UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
ESCOLA DE ENGENHARIA
PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA ELÉTRICA

JULIANO DE LIMA

METODOLOGIA PARA UTILIZAÇÃO DE CONTROLADORES PROGRAMÁVEIS STANDARD EM SISTEMAS DE SEGURANÇA

Porto Alegre
2020

JULIANO DE LIMA

METODOLOGIA PARA UTILIZAÇÃO DE CONTROLADORES PROGRAMÁVEIS STANDARD EM SISTEMAS DE SEGURANÇA

Dissertação de mestrado apresentada ao Programa de Pós-Graduação em Engenharia Elétrica, da Universidade Federal do Rio Grande do Sul, como parte dos requisitos para a obtenção do título de Mestre em Engenharia Elétrica.

Área de concentração: Controle e Automação – Sistemas de Automação.

ORIENTADOR: Ivan Muller

Porto Alegre

2020

JULIANO DE LIMA

METODOLOGIA PARA UTILIZAÇÃO DE CONTROLADORES PROGRAMÁVEIS STANDARD EM SISTEMAS DE SEGURANÇA

Esta dissertação foi julgada adequada para a obtenção do título de Mestre em Engenharia Elétrica e aprovada em sua forma final pelo Orientador e pela Banca Examinadora.

Orientador: _____

Prof. Dr. Ivan Muller, UFRGS

Doutor pela UFRGS- Porto Alegre, Brasil

Banca Examinadora:

Prof. Dr. Diego Eckard, UFRGS

Doutor pela Universidade Federal do Rio Grande do Sul – Porto Alegre, Brasil

Prof. Dr. Edison Pignaton de Freitas, UFRGS

Doutor pela Universidade Federal do Rio Grande do Sul – Porto Alegre, Brasil

Prof. Dr. Marcelo Götz, UFRGS

Doutor pela Universität Paderborn – Paderborn, Alemanha

Coordenador do PPGEE: _____

Prof. Dr. João Manoel Gomes da Silva Junior

Porto Alegre, Março de 2020.

DEDICATÓRIA

Dedico este trabalho a todos que de certa forma contribuíram para que eu conseguisse concluir este grande projeto, em especial à Universidade Federal do Rio grande do Sul que me recebeu de portas abertas, aos professores que muito me ensinaram neste período, aos colegas e amigos que fiz nesta jornada e aos familiares que me deram todo apoio. Muito obrigado.

AGRADECIMENTOS

Ao Programa de Pós-Graduação em Engenharia Elétrica, PPGEE, pela oportunidade de realização de trabalhos em minha área de pesquisa.

Aos professores do PPGEE pelos ensinamentos e pela oportunidade de ingresso ao programa.

Aos colegas de aula pelo auxílio nas tarefas desenvolvidas durante o curso e apoio na revisão deste trabalho.

Ao professor Ivan pela paciência, persistência e sabedoria na sua condução dos seus orientandos.

À minha esposa pela colaboração e disposição para que eu conseguisse estudar.

Aos meus filhos pelo estímulo, energia e inspiração para seguir no caminho.

RESUMO

O uso de controladores programáveis dedicados à segurança de plantas industriais desempenha um papel fundamental em um Sistema Instrumentado de Segurança – SIS. Estes equipamentos são certificados de acordo com o Nível de Integridade de Segurança - SIL, classificados a partir de quatro níveis, onde as principais métricas para determinação destes níveis são: disponibilidade, probabilidade de falha na demanda e fator de redução de risco. O custo de uma plataforma certificada para Sistemas de segurança é muito elevado podendo inviabilizar um projeto onde a certificação pode não ser a exigência principal. Diante deste fato, este trabalho apresenta um estudo para utilização de controladores programáveis standard não certificados, para que sejam empregados em funções de segurança de processos industriais. Foram propostos estudos comparativos das principais métricas de confiabilidades entre os controladores standard e de segurança, onde cálculos de tempo médio entre falhas – MTBF, disponibilidade, probabilidade de falha na demanda e fração de falha segura são apresentados. De acordo com os dados apresentados por fabricantes de controladores standard, pode-se atingir métricas de segurança SIL a partir de aplicação de arranjos de arquiteturas e cálculos das métricas supracitadas. Conforme apresentado neste texto, uma plataforma de controlador standard formada por fonte, CPU e módulos de comunicação em um chassi e módulos de entrada e saída em um outro chassi montados em um arranjo de arquitetura 1oo1 resultou em métricas SIL 2 para intervalos de teste de cinco anos. A mesma plataforma formada por um sistema redundante do tipo *Hot-Standby* formado por fonte, CPU e módulos de comunicação montados em dois conjuntos distintos e módulos de I/O em arranjo 1oo2 resultaram métricas SIL 2 para intervalos de testes de vinte anos, intervalo médio utilizado para certificação SIL.

Palavras-chave: *Safety Integrity Level*, Disponibilidade, Probabilidade de Falhas, Segurança Funcional, Arquiteturas de alta disponibilidade, Tolerância a falhas.

