndio na fábrica de plásticos *Formosa Plastics*, em abril de 2004 no estado do Texas, EUA;
e) explosão e incêndio na plataforma de produção de petróleo North Sea, em julho de 1988 no Reino Unido;
f) ruptura num reator químico causando problemas de saúde de longo prazo e milhares de animais mortos, em julho de 1976 na Itália;
g) explosão em uma fábrica de produtos químicos, em junho de 1974 no Reino Unido.

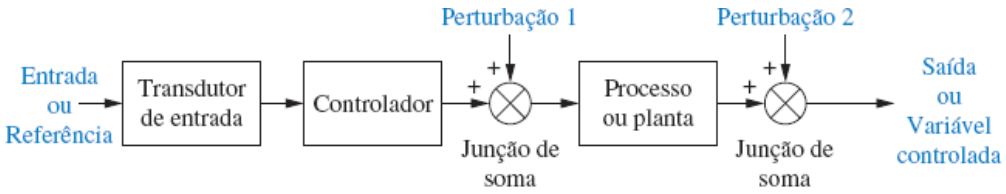
Torres (2020) também diz que a maior causa dessas falhas foi a manutenção inadequada no sistema, *design* inseguro dos processos, gerenciamento de segurança inadequado, falta de uma cultura de segurança, procedimentos de segurança, entre outros. Por isso, é importante haver não só um sistema, mas todo um gerenciamento e hábitos/práticas que levem à organização a ter uma consciência sobre a importância de ter um processo seguro e com prevenção de riscos.

Nos próximos subcapítulos, serão vistos os dois sistemas de controle que existem e suas características.

2.3.1 Sistema de Malha Aberta

O sistema de malha aberta faz o controle do processo de modo independente do estado da saída, pois não há um elemento de realimentação no circuito (Franchi, 2011). Desse modo, o controle não consegue perceber perturbações na entrada e nem fazer correções a elas, sendo um sistema que que é simplesmente comandado pela entrada (Nise, 2017). A Figura 7 demonstra o diagrama de blocos de um sistema de malha aberta.

Figura 7 – Sistema de malha aberta



Fonte: Nise (2017, p. 6).

A seguir, o subcapítulo 2.3.2 abordará os sistemas de malha fechada.

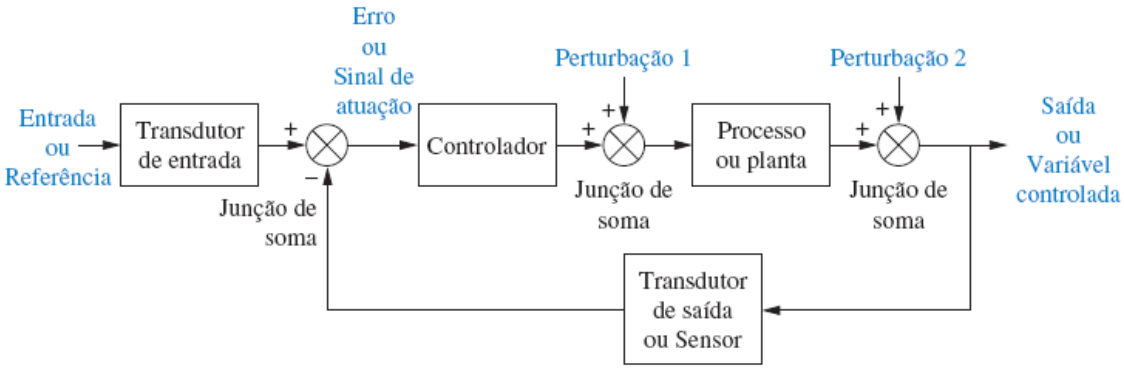
2.3.2 Sistema de Malha Fechada

Um sistema de malha fechada é um sistema de controle que ao contrário de um sistema de malha aberta, faz o controle do processo de modo dependente do estado da saída. Esse sistema possui meios de medir a saída, também conhecido como variável de processo, em inglês *Process Variable* (PV), comparar com o valor desejado na entrada, conhecido como *Setpoint* (SP) e efetuar uma correção para que o sistema chegue a esse valor (Franchi, 2011). Esse efeito de comparar a saída com a entrada é chamado de malha de realimentação, em inglês *feedback*, e é representado por uma junção de soma negativa no diagrama de blocos da Figura 8.

Já em relação às perturbações que possam ocorrer no sistema, Nise (2017, p. 06) diz que:

> O sistema em malha fechada compensa o efeito das perturbações medindo a resposta da saída, realimentando essa medida através da malha de realimentação e comparando essa resposta com a entrada na junção de soma. Se existir qualquer diferença entre as duas respostas, o sistema aciona a planta, através do sinal de atuação, para fazer uma correção. Se não há diferença, o sistema não aciona a planta, uma vez que a resposta da planta já é a resposta desejada.

Figura 8 - Diagrama de blocos de um sistema de malha fechada



Fonte: NISE (2017, p. 6)

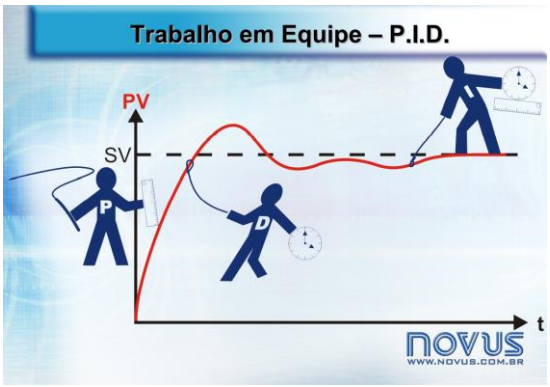
O subcapítulo 2.4 abordará sobre o processo de controle PID e suas características.

2.4 Controladores PID

Esses controladores utilizam a configuração malha fechada (com realimentação), proporcionando a vantagem de não haver necessidade de conhecer a fundo o processo (Franchi, 2011). Além disso, os controladores têm a capacidade de, quando configurados corretamente, fazer o controle antecipatório, diminuir e eliminar ruídos, tornando-o desejável no controle de processos (Alpi, 2019).

O controle PID é composto de três controles diferentes: controle proporcional, controle Integral e controle derivativo e cada tipo atua de forma diferente no processo, demonstrado pela Figura 9:

Figura 9 – Trabalho em conjunto dos componentes do controle PID



Fonte: Dillenburg (2019).

Segundo Dillenburg (2019):

a) a componente proporcional faz uma correção proporcional ao erro do sistema.
b) a componente integral faz uma correção mais intensa relacionado ao produto erro x tempo e elimina desvios causados pela componente proporcional
c) o componente derivativo faz uma correção relacionada à velocidade de variação do erro, fazendo com que se reduza as oscilações do sistema.

A combinação desses três componentes do PID é capaz de fazer com que o sistema tenha erros nulos, efeitos oscilatórios suprimidos e uma boa estabilidade no processo (Alpi, 2019).

2.5 Trabalhos correlatos

Usou-se, neste trabalho, o artigo *Architecture of an industrial analog input designed to meet safety requirements* Moraes et al (2018)., em que foi relatada a arquitetura do hardware de um módulo de entrada analógica com SIL 3 em parceria com uma fabricante de equipamentos de controle industrial. Assim, este trabalho foi importante para entender como foi realizada a redundância no sistema e principalmente a comunicação entre o dispositivo modular com a CPU controladora do sistema.

O próximo capítulo irá apresentar a metodologia utilizada para desenvolver esse projeto.

3 METODOLOGIA

No presente trabalho de pesquisa é descrito o projeto da modificação de um produto já homologado pelo mercado para receber melhorias nas características de segurança e atender assim o objetivo proposto para este trabalho.

No próximo subcapítulo serão descritas as características do controlador N1200.

3.1 Características do controlador N1200

O controlador de temperatura PID em questão é um equipamento eletrônico que possui na sua forma mais básica: uma entrada analógica, um processador central e uma saída. A Figura 10 mostra um controlador de temperatura da Empresa Novus Produtos Eletrônico.

Figura 10 – Controlador de temperatura PID N1200

Fonte: NOVUS (2022).

Este controlador trata-se de um N1200, que faz parte de uma linha dos controladores mais avançados e com mais recursos programáveis, tais como:

a) entrada universal multissensor, sem alteração de hardware;
b) proteção para sensor aberto em qualquer condição;
c) saídas de controle do tipo relé, 4-20 mA e pulso, todas disponíveis;
d) autossintonia dos parâmetros PID;
e) função Automático/Manual com transferência “*bumpless*”;

f) quatro alarmes independentes, com funções de mínimo, máximo, diferencial (desvio), sensor aberto e evento;
g) temporização para todos os alarmes;
h) retransmissão de PV ou SP em 0-20 mA ou 4-20 mA;
i) entrada para *setpoint* remoto;
j) entrada digital com 5 funções;
k) *soft-start* programável;
l) rampas e patamares com 20 programas de 9 segmentos, concatenáveis num total de 180 segmentos;
m) senha para proteção do teclado;
n) função LBD (*loop break detector*);
o) alimentação *bivolt*.