ABSTRACT

The use of programmable controllers dedicated to the safety of industrial plants plays a fundamental role in the Instrumented Safety System - SIS. This equipment is certified according to the Safety Integrity Level - SIL, classified from four levels, where the main measures to measure the levels are: availability, probability of failure in demand and risk reduction factor. The cost of a certified platform for Security Systems is very high, making unviable a project where certification may not be the main principle. Thus, this study proposes use a standard programmable controller where certifications are not required, it can be used in safety functions of industrial processes. Comparative studies of the main reliability metrics between standard and safety controllers were presented, where calculations of mean time between failures - MTBF, availability, probability of failure in demand and fraction of safe failure are indicated. According to the data presented by the manufacturers of standard controllers, SIL security metrics can be achieved through the application of architectural arrangements and calculations of the metrics already said. As defined in this text, a standard controller platform consisting in: power supply, CPU, communication and input and output modules in another chassis mounted in a 1oo1 architecture arrangement resulted in SIL 2 metrics for five-year tests. The same platform formed by a redundant system (Hot-Standby) type formed by power supply, CPU, communication modules and I / O modules composed in two different sets 1oo2 arrangement resulted in SIL 2 measurements for test intervals of twenty years, interval medium used for SIL certification

Keywords: Safety Integrity Level, Availability, Probability of Failure, Functional Safety, High Availability Architectures, Fault Tolerance.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS

ATEX Directive Appareils Destinés à Être Utilisés en Atmosphères Explosives

CE Conformité Européenne

CPU Central Processing Unit

DC Diagnostic Coverage

DNV Det Nork Veritas

EAC: Eurasian Union Conformity

EPA Environmental Protection Agency

E/E/EP Electrical/Electronic/Programmable Electronic

ERP Enterprise Resource Planning

IEC International Electrotechnical Commission

IED Intelligent Electronic Device

HAZOP Hazard and Operability Study

HSE Health and Safety Executive

LOPA Layer of Protection Analysis

MES Manufacturing Execution System

MooN M out of N channel architecture

MooND M out of N channel architecture with Diagnostic

MTBF Mean Time Between Failures

MTTF Mean Time to Fail

MRT Mean Repair Time

MTTFS Mean Time to Fail Safe

MTTR Mean Time to Repair

OSHA Ocupation Safety and Health Administration

PE Programmable Electronic

PFD Probability of Dangerous Failure on Demand

PFD_{avg} Average Probability of dangerous Failure on Demand

PFH Average frequency of dangerous failure [h-1]

PTI Proof Test Interval

PLC Programmable Logic Controller

RBD: Reliability Block Diagram

RRF Risk Reduction Factor

SCADA Supervisory Control and Data Acquisition

SDIM Safety Digital Input Monitored

SDOM Safety Digital Output Monitored

SIF Safety Instrumented Function

SIL Safety Integrity Level

SIS Safety Instrumented System

SMCU Safety Microcontroller Unit

S-PLC Safety PLC

S-CPU Safety CPU

SRS Security Requirements specifications

SRCS Safety Related Control Systems

SFF Safe Failure Fraction

TCE Channel Equivalent Down Time

TGE System Equivalent Down Time

TMR Triple Modular Redundancy

UL Underwriters Laboratories

LISTA DE SÍMBOLOS

β ou CCF Common Cause Failure Rate

β_d ou CCF_d Common Cause Failure Rate, Dangerous

λ Failure Rate

λ_s Rate of Safe Failures

λ_d Rate of Dangerous Failures

λ_{dd} Dangerous, Detected Failure Rate

λ_{du} Dangerous, Undetected Failure Rate

λ_{su} Safe, Undetected Failure Rate

λ_{sd} Safe, Detected Failure Rate

μ taxa de reparos

D disponibilidade

LISTA DE NORMAS

EN/ISO 13849 Safety of Machinery – Safety-related Parts of Control Systems

EN 50126 Railway Applications – The Specification and Demostration of Reliability, Availability Maintainability and Safety (RAMS)

EN 50128 Railway Applications - Communication, Signalling and Processing systems - Software for Railway Control and Protection Systems

EN 50129 Railway applications – Communication, Signalling and Processing Systems – Safety Related Electronic Systems for Signalling

EN 54402 Electrical Apparatus for the Detection and Measurement of Combustible or Toxic Gases or Vapours or of Oxygen - Requirements on the Functional Safety of Gas Detection Systems

EN 50271 Electrical Apparatus for the Detection and Measurement of Combustible Gases, Toxic Gases or Oxygen - Requirements and Tests for Apparatus Using Software and/or Digital Technologies

IEC 61508 Functional Safety of electrical/Electronic/Programmable Electronic Safety-Raletade Systems

IEC 61511 Functional Safety – Safety Instrumented Systems for the Process Industry Sector

IEC 62061 Safety of Machinery - Functional Safety of Electrical, Electronic and Programmable Electronic Control Systems

IEC 61513 Nuclear power plants - Instrumentation and control important to safety

IEC 61800 Adjustable speed electrical power drive systems

IEC-ACOS IEC Advisory Committee on Safety

EN 60079-X Electrical Apparatus for Explosive Gas Atmospheres

MIL-HDBK-217F Military Handbook, Reliability Prediction of Electronic Equipment

N 2595 Critérios de Projeto, Operação e Manutenção de Sistemas Instrumentados de Segurança em Unidades Industriais

SUMÁRIO

1 INTRODUÇÃO

Segurança em processos industriais tem se tornado um requisito cada vez mais importante no cenário mundial, uma vez que acidentes graves em usinas nucleares, plantas petroquímicas, sistemas de transporte e armazenamento de combustíveis, por exemplo, causam grande impacto econômico, ambiental e pessoal. Estas causas têm se tornado intoleráveis aos órgãos competentes de cada país.