3.2 Componentes tolerantes a falha

O controlador de temperatura PID é dividido em partes de funcionamento independentes: Alimentação, Interface Homem-Máquina (IHM), tal como *display* e teclado, entrada analógica (sensores termopares, PT100 e entradas lineares), unidade de processamento central (CPU) para tomada de decisão, saída analógica, saída pulsada, saída a relé e barramento de comunicação serial *Modbus* (RS485). Alguns componentes têm importância severa quanto ao funcionamento do equipamento, enquanto outros não têm influência em comportamentos que levem o sistema a uma falha. A seguir, será descrito o seu grau de influência no sistema e se deve ou não ter tolerância a falha.

a) IHM: É composta de um *display* para visualizar os parâmetros e o teclado para acessá-lo. Estes componentes não têm influência em um possível mau comportamento do controlador do processo em caso de falha devido a sua influência de exibir e modificar as suas configurações.

b) Alimentação: É um componente de alto grau de importância, pois tem a função de energizar e manter o funcionamento de todo o circuito. Para

um sistema de segurança funcional, é crítico haver redundância da alimentação.

c) CPU: Parte fundamental na tomada de decisão e lógica do circuito. É responsável por controlar o processo na forma de um *loop* de malha aberta ou fechada. Assim como na alimentação, é importante haver uma redundância neste ponto, de modo a haver um segundo elemento que garante o funcionamento do sistema.

d) Entradas analógicas: Normalmente utilizada como entrada de sensor ou entrada de sinal linear (entrada de corrente ou tensão). Em controladores universais de processos, normalmente é utilizado N tipos de sensores termopares, sensores resistivos do tipo PT (Pt100, Pt1000), entradas de corrente com padrão 0-20 ou 4-20 mA e entradas de tensão (50mV, 5V ou 10V). Esta parte também é essencial para o processo, pois tem a função de informar a CPU de controle as informações sobre a temperatura do processo.

e) Saídas digitais: São responsáveis por atuar no processo sendo essas feitas por relé ou sinal pulso para ligar um SSR. A saída digital do controlador é a parte que aciona os atuadores em um modelo *on-off* ou por Modulação por Largura de Pulso, em inglês Pulse Width Modulation (PWM).

3.3 Requisitos de produto

Os controladores Novus contam com aplicações em diferentes negócios e processos, entre eles o controle de temperatura de fornos industriais, refrigeração no processo de fabricação de cerveja, controle de umidade em estufas entre muitas outras aplicações. Foram utilizados controladores N1200 da fabricante Novus, que desempenham as seguintes funções: entrada analógica, CPU de controle e CPU Mestre para elaborar a prova de conceito de um controlador de temperatura com características de segurança funcional que será chamado nesse ponto de Controlador *Safety*.

Em cada módulo (entrada analógica, CPU e mestre), um controlador N1200 desempenhou tal função, totalizando seis controladores N1200 no projeto. Para ocorrer a atuação da saída digital no processo, optou-se por um módulo de relé, que pode ser acionado por ambas as CPU's controladoras. Seu software e seu hardware foram adaptados para receber as modificações necessárias.

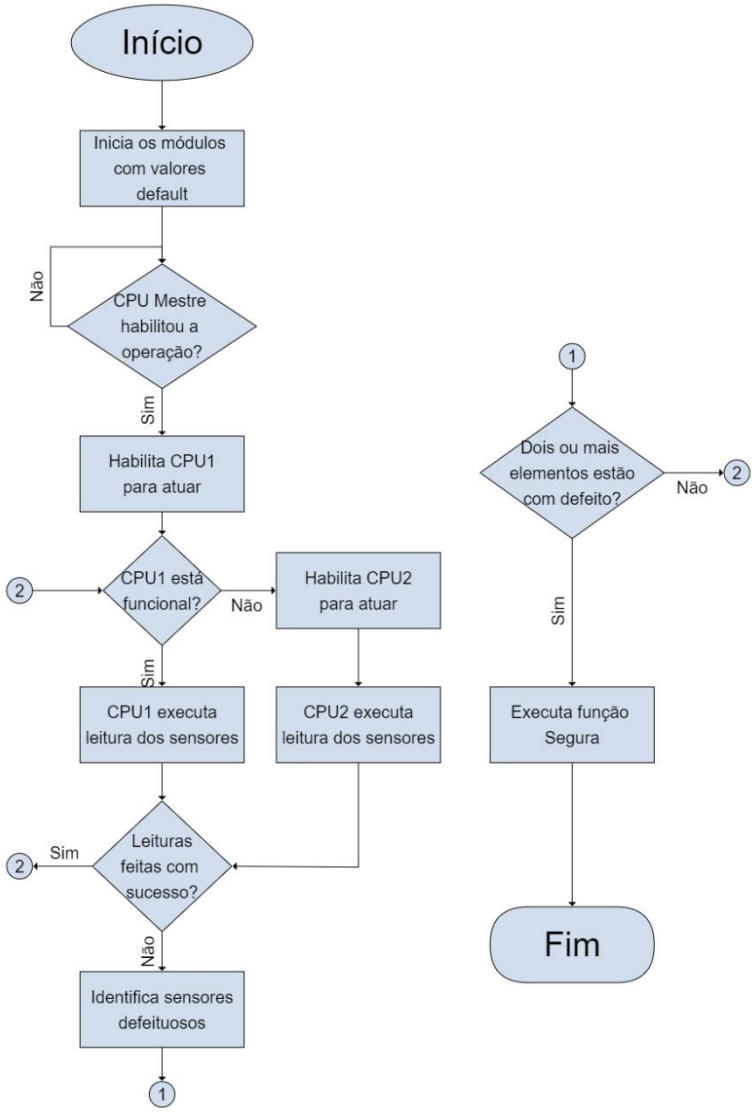
Os requisitos do projeto são:

a) Três CPU's para fazer a leitura das entradas analógicas utilizando sensores termopares tipo K;
b) Faixa de leitura do sensor de -110 a 1370 °C;
c) Duas CPU's para controle de processo;
d) Uma CPU mestre para habilitar ou desabilitar as CPU's que atuarem diretamente no processo;
e) Comunicação Serial *Modbus* RTU entre CPU de controle e CPU de entrada analógica;
f) Atuador do processo com módulo de relé;
g) Processo de aquecimento resistivo;
h) Arquitetura 2oo3.

O Controlador *Safety* é integrado de forma modular, ou seja, ele possui partes que funcionam independentes e sua comunicação é do tipo serial. As CPU's que controlam o processo utilizam o mesmo barramento de comunicação RS485 e ambos utilizam a arquitetura mestre, enquanto as CPU's de entradas analógicas atuam como escravos, fazendo as medidas e as fornecendo-as para as controladoras. Há também uma CPU mestre que pode habilitar ou desabilitar a CPU controladora e recebe o sinal de *Keep Alive* dessas CPU's, sinal esse que em caso de timeout de 500 ms, a CPU mestre desabilita a CPU controladora atual e habilita a próxima, continuando desse modo o processo em execução. A arquitetura 2oo3 conta com um sistema de votação majoritária e garante que só haverá execução da função de segurança em caso de 2 módulos em falha.

A figura 11, a seguir, mostra o fluxograma do processo de funcionamento.

Figura 11 - Fluxograma de funcionamento do Controlador *Safety*



Fonte: Elaborada pelo autor (2022).

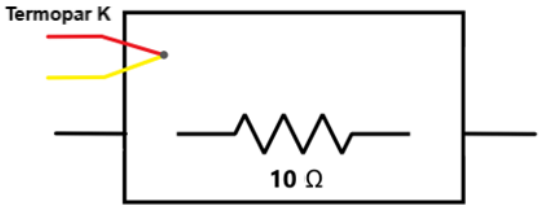
Dessa forma, o trabalho é separado em cinco etapas independentes: processo, entradas analógicas, CPU de controle, CPU Mestre e atuador. Nas próximas seções serão abordadas cada uma dessas etapas.

3.4 Processo Resistivo

Utilizou-se um processo do tipo resistivo para simular o ambiente de controle para o Controlador *Safety*. Seu funcionamento é feito aplicando uma tensão elétrica entre os terminais do resistor de mais ou menos 5 V em corrente contínua (VCC),

fazendo com que a energia elétrica seja transformada em energia térmica dissipada pela carcaça do resistor. A Figura 12 mostra a representação do processo resistivo.

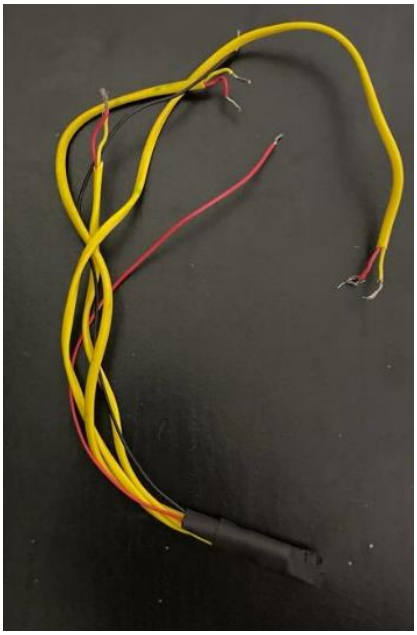
Figura 12 – Representação em bloco do processo resistivo utilizado no projeto



Fonte: Elaborada pelo autor (2022).

Sua construção se fez colocando três termopares do tipo K isolados com tubo termo retrátil em volta da superfície do resistor, de forma a ficarem os mais próximos possíveis da área de aquecimento. Desse modo, foi obtido um processo em malha fechada, com uma entrada, uma saída e um *feedback* negativo representado pelos termopares. A Fotografia 1 mostra o processo resistivo utilizado.

Fotografia 1 - Processo Resistivo com três termopares



Fonte: Registrada pelo autor (2022).

O próximo subcapítulo tratará de falar sobre as CPU’s de entrada analógica do sistema.

3.5 Entrada Analógica

A entrada analógica do Controlador *Safety* é composta por três CPU's, cujo processo de medição tem as mesmas características do controlador original N1200 e cada CPU possui um endereço próprio *Modbus* na configuração escravo. Para esse projeto, foram utilizados os endereços 1, 2 e 3.

Após fazer uma leitura válida, ou seja, com a entrada de sensor válida e dentro da faixa de medição do termopar K, o resultado absoluto é armazenado em um registrador interno chamado HR_PV. No momento de uma requisição de leitura via *Modbus*, a CPU do sensor verifica se o pacote tem como destino o endereço escravo configurado, verifica o CRC e reenvia a resposta. É esperado que a CPU de entrada analógica sempre receba um comando de leitura para o *holding register* HR_PV, que é o endereço 1. O Quadro 1 mostra todas as possibilidades de pacotes que as CPU's de entrada analógica receberão e o quadro mostra as respostas.

Quadro 1 – Pacotes de requisição para leitura do Sensor

Escravo	Comando	Endereço do primeiro *Holding Register*	Número total de *Holding Registers* requisitados	CRC para checagem de erros
0x01	0x03	0x01	0x01	0xD5CA
0x02	0x03	0x01	0x01	0xD5F9
0x03	0x03	0x01	0x01	0xD428

Fonte: Elaborado pelo autor (2022).

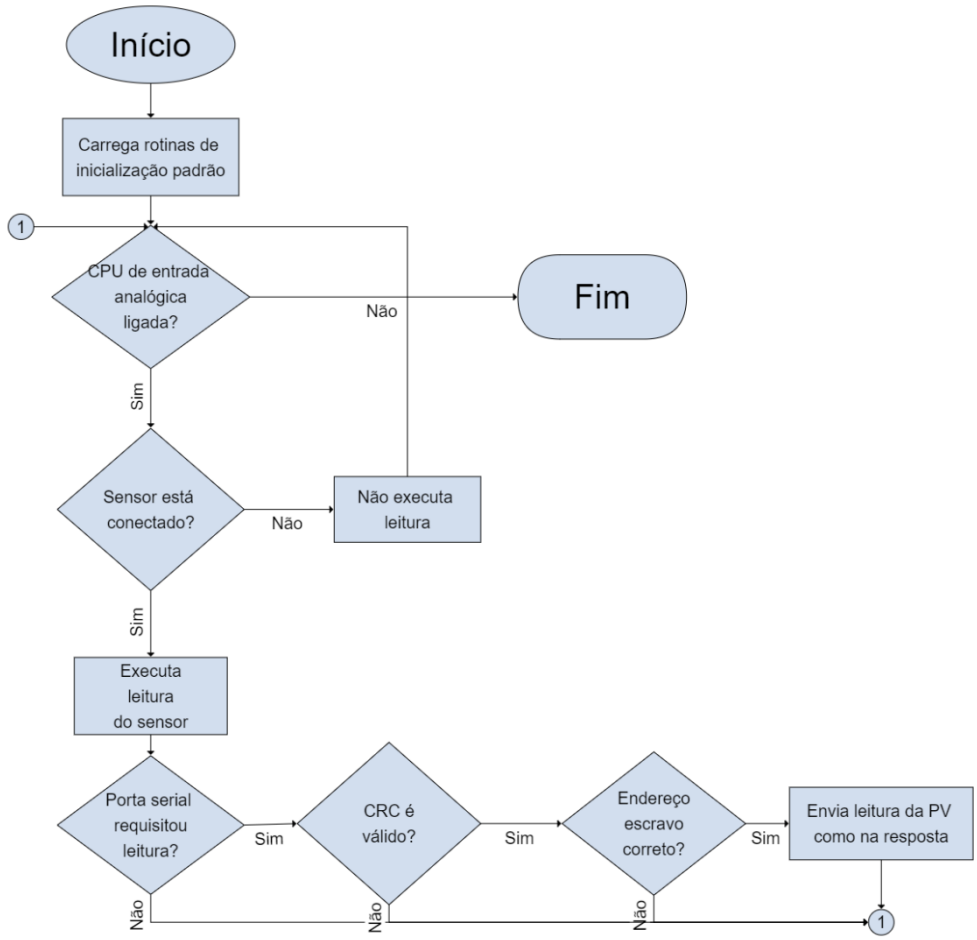
Quadro 2 - Pacotes de resposta para requisição de leitura do Sensor

Escravo	Comando	Número de *bytes* da resposta	Conteúdo do registrador	CRC para checagem de erros
0x01	0x03	0x02	(valor do sensor)	(valor variável)
0x02	0x03	0x02	(valor do sensor)	(valor variável)
0x03	0x03	0x02	(valor do sensor)	(valor variável)

Fonte: Elaborado pelo autor (2022).

O pacote de resposta completo do quadro depende do que é lido no sensor, desse modo foi colocado apenas os comandos que são fixos. A Figura 13 mostra o fluxograma completo das CPU's de entrada analógica.

Figura 13 - Fluxograma de funcionamento da CPU de entrada analógica



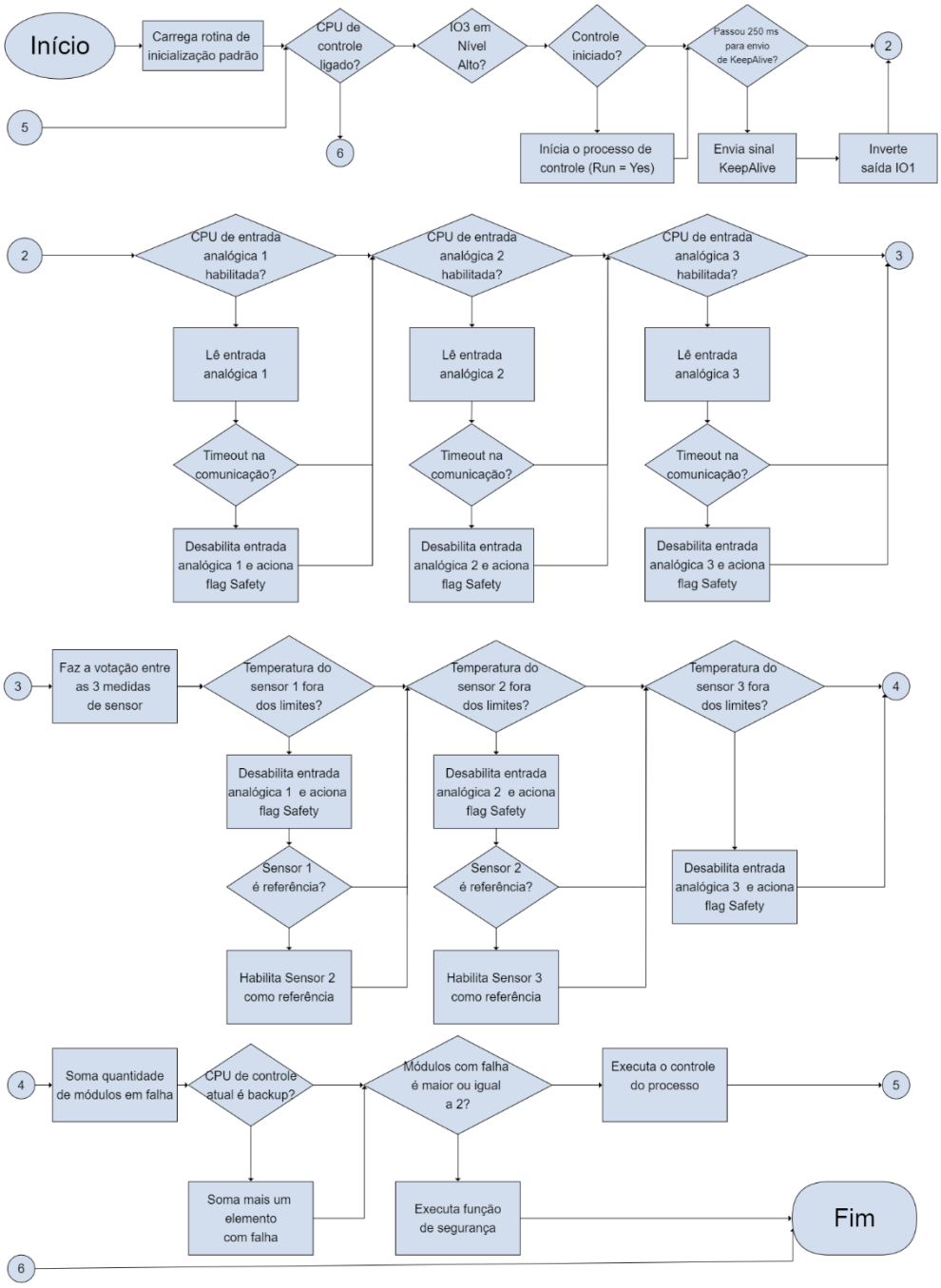
Fonte: Elaborada pelo autor (2022).