Normas específicas para aplicação e projeto de equipamentos dedicados a este fim foram desenvolvidas e têm sido aperfeiçoadas ao longo do tempo, como exemplo a IEC 61511, *Safety Instrumented System* - SIS e a IEC 61508 – *Safety Integrity Level* - SIL. A primeira norma citada descreve aplicações de sistemas de segurança voltados para indústria de processos e a segunda, conceitos e diretivas para desenvolvimento de equipamentos dedicados para aplicação em sistemas de segurança.

Controladores programáveis para sistemas de segurança, ou simplesmente *Electronic Programmable* (EP) conforme IEC-61508, são produtos desenvolvidos para executar lógicas de segurança de processos industriais, e são aplicados em medições de temperatura, nível, pressão, vazão, viscosidade entre outras variáveis de processos industriais, além da detecção de alarmes e comandos de *trip* (desligamento) dos processos em geral.

O ciclo de vida de projeto de um EP SIL consiste numa série de etapas e de uma documentação detalhada, devendo ser validada por algum órgão certificador, onde toda documentação deve passar por criteriosos processos de revisão a fim de garantir o sucesso da certificação do produto, tornando o processo lento e muito caro.

Por outro lado, controladores programáveis industriais não certificados, conhecidos na indústria como controladores de mercado ou controladores standard conforme designados neste trabalho, são equipamentos utilizados para controle do processo de máquinas e de plantas industriais, não sendo empregados em processos de segurança, não se abstendo de outras

certificações e ou diretivas de qualidade e segurança, tais como, CE, UL, DNV, EAC entre outras. Os EPs standard são compostos de fontes, CPU, módulos de entrada e saída digitais e analógicas, conforme padronização da norma IEC 61131.

Em aplicações de missão crítica com controladores standard, arranjos especiais podem ser aplicados com o objetivo de atendimento dos requisitos das normas de segurança funcionais.

Conforme introduzido anteriormente, custo de uma plataforma certificada para sistemas de segurança é muito elevado podendo inviabilizar um projeto onde a certificação pode não ser a exigência principal. As normas referentes à segurança funcional são muito extensas e complexas, onde um projeto de um dispositivo certificado SIL pode levar muito tempo para ser concluído.

Diante destes fatos, este trabalho apresenta o estudo e o desenvolvimento de uma metodologia de projeto para utilização de controladores programáveis standard não certificados para que sejam empregados em funções de segurança de processos industriais, ou simplesmente utilizadas as mesmas técnicas para aplicações em processos de missão crítica. Esta metodologia resulta em arranjos e cálculos dos componentes a fim de atingir as mesmas métricas aplicadas nos equipamentos certificados. Este estudo pode ser aplicado em qualquer controlador standard de mercado que possua flexibilidade de arranjos de arquiteturas podendo popularizar a metodologia com objetivo de aumento de segurança funcional em processos críticos onde a certificação não foi exigida. A adoção desta metodologia pode contribuir para aumento de confiabilidade de máquinas e processos de automação mitigando o número de acidentes ocasionados por possíveis falhas de controladores programáveis e sistemas de instrumentação.

Como forma de validação desta dissertação, propõe-se um comparativo de atendimento às principais métricas de segurança entre controladores SIL e controladores programáveis standard, tanto ao atendimento de seus principais requisitos de segurança, quanto ao desempenho e confiabilidade necessária.

Através da forma de cálculo de redundância MooN e inclusão de taxas de falhas e cálculos de probabilidade de falha na demanda, um modelo de controlador standard de um fabricante brasileiro atingiu métricas de um controlador SIL2 para intervalo de testes de vinte anos. Para alcançar este objetivo, foi projetado um arranjo de arquitetura redundante nos chassis de fontes, CPUs e placas de comunicação e arquitetura 1oo2 para os módulos de aquisição de dados e saídas do sistema. Este trabalho está dividido da seguinte forma: No capítulo 1 é apresentada uma introdução do tema. No capítulo 2 é apresentada a fundamentação teórica, no capítulo 3 os trabalhos relacionados ao objetivo da dissertação. No capítulo 4 é descrita a metodologia adotada apresentando as principais formas de cálculo das métricas envolvidas em um projeto de EP SIL. No capítulo 5 é apresentado o estudo de caso e os resultados obtidos. Por fim o capítulo 6 apresenta a conclusão do trabalho e possíveis trabalhos futuros.

Este trabalho se diferencia dos demais por aproximar a metodologia de projeto dos controladores standard com os controladores de segurança comparando-os através de MTBF, disponibilidade, probabilidade de falhas, fator de redução de risco, fração de falhas seguras entre outras métricas não menos importantes. O trabalho propõe a aplicação dos controladores standard em funções de segurança onde certificações SIL não são exigidas, além disso a utilização de técnicas estudadas para emprego em sistemas de missão crítica com intuito de mitigação de possíveis falhas e melhoria de performance de segurança.