O próximo subcapítulo tratará de falar sobre as CPU's de controle do sistema.

3.6 CPU de Controle

A CPU de controle, cujo fluxograma de processo é mostrado na Figura 14, tem a função de receber os dados das entradas analógicas, fazer uma lógica de votação entre os valores para validar o sinal de sensor e então controlar o processo.

Figura 14 - Fluxograma de funcionamento da CPU de controle



Fonte: Elaborada pelo autor (2022).

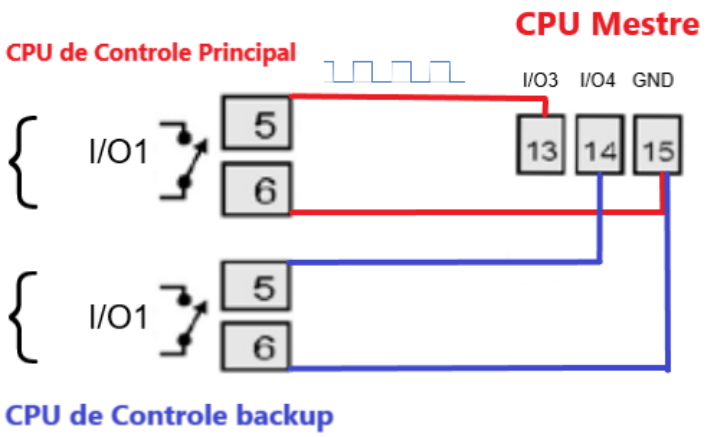
Assim, seu funcionamento é explicado por partes nos subcapitulos conseguintes.

3.6.1 Início de operação e *reset*

A CPU de controle começa a operar após ter sua entrada digital IO3 acionada em nível HIGH, fazendo com que o habilitador do controle nativo do N1200 (registrador *Run*) seja acionado. Imediatamente após isso, a CPU começa a atuar no processo de acordo com o PID configurado. Neste projeto, o PID foi calculado utilizando uma função nativa do controlador N1200: a auto-sintonia. Ela consiste em um cálculo automático dos componentes PID através de acionamentos do tipo *ON-OFF* e diferentes ciclos de trabalho, em inglês, *Duty Cycles*. Como nesse caso o processo utilizado era do tipo resistivo e com alta velocidade na transição da temperatura, utilizou-se um ciclo de 0.5 segundos no PWM.

Além da atuação no processo em si, a CPU de controle tem que fornecer um sinal de KEEP ALIVE para a CPU Mestre. Este sinal possui forma de uma onda quadrada e tem a finalidade de resetar o *Watchdog* da CPU Mestre de forma que se identifique rapidamente um problema de travamento ou *reset* do equipamento, e se o mesmo ocorrer, deve-se levar ao uso da CPU de controle *backup*. Foi configurado para que a CPU de controle principal envie um sinal de KEEP ALIVE a cada 250 ms em sua saída IO1 até a entrada IO3 da CPU mestre enquanto a CPU de controle de backup envia o sinal de KEEP ALIVE pela entrada IO4 da CPU Mestre. A Figura 15 mostra a conexão entre os pinos da CPU de controle principal, CPU de controle backup e CPU Mestre.

Figura 15 – Conexão de sinal de *Keep Alive* entre as CPU's de controle e a CPU Mestre.



Fonte: Elaborada pelo autor (2022).

O subcapítulo 3.6.2 vai falar sobre a leitura das entradas analógicas.

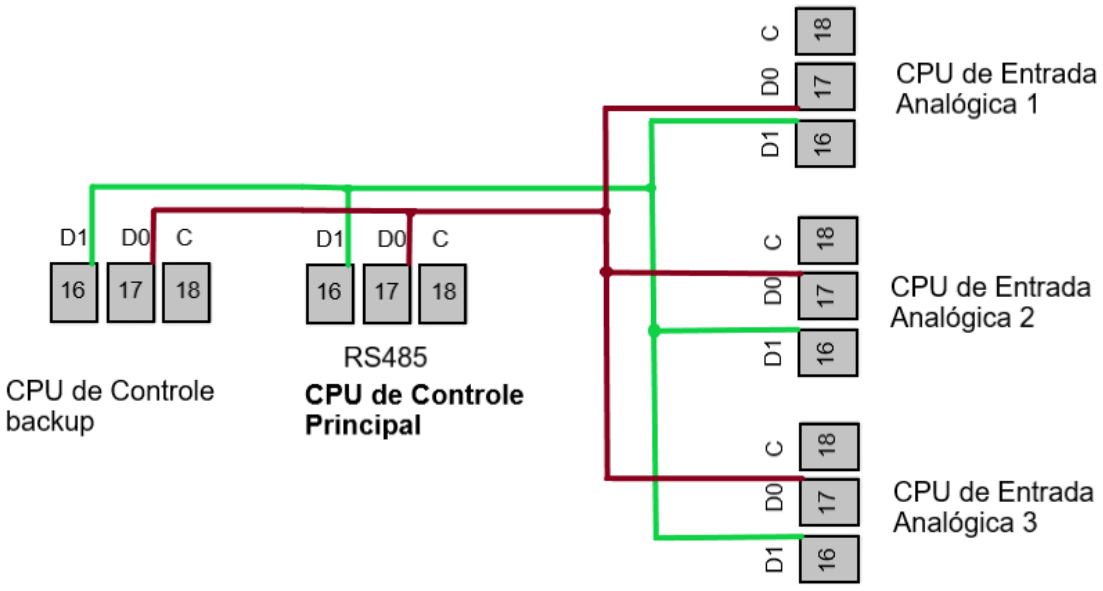
3.6.2 Leitura de Dados das Entradas Analógicas

A sequência da leitura dos dados de sensor das CPU's de entrada analógica segue a seguinte lógica:

a) verifica-se se a CPU de entrada analógica está habilitada para operação. Se não estiver, ela passa para a leitura da próxima entrada analógica.
b) faz-se a leitura do registrador serialmente via protocolo *Modbus* seguindo o pacote demonstrado, já mostrado no Quadro 1.
c) aguarda-se o pacote de resposta. Se ocorrer um *timeout* na recepção, é feito uma tentativa de no máximo três vezes. Se nenhuma das tentativas for bem-sucedida, a CPU de controle identifica esse módulo como falho e desabilita as suas próximas verificações.

No caso de dois ou mais módulos estiverem com falha na comunicação, a CPU de controle aciona a operação de modo seguro. A Figura 16 mostra as conexões seriais entre CPU's de controle e CPU's de entrada analógica.

Figura 16 – Conexão serial RS485 entre as CPU's de controle e a CPU's de entrada analógica



Fonte: Elaborada pelo autor (2022).

No subcapítulo 3.6.3, discorrer-se-á sobre como é feito o processamento dos dados coletados pelo controlador através das entradas analógicas.

3.6.3 Processamento de Dados dos Sensores

A CPU de controle sempre utiliza apenas um valor dentre as três medidas de sensores para fazer o controle do processo. Além disso, os sensores sempre medem a temperatura com uma tolerância uns dos outros devido tanto à sua construção, quanto à posição no local do processo, que mesmo próximos, nunca medirão exatamente o mesmo local, fazendo com que haja pequenas diferenças no resultado.