2 FUNDAMENTAÇÃO TEÓRICA

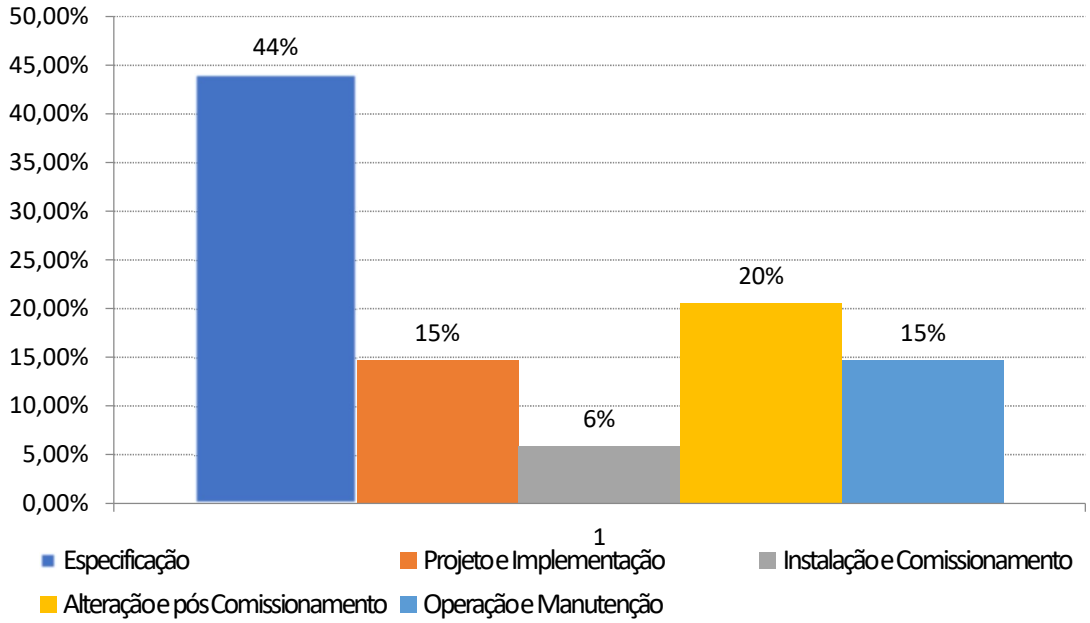
Inicialmente, sistemas de proteção de processos industriais eram projetados utilizando lógicas pneumáticas ou relés elétricos, uma vez que estes componentes tendem a falhar no modo desenergizado. À medida que os processos se tornaram mais complexos, lógicas fixas começaram a perder espaço devido à grande dimensão e retrabalho nas instalações, então deu-se início à utilização de eletrônica de estado sólido. Atualmente utiliza-se lógica programável inclusive nos sistemas de proteção, devido ao grande esforço dos pesquisadores do setor para tornar estes produtos confiáveis, de acordo com as normas vigentes.

Tal evolução forçou a indústria e os órgãos competentes para que desenvolvessem regras para aplicação de sistemas voltados à segurança de processos, como a IEC-ACOS (IEC *Advisory Committee on Safety)*, comitê especializado em segurança. A grande preocupação deveu-se aos problemas relacionados a acidentes em unidades industriais, provenientes de erros em todas as etapas de projeto, implantação e manutenção destas unidades.

Conforme entidades como EPA (*Environmental Protection Agency*), OSHA (*Ocupation Safety and Health Administration*) e HSE (*Health and Safety Executive*) as principais causas de falhas em sistemas de automação estão relacionadas a erros de especificações de produtos e projetos, seguido por problemas relacionados com alterações após comissionamento, projeto e implementação de máquinas, equipamentos e sistemas, juntamente com erros de operação e manutenção, e, por último, problemas de instalação e comissionamento.

A Figura 1 quantifica os principais motivos de acidentes em unidades industriais durante ciclo de vida de projetos da automação.

Figura 1 - Falhas prematuras em sistemas de automação.



Fonte: HSE.

Segurança em sistemas de automação industrial estão sustentados por três divisões básicas:

Segurança Elétrica: consiste em garantir a redução de riscos operacionais, choques elétricos ao operador em caso de falha. Normas IEC 61131, UL, diretiva CE são algumas das normas vigentes.

Segurança Intrínseca: consiste no desenvolvimento de técnicas de proteção para utilização de equipamentos elétricos e eletrônicos em áreas perigosas com liberação de gases ou líquidos inflamáveis potencialmente explosivos com limitação de energia e temperatura de forma a garantir que não ocorrerá ignição do material inflamável. Diretivas ATEX e IECEx, são as principais normas utilizadas.

Segurança Funcional: aborda técnicas para garantir funcionamento conhecido, mesmo em caso de falha. A segurança funcional busca a redução da probabilidade de falha perigosa, onde as normas IEC 61508, IEC 61511, ISO-13849 (*Safety of Machinery – Safety-related Parts of Control Systems*) são as mais utilizadas.

2.1 SAFETY INTEGRITY LEVEL- SIL

Basicamente, esta norma é uma padronização para especificação de requerimentos com o objetivo de atingir os níveis de integridade de segurança, e foi dividida em sete partes para melhor compreensão. A norma foi elaborada a partir da IEC (*International Electrotechnical Commission*) com o objetivo de orientar a gestão de todos os componentes dos sistemas de segurança relacionados abrangendo desde sensores e atuadores, até solucionadores de lógica para aplicações de segurança de determinado processo, levando em conta a pré determinação de variáveis para garantir um estado seguro de determinado equipamento, processo ou sistema.

A norma aplica-se a todo o ciclo de vida do sistema de segurança, desde o conceito, especificação, concepção, operação e utilização até a descontinuidade do produto ou sistema.

As três primeiras partes da norma correspondem ao desenvolvimento e aplicação do hardware e do software dos produtos E/E/EP (*Electrical/Electronic/Programmable Electronic*) e os demais capítulos servem de apoio para entendimento destas três primeiras. A tabela I ilustra a divisão da norma IEC 61508.

Tabela 1 - Divisão da IEC-61508.

Norma Internacional IEC-61508	
IEC-61508-1	Requisitos Globais
IEC-61508-2	Requisitos para sistemas E/E/EP ligados à segurança
IEC-61508-3	Requisitos de software
IEC-61508-4	Abreviaturas e definições de conceitos
IEC-61508-5	Exemplos de processo de avaliação de níveis de integridade de segurança
IEC-61508-6	Diretrizes para a aplicação das partes IEC-61508-2 e IEC-61508-3
IEC-61508-7	Visão global de técnicas e métricas utilizadas

Os produtos voltados para área de segurança funcional são classificados entre quatro níveis de integridade, denominados de SIL1 a SIL4 onde a delimitação de cada nível está

relacionada como o grau de disponibilidade, probabilidade de falha na demanda (PFD) e fator de redução de risco (RRF), conforme tabela 2 abaixo:

Tabela 2 - Níveis de integridade e segurança – SIL.

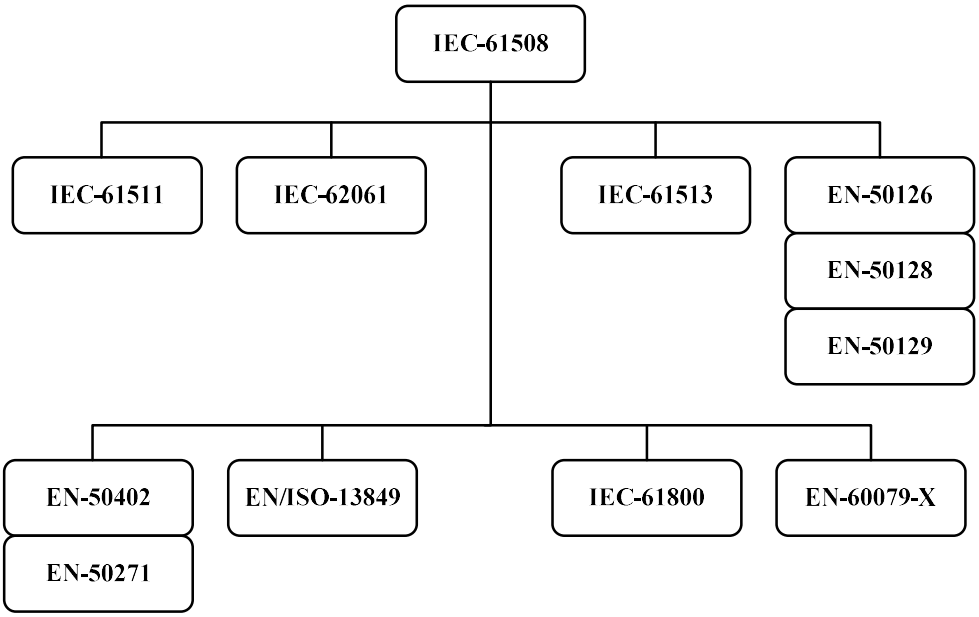
SIL	DISPONIBILIDADE	PFD	RRF
4	>99,99%	<0,01%	>10.000
3	99,90 a 99,99%	0,01 a 0,1%	1.000 a 10.000
2	99,00 a 99,90%	0,1 a 1%	100 a 1.000
1	90,00 a 99,00%	1 a 10%	10 a 100

Para o desenvolvimento do produto certificado, é necessário obedecer ao ciclo de vida do projeto, também descrito na norma supracitada, sendo este o item primordial para o sucesso do projeto.

Existem divisões para cada tipo de aplicação, dentre elas, pode-se destacar: IEC-61511 voltada para sistemas instrumentados de segurança, IEC-62061 (*Safety of Machinery: Functional Safety of Electrical, Electronic and Programmable Electronic Control Systems*) direcionada para segurança de máquinas operatrizes, IEC-61513 (*Nuclear power plants - Instrumentation and control important to safety*) para operação e segurança de usinas nucleares de geração de energia elétrica, EN-50126 (*Railway Applications – The Specification and Demostration of Reliability*), EN-50128 (*Railway Applications - Communication, Signalling and Processing systems - Software for Railway Control and Protection Systems*) e EN-50129 (*Railway applications – Communication, Signalling and Processing Systems – Safety Related Electronic Systems for Signalling*) voltada para segurança funcional de sistemas de transportes ferroviários, EN-50402 (*Electrical Apparatus for the Detection and Measurement of Combustible or Toxic Gases or Vapours or of Oxygen - Requirements on the Functional Safety of Gas Detection Systems*) e EN-50271 (*Electrical Apparatus for the Detection and Measurement of Combustible Gases, Toxic Gases or Oxygen - Requirements and Tests for Apparatus Using Software and/or Digital Technologies*) específica para sensores de gás, EN

ISO-13849, direcionada para máquinas de baixa complexidade, IEC-61800 (*Adjustable speed electrical power drive systems*) requisitos de segurança funcional para sistemas de acionamento de potência e velocidade de motores elétricos, EN-60079-X (*Electrical Apparatus for Explosive Gas Atmospheres*) especificação de requisitos gerais para construção, ensaios e marcação de componentes elétricos destinados à atmosfera explosiva. A Figura 2 ilustra as principais normas de segurança e seus níveis de hierarquia.