O processamento dos dados providos pelas CPU's de entrada analógica é feito de forma a comparar o valor entre elas, verificar se ultrapassa o limite pré-estabelecido e fazer a decisão em um sistema de votação 2oo3. Para isso, é feito um cálculo que tira a diferença absoluta entre as medidas 1-2, 1-3 e 2-3 como mostra a equação 1, sendo então comparado com o limite de 3 °C. Se for maior que 3 °C, o sistema deve desabilitar esse módulo, sinalizar internamente essa falha e se necessário, mudar a referência do sensor atual para o próximo sensor que não identificou o problema.

$$\begin{cases} \mathrm{PV}_{1-2} \leq |\mathrm{PV}_1 - \mathrm{PV}_2| \\ \mathrm{PV}_{1-3} \leq |\mathrm{PV}_1 - 3| \\ \mathrm{PV}_{2-2} \leq |\mathrm{PV}_2 - \mathrm{PV}_3| \end{cases} \tag{2}$$

3.6.4 Execução do processamento do modo seguro

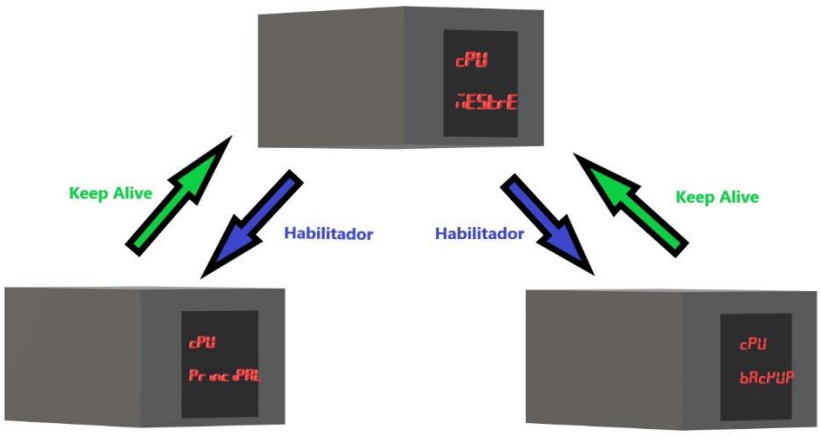
O modo seguro do Controlador *Safety* é acionado quando estiver com dois ou mais módulos de controle, CPU ou entrada analógica em falha. O comportamento do controlador, em caso de modo seguro, é decidido préviamente pelo usuário que configurou o sistema. Como se trata de um controlador PID, é possível escolher uma saída de potência entre 0 (desligado) até 100% (ligado a plena carga). Esse comportamento só é finalizado depois de uma intervenção do operador nos equipamentos.

O subcapítulo 3.7 abordará o último componente do Controlador *Safety*, a CPU mestre.

3.7 CPU Mestre

É denominado CPU Mestre o módulo que habilita e desabilita as CPU's de controle para atuarem no processo. Seu funcionamento consiste por padrão, habilitar a CPU de controle principal para fazer a atuação e controle do processo, ao mesmo tempo em que recebe um sinal pulsado desse mesmo controlador. Esse sinal pulsado faz o *reset* de um contador *Watchdog* de 500 ms e em caso de não receber esse sinal, a CPU Mestre atua imediatamente desabilitando a CPU de controle principal e habilitando a CPU. A Figura 17 mostra o vínculo entre a CPU mestre e CPU's de controle.

Figura 17 – Ligações e vínculo entre a CPU mestre e as CPU's de controle



Fonte: Elaborada pelo autor (2022).

O sistema incluindo as CPU's tanto de controle quanto de medição do sensor é mostrado na Fotografia 2.

Fotografia 2 – Controlador *Safety*

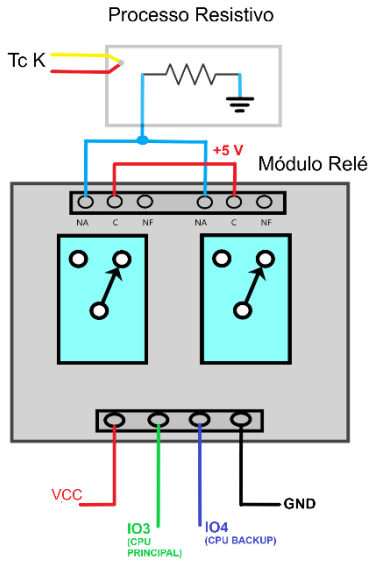
Fonte: Registrada pelo autor (2022).

A ordem das CPU's, seguindo da esquerda para a direita é: CPU Mestre, CPU de Controle 2, CPU de Controle 1 e CPU's de entrada analógica. O próximo subcapítulo discorrerá sobre o atuador do Controlador *Safety.*

3.8 Atuador

As saídas foram feitas de um modo simples, utilizando um módulo com dois relés, no qual cada um acionado de forma independente e os pinos Normalmente Aberto (NA) de ambos relés são ligados de forma paralela. Assim, tanto a CPU de controle principal quanto a de *backup* conseguem atuar no processo. A Figura 18 mostra as conexões do atuador.

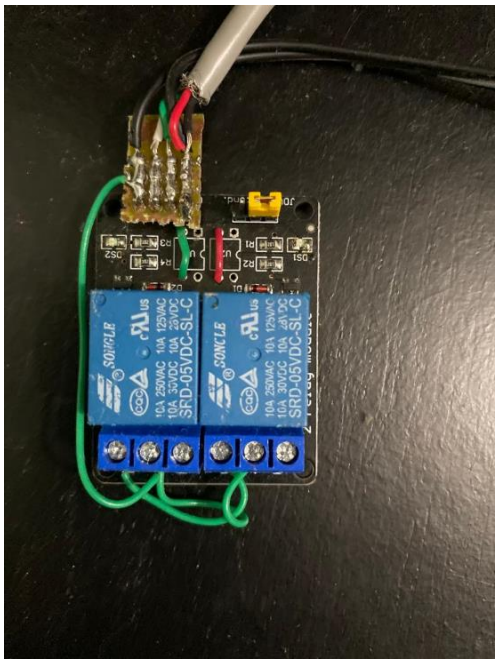
Figura 18 – Conexão entre pinos das CPU's de controle e o atuador do processo



Fonte: Elaborada pelo autor (2022).

Já o sistema atuador do Controlador *Safety* é mostrado na Fotografia 3, a seguir.

Fotografia 3 – Atuador do Controlador *Safety*



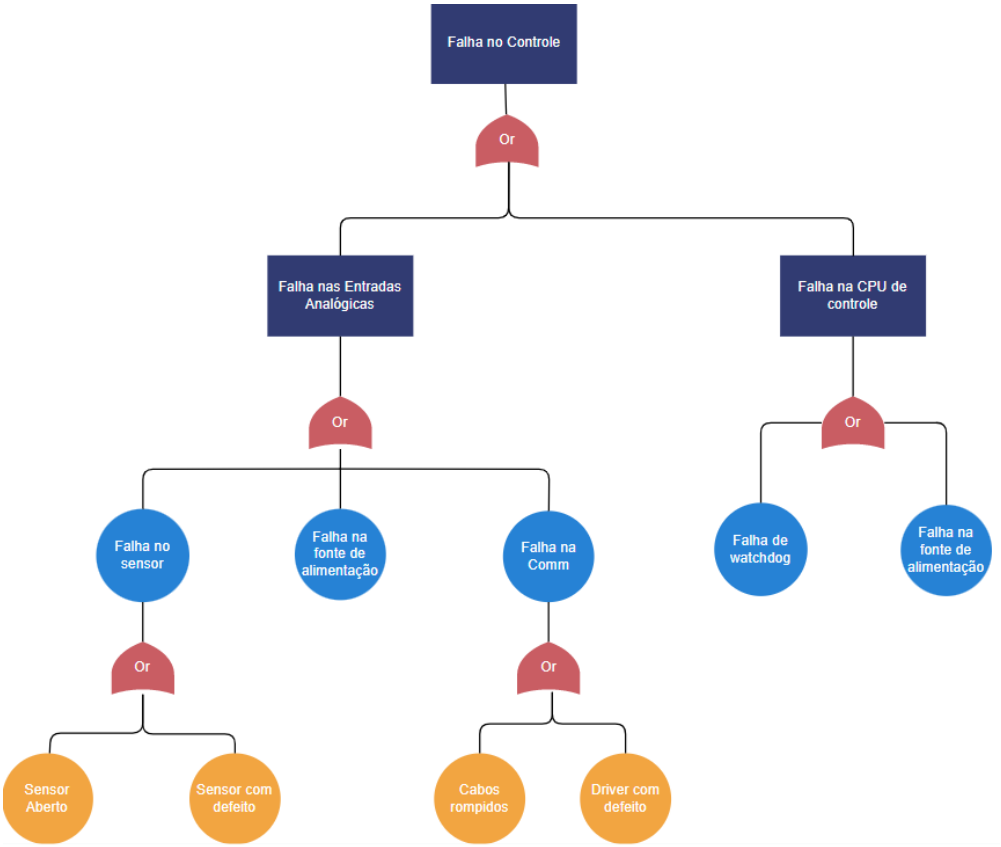
Fonte: Registrada pelo autor (2022).

No próximo subcapítulo, será abordadoa a árvore de falhas do sistema do Controlador *Safety*.

3.9 Visão Sistêmica Sob Uma Árvore de Análise de Falhas

Para facilitar a visualização e pensamento sistêmico sobre as causas de falha do *Controlador Safety*, se faz necessário o uso de uma Árvore de Análise de Falhas, em inglês *Fault Tree Analysis* (FTA). A FTA do controlador se baseia em uma quantidade finita de falhas, que puderam ser tratadas e implementadas no software baseado na limitação do *hardware* e do escopo do projeto. A Figura 19 mostra a FTA do Controlador Safety.