Figura 2 - Comparativo e hierarquia de normas de segurança funcional.



Fonte: do autor.

A classificação entre níveis de probabilidade de falhas e disponibilidade pode ser obtida de diversas formas, onde uma delas é feita a partir de cálculos de taxas de falhas dos componentes do produto. Outras técnicas são utilizadas, como análises de causa e consequência, árvore de falhas, análise por modelos de Markov, diagramas de blocos de confiabilidade, redes de Petri, métodos HAZOP, LOPA ou até mesmo a adoção de mais de uma técnica para resolução do problema.

Conceitualmente estas técnicas utilizam da mesma base para chegar aos resultados, neste caso, a classificação de falhas, a probabilidade de cada tipo de falha acontecer e medidas para mitigação do possível problema. Uma falha é considerada como um evento caracterizado por perda da capacidade de um dispositivo de não conseguir executar sua função, as falhas podem ser classificadas como:

Falhas aleatórias: quando ocorrem de maneira imprevisível, exemplo, defeitos de fabricação ou de instalação de determinado equipamento;

Falha de causa comum: ocorre em mais de um dispositivo ao mesmo tempo ou em um intervalo curto, exemplo, falta de energia elétrica, vibração, corrosão;

Falha na demanda: ocasionada quando o dispositivo deve ser acionado, tipo de falha ocasionada por falta de diagnóstico;

Falha oculta: só percebida quando se necessita do dispositivo ou o mesmo é testado;

Falha perigosa: potencial de impedir que uma função de segurança atue sob demanda;

Falha segura: pode causar o acionamento de um dispositivo de segurança sem a real necessidade.

Utilizando técnicas de estatística, a probabilidade de falha na demanda – PFD é a probabilidade de uma camada de proteção falhar em realizar sua função específica em resposta a uma demanda.

A Probabilidade média de falha na demanda – PFD_{awg} é o indicador de confiabilidade de uma camada de proteção calculado pela probabilidade média em um dado intervalo de tempo que a mesma falhe quando demandada.

O fator de redução de risco – RFF é a medida de desempenho de uma camada de proteção dada pela razão entre os riscos sem e com a implementação desta camada de proteção.

A disponibilidade é a proporção de tempo no qual o equipamento ou o sistema trabalha sem falhas.

As definições acima são as principais métricas utilizadas para cálculos de confiabilidade de sistemas de segurança conforme IEC-61508.

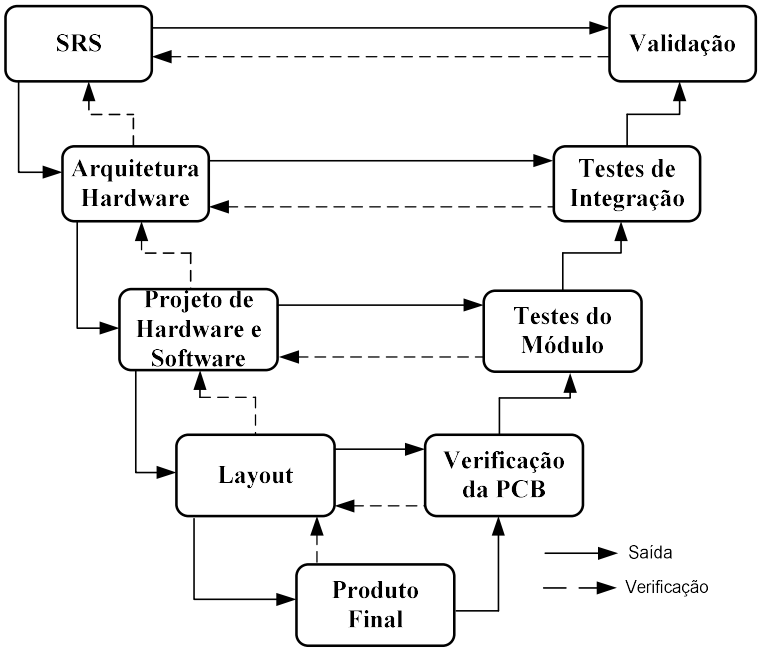
O ciclo de vida de um projeto de EP SIL é um processo de engenharia que utiliza etapas específicas para garantir que o equipamento seja eficaz no seu principal objetivo, a redução de riscos, além de ser rentável ao longo de sua vida útil. Este processo é um ciclo contínuo que inicia a partir do projeto conceitual do produto e termina somente após a sua descontinuidade.