Figura 19 – Árvore de Análise de Falhas do Controlador *Safety*



Fonte: Elaborada pelo autor (2022).

Assim, os defeitos que serão cobertos nesse trabalho serão: sensor com defeito, falha na alimentação, cabos rompidos e falha de *watchdog*.

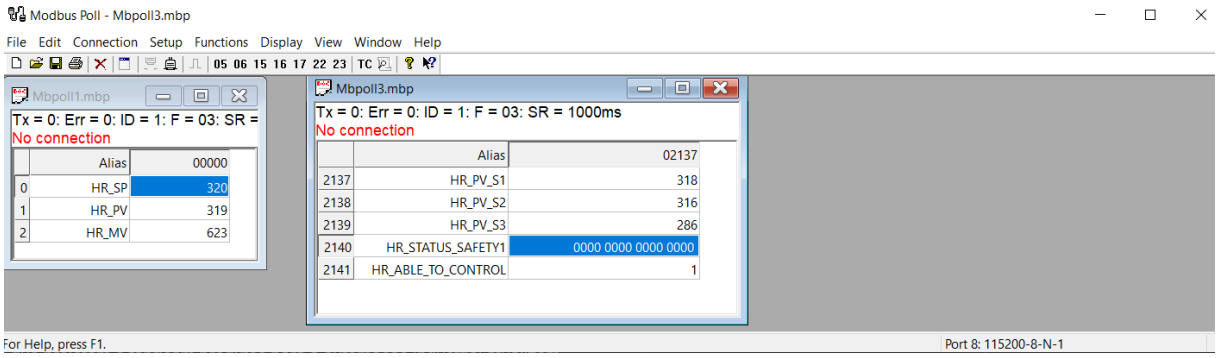
4 ANÁLISE DOS RESULTADOS

O objetivo de controlar um processo resistivo de forma segura foi atingido com sucesso. Portanto, no próximo subcapítulo, serão detalhados os testes executados e a resposta do sistema para os estímulos aplicado.

4.1 Testes Analisando a Função Segura do Controlador

Os testes foram feitos através da leitura da porta USB da CPU de controle utilizando o software *Modbus Poll*. Leram-se os registradores de temperatura das CPU's de entradas analógicas e lido o registrador da PV principal do controlador e feito um gráfico dos resultados ao longo do tempo. A Figura 20 mostra o software utilizado para a leitura serial dos registradores do controlador.

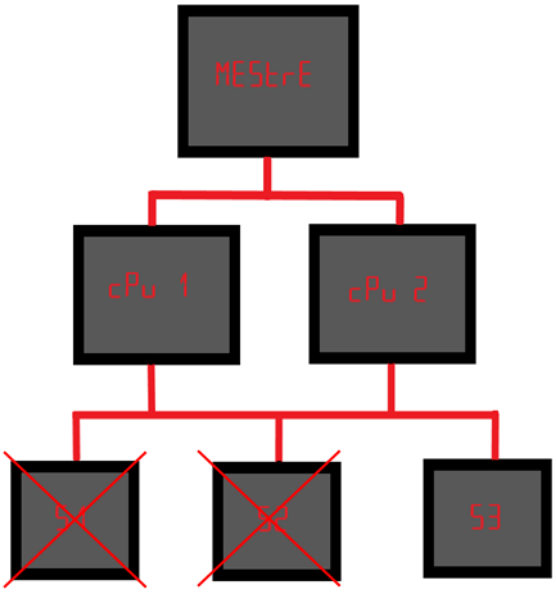
Figura 20 – Software *Modbus Poll*



Fonte: Elaborada pelo autor (2022).

O primeiro teste teve como objetivo verificar a atuação da função segura do controlador após dois sensores falharem. Inicialmente, foi colocado o equipamento para atuar no processo controlando-o a 50°C e com uma função segura que desliga o processo. A figura 21 mostra a representação dos defeitos no sensor 1 e no sensor 2.

Figura 21 – Sistema com dois sensores em falha

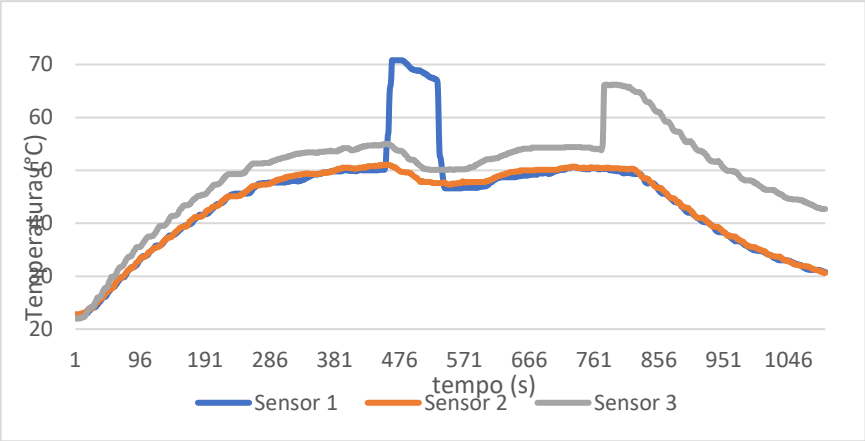


Fonte: Elaborada pelo autor (2022).

Observa-se no gráfico 1, que o processo começa o controle em 20°C e em aproximadamente 380 segundos, o processo estabiliza em todos os 3 sensores. Nesse tempo, é aplicado uma falha de *Overshoot* no sensor 1, fazendo com que o sistema de votação capture essa falha e descarte o sensor 1 do controle do processo. Verifica-se também que a temperatura cai pouco antes de voltar ao controle estável de 50°C. Isso é devido ao fato de o PID ter levado esse *Overshoot* em consideração no cálculo e feito um controle adequado a esse erro.

No instante próximo dos 760 segundos, é aplicado um novo *Overshoot* no sensor 3, fazendo com que o controlador entre em um estado seguro desligando o processo.

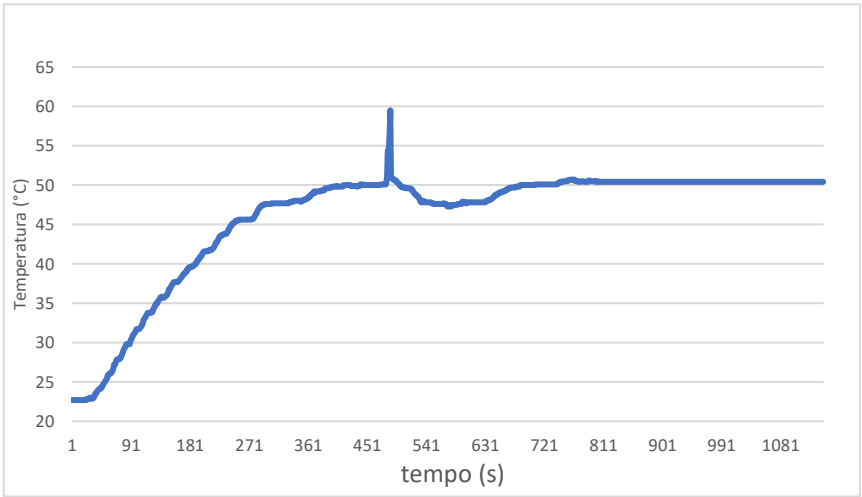
Gráfico 1 – Medidas dos módulos de entradas analógicas no primeiro teste



Fonte: Elaborado pelo autor (2022).

Já no gráfico 2, é possível observar o controle do processo do ponto de vista do controlador. Para fazer esse controle, ele assume apenas a PV de um sensor (nesse caso, o sensor 1), e ao observar um pico de temperatura, ele trocar sua referência para o sensor 2 e continua atuando no processo até ocorrer a segunda falha, onde as saídas são desabilitadas mesmo que no Gráfico 2 ainda pareça estar estável.

Gráfico 2 – Temperatura vista pelo controlador PID no primeiro teste

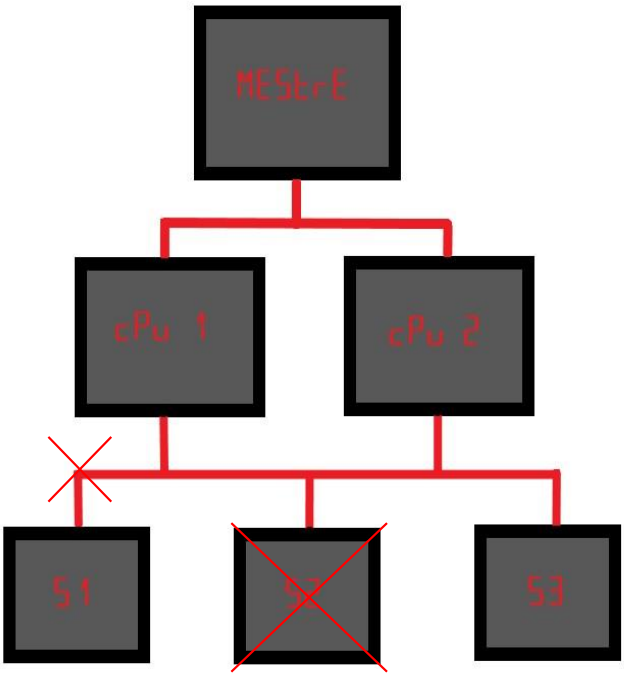


Fonte: Elaborado pelo autor (2022).