A primeira fase do ciclo de vida é a análise de riscos onde é estudada a necessidade de redução de riscos. Para tanto, utiliza-se de cálculos probabilísticos para verificação da integridade do projeto de segurança, definida como isenção de riscos inaceitáveis.

A fase de realização é iniciada após a identificação de todas as funções de segurança do produto. Um projeto conceitual deve ser desenvolvido escolhendo a tecnologia dos componentes, arranjo entre estes, como redundância de circuitos para aumento dos níveis de integridade de segurança. Ao final desta etapa, a arquitetura do hardware do produto deve ser concluída.

O desenvolvimento do hardware e do software inclui a etapa seguinte do processo, onde deve-se descrever todas as funções de cada circuito projetado tanto para o hardware quanto para o software com o objetivo de sustentar a etapa de validação do produto. Ao final desta etapa, os digramas elétricos e o desenvolvimento do software embarcado devem ser concluídos, e ferramentas dedicadas para projeto e simulações são utilizadas para sustentar esta tarefa. O layout do circuito deve ser desenvolvido após a validação do projeto de hardware e de software, após o desenvolvimento do layout de placa e mecânica do produto, este estará sujeito a um processo criterioso de testes para certificar que todo o processo de desenvolvimento foi concluído com êxito. Este processo deve seguir o modelo recomendado pela norma, chamado modelo V onde cada etapa passa por uma rigorosa fase de verificação, conforme Figura 3 abaixo.

Figura 3 - Fluxograma do ciclo de vida do projeto de um EP.



Fonte: do autor.

2.2 SAFETY IINSTRUMENTED SYSTEM - SIS

Sistema Instrumentado de Segurança é o conjunto de funções instrumentadas de segurança – SIF (*Safety Instrumented Function*) de um determinado processo de segurança de uma planta industrial cuja função principal é levar este processo a um estado seguro em caso de falhas. Todos os componentes utilizados em um projeto de segurança fazem parte deste sistema. Os principais componentes de um SIS são:

Sensores: equipamentos responsáveis pela aquisição de dados do processo, classificados como digitais ou analógicos, podendo ser desde uma simples chave fim de curso ao um moderno sensor de temperatura, pressão ou um analisador de gás por exemplo.

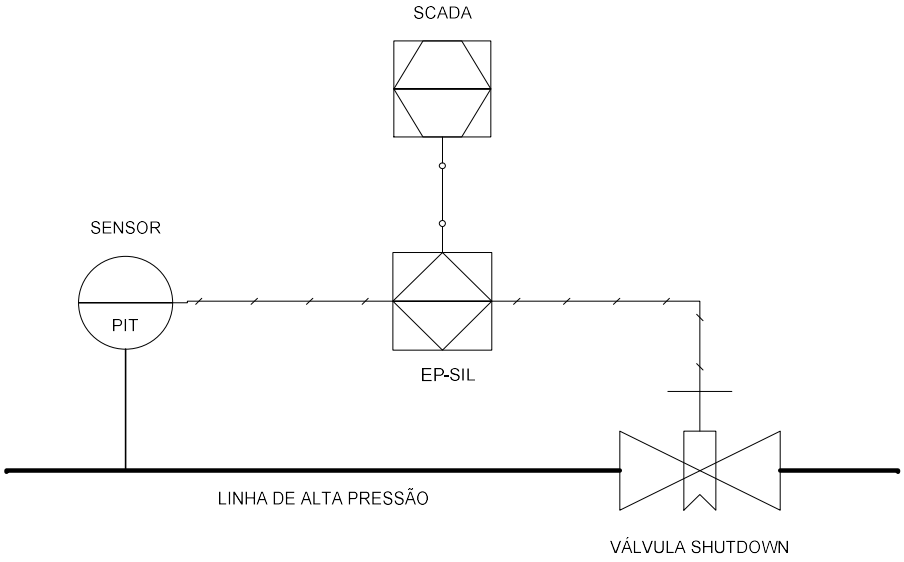
Controladores programáveis: equipamentos eletrônicos programáveis que realizam a leitura dos sensores e processam todas informações para tomada de decisão do processo de segurança.

Atuadores: elementos de acionamento que ficam interligados aos controladores programáveis do processo, como exemplo, relés, sirenes, válvulas On/Off ou válvulas de controle, entre outros.

Software: denominado SCADA, é o sistema que realiza comunicação com os controladores programáveis e faz a interface entre operadores do processo e demais sistemas como, ERP (*Enterprise Resource Planning*), MES (*Manufacturing Execution System*), bancos de dados, sistemas de gestão, entre demais sistemas. Normalmente a camada de software de interface dos sistemas de segurança possui sua plataforma dedicada e isolada dos demais sistemas para garantir acesso restrito ao pessoal especializado, sendo que o resumo das ocorrências é enviado aos demais sistemas de uma unidade de produção.

A Figura 4 representa um SIS com uma função instrumentada de segurança – SIF composta por um transmissor e indicador de pressão, um controlador de segurança e uma válvula de segurança do tipo *shutdown*.