O segundo teste foi para verificar a atuação da função segura do controlador após um sensor ter sua comunicação interrompida e o outro ter um *Overshoot* em sua leitura. O controlador foi novamente colocado para atuar no processo controlando-o a

50 °C e com uma função segura que desliga o processo. A figura 22 mostra a representação dos defeitos na linha de comunicação do módulo de sensor 1 e no módulo de sensor 2.

Figura 22 – Sistema com linha de comunicação e um sensor em falha

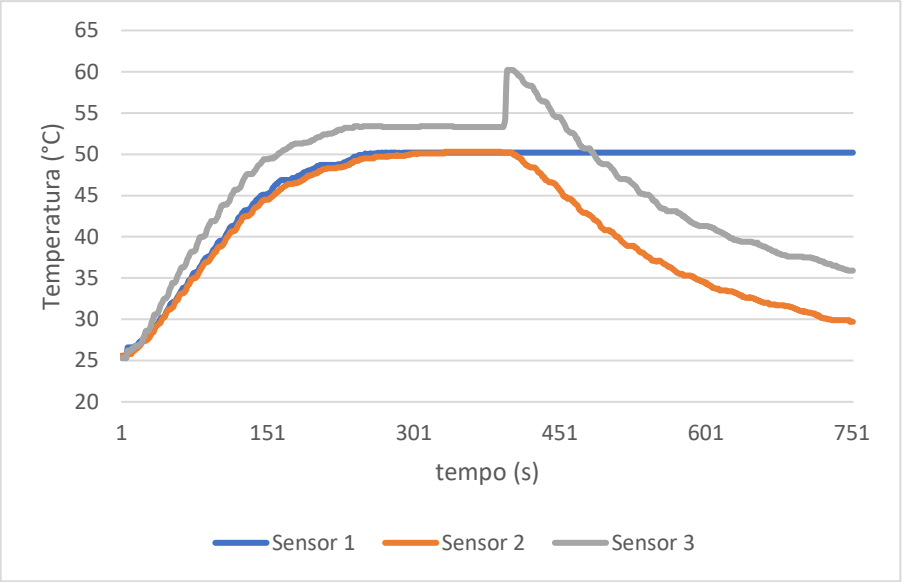


Fonte: Elaborada pelo autor (2022).

O Gráfico 3 mostra que o processo começa o controle em 25 °C e em aproximadamente 300 segundos, o processo estabiliza em todos os 3 sensores. Nesse tempo, é aplicado uma falha na comunicação do sensor 1, fazendo com que o sistema capture essa falha e descarte o sensor 1 do controle do processo. Como não há uma mudança na PV, pois não ocorreu um *Overshoot*, e sim uma troca de sensores já estáveis, a temperatura no processo permanece estável.

No instante próximo dos 400 segundos, é aplicado novamente um *Overshoot* no sensor 3, fazendo com que o controlador entre em seu estado seguro e desligando o processo.

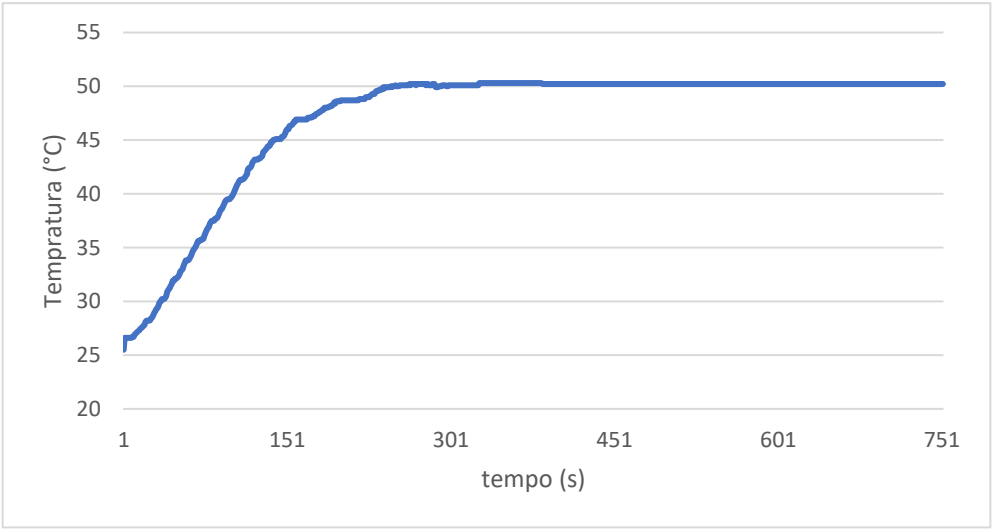
Gráfico 3 – Medidas dos módulos de entradas analógicas no segundo teste



Fonte: Elaborado pelo autor (2022).

É possível observar no Gráfico 4 o mesmo comportamento estável do controlador em relação ao processo. A grande diferença nesse teste comparado ao anterior, se deve ao fato de não haver mudança na temperatura na PV de referência do controlador, fazendo com que haja apenas uma troca de sensor que está estável e na mesma altura.

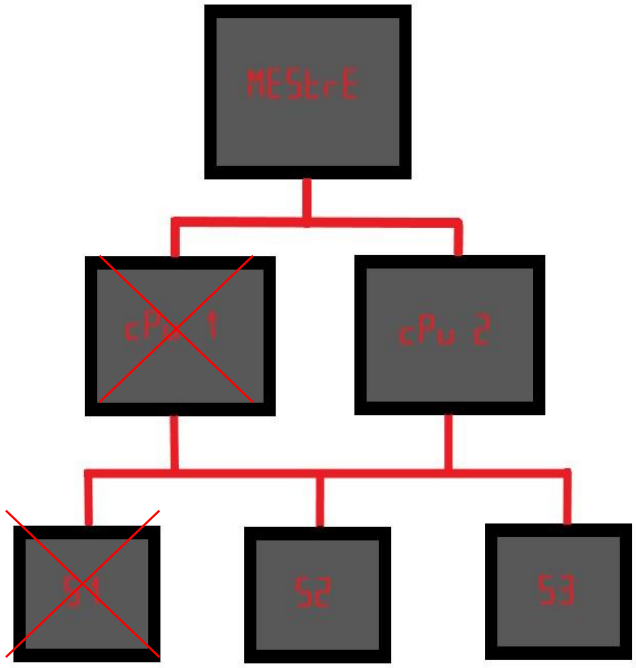
Gráfico 4 – Temperatura vista pelo controlador PID no segundo teste



Fonte: Elaborado pelo autor (2022).

O último teste teve o intuito de verificar a atuação da função segura do controlador após uma CPU entrar em *Watchdog*, interrompendo sua atuação e após haver um *Overshoot* em um dos sensores. Novamente o controlador atuou no controle do processo em 50 °C. A figura 23 mostra a representação dos defeitos na CPU de controle principal e no módulo de sensor 2.

Figura 23 – Sistema com CPU de controle e sensor em falha

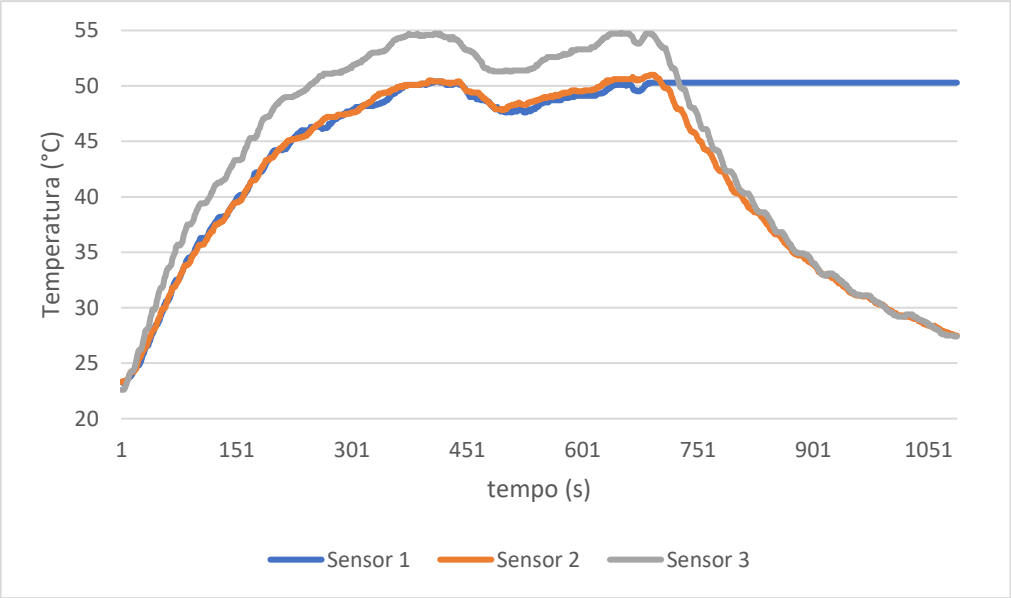


Fonte: Elaborada pelo autor (2022).

Observa-se no Gráfico 5 que o processo começa o controle em aproximadamente 25 °C. Próximo de 300 °C, o processo estabiliza em todos os três sensores. Após isso, é aplicada uma falha na alimentação da CPU 1, fazendo com que a CPU Mestre não identifique o pulso para *resetar* o sistema de *Watchdog*. Isso faz com que ele desabilite a CPU 1 de controle e habilite a CPU 2 de controle. Novamente há uma pequena queda na temperatura devido ao cálculo do PID da CPU 2 iniciar zerado.

No instante próximo dos 750 segundos, é aplicada outra falha de *Overshoot* no sensor 3, fazendo com que a CPU 2 entre em seu estado seguro e desligando o processo.

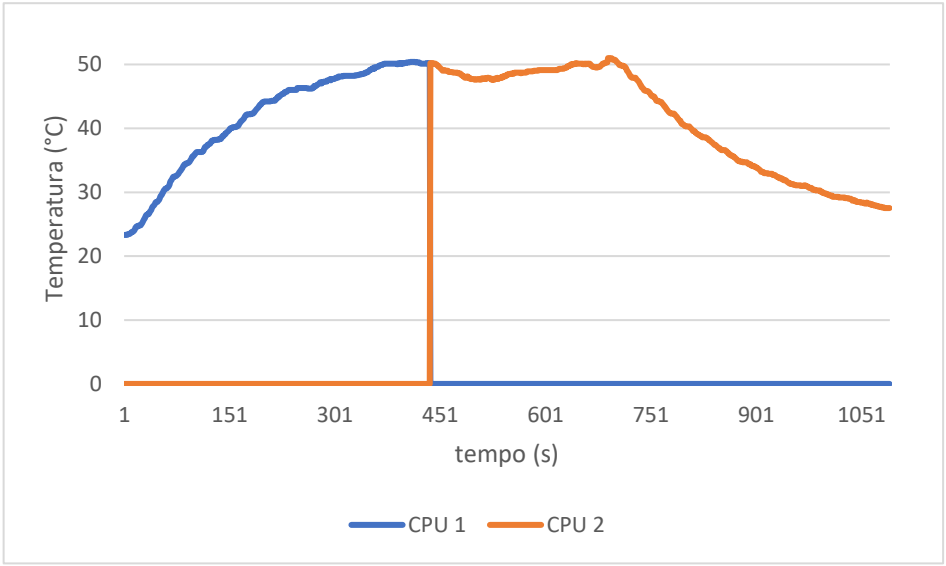
Gráfico 5 – Temperatura vista pelo controlador PID no terceiro teste



Fonte: Elaborado pelo autor (2022).

É possível observar no Gráfico 6 a atuação de ambas *CPU's* e o tempo em que elas começam a sua operação. No tempo próximo a 450 segundos, a CPU 1 sai de operação e imediatamente a CPU 2 inicia a operação, levando mais algum tempo para o cálculo do PID chegar a uma atuação estável do processo.

Gráfico 6 – Temperatura vista pelas duas CPU's do controlador no terceiro teste



Fonte: Elaborado pelo autor (2022).

Em todos os testes, executou-se com sucesso a função segura do Controlador *Safety*, atingindo plenamente o objetivo de elaborar um protótipo de um controlador de temperatura PID com características de segurança funcional.

5 CONCLUSÃO

Atualmente, está sendo valorizada cada vez mais segurança em controle de processos, a fim de se evitar prejuízos e desastres industriais. Logo, se faz necessário que as empresas que projetam e fabricam produtos para a automação industrial atualizem seu portfólio com produtos que tenham certificação em segurança funcional para atender às necessidades do mercado. Em razão disso, este trabalho, em conjunto com a Novus Produtos Eletrônicos, se propôs a fazer o protótipo de um controlador de temperatura PID com arquitetura 2oo3 capaz de controlar um processo de forma segura e com as mesmas características do controlador já consolidado no mercado.

Houve algumas limitações no planejamento e execução do projeto tanto no *hardware* do projeto quanto no *software*. Em termos de hardware, o escopo foi limitado a medição (entrada analógica) e controle, pois são pontos críticos em um processo. O atuador (saída digital e/ou analógica) não deixa de ser um ponto crítico, mas para essa primeira prova de conceito dois elementos importantes já seriam o suficiente para o objetivo do trabalho. Já no software, foi testado apenas o controle de processo, sendo deixado de lado o teste de funcionalidades do controlador N1200, como alarmes, programa de rampas e patamares e temporizadores. Para a execução dos testes no protótipo, foi escolhido três tipos de falhas: falha no sensor, falha nos cabos da comunicação dos módulos de entrada analógica e falha no *Watchdog* de uma das CPU's de controle. Esses tipos de falha foram selecionados por sua facilidade de implementação, pois todas eram causadas de modo físico.

O resultado obtido pelo trabalho foi um controlador PID com arquitetura 2oo3 que consegue continuar atuando no processo caso uma CPU de controle ou entrada analógica estiver em uma situação de falha e executa sua função segura quando um segundo elemento entra em falha. Considerando, então, a metodologia proposta e os resultados alcançados, considera-se que os objetivos desse trabalho foram atendidos, sendo eles comprovados pelos testes executados. A utilização de redundâncias no projeto do Controlador *Safety* mostrou resultados satisfatórios tanto na atuação do processo quanto no aumento da segurança do processo em caso de duas ou mais falhas.

Por fim, como sugestão para trabalhos futuros, estão os seguintes objetivos: projetar o software dos módulos redundantes de saída digital e analógica; projetar o

hardware seguindo as normas de segurança funcional; e pesquisa e implementação do protocolo aberto *OpenSafety,* que é um padrão aberto que pode trafegar sobre qualquer protocolo, incluindo *Modbus* usando o conceito de *black channel*.

REFERÊNCIAS

ALPI, Lucas. **Controle PID: rompendo a barreira do tempo**. Disponível em: <https://www.novus.com.br/site/default.asp?Idioma=55&TroncoID=053663&SecaoID=0&SubsecaoID=0&Template=../artigosnoticias/user_exibir.asp&ID=736280>. Acesso em: 16 abr. 2022.

BALEN ,T. R. ; Lubaszewski , M., **"Teste e Projeto Visando a Testabilidade de Circuitos e Sistemas Integrados"**, Julho, 2014. [Online]. Disponível em: <https://www.researchgate.net/publication/263580297_Teste_e_Projeto_Visando_a_Testabilidade_de_Circuitos_e_Sistemas_Integrados>. Acesso em: 02 nov. 2021.

DILLENBURG, Marcos R. **Indo Além do Controle P.I.D**. Disponível em: <https://www.novus.com.br/download /Arquivos/indoalemdocontrolepid.pdf>.Acesso em: 16 abr. 2022.

FRANCHI, Claiton Moro. **Controle de processos industriais: princípios e aplicações**. 1. ed. São Paulo: Érica, 2011. 1 recurso online ISBN 9788536518282.

IEC (International Electrotechnical Commission). **IEC 61508 all parts: Functional safety of electrical/electronic/programmable electronic safety-related systems**. Edition 2.0. 2010.

J. DE MORAES et al., "**Architecture of an industrial analog input designed to meet safety requirements**," 2018 IEEE 19th Latin-American Test Symposium (LATS), 2018, pp. 1-4, doi: 10.1109/LATW.2018.8349673.

JULSEREEWONG, A. Thepmanee, T. **Design and Implementation of Functional Safety for Repairable Systems**. 57th Annual Conference of the Society of Instrument and Control Engineers of Japan (SICE). Nara, Japan. Pp 1638-1643.2018.

MEANY, T. **Functional Safety and Industrie 4.0**. 28th Irish Signals and Systems Conference (ISSC). Killarney, Ireland. Pp 1-7. 2017.

NISE, Norman S. **Engenharia de sistemas de controle**. 7. ed. Rio de Janeiro: LTC, 2017. Recurso online ISBN 9788521634379.

Novus Produtos Eletrônicos. **Manual de Operação N1200**. Canoas, RS. 2022. Disponível em: <https://www.novus.com.br/downloads/Arquivos/v20x_manual_n1200_port.pdf>. Acesso em: 01 dez. 2021.

TORRES, E. S. Sriramula, S. Celeita,D. Ramos, G. **Reliability Model and Sensitivity Analysis for Electrical/Electronic/Programmable Electronic Safety - Related Systems**. **IEEE Transactions on Industry Applications.** Volume: 56, Issue: 4, July-Aug. 2020. Pp 3422 - 3430. 2020.