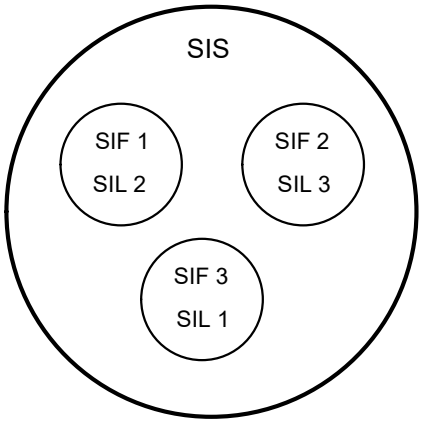
Figura 4 - Exemplo de um SIS com uma SIF.



Fonte: do autor.

A Figura 5 representa a hierarquia de um SIS que executa três funções de segurança, uma com SIL 1, uma com SIL 2 e uma com SIL 3. Para que isto seja possível, os componentes de cada SIF devem ter no mínimo o valor SIL requerido de cada SIF e o SIS deve possuir o valor SIL da SIF de maior índice.

Figura 5 - Hierarquia dos sistemas instrumentados de segurança.



Fonte: do autor.

2.3 CARACTERÍSTICAS CONSTRUTIVAS DE UM EP STANDARD

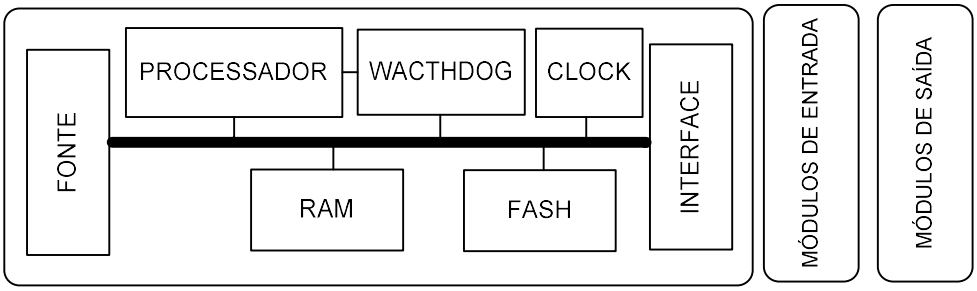
Controlador standard é um sistema de controle industrial de tempo real que executa um programa aplicativo armazenado em sua memória interna, pois deve funcionar independentemente do funcionamento de uma rede de comunicação como geralmente é projetado, garantido a continuidade do processo ao qual foi implementado. A programação deste equipamento é normatizada pela IEC-61131-3 e pode ser feita em até 6 linguagens de programação diferentes que podem ser utilizadas de forma mista no programa aplicativo, ou seja, pode ser programado em blocos de função para cada parte do programa, tornando mais organizado e de fácil entendimento para os demais usuários do sistema.

Como explicado anteriormente, este tipo de controlador é geralmente modular e dividido em blocos de entrada, CPU, fonte, módulos de comunicação e blocos de saída e são geralmente acoplados em um bastidor.

2.3.1 CPU

Uma CPU de um controlador Standard é formada por uma unidade de processamento, memórias RAM e Flash, relógio de tempo real, portas de programação e comunicação e circuito de monitoramento denominado *watchdog*, conforme Figura 6.

Figura 6 - Diagrama básico da CPU de um EP standard.



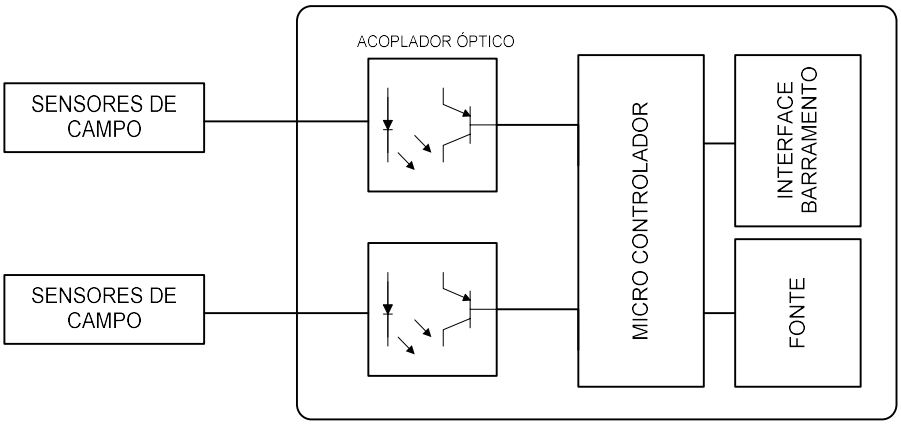
Fonte: do autor.

Os módulos de entrada e saída do EP standard são compostos de entradas digitais e analógicas e saídas digitais, e analógicas, cujos sinais de leitura e acionamento são definidos pela norma IEC-61131.

2.3.2 Módulos de Entradas Digitais

Módulos de entradas digitais normalmente são padronizados para sinais de campo de 24Vcc com capacidade de leitura geralmente de 8 ou 16 pontos de acordo com as especificações de cada fabricante. Estes módulos possuem um circuito de entrada com filtros, tratamento do sinal de entrada, acopladores ópticos para isolação do sinal de campo com o circuito digital, que por sua vez possui um circuito lógico geralmente utilizando um microcontrolador ou lógica programável do tipo EPLD ou similar, reguladores de tensão e circuito de interface do barramento de comunicação com a CPU conforme a Figura 7.

Figura 7 - Diagrama simplificado de um módulo de entradas digitais.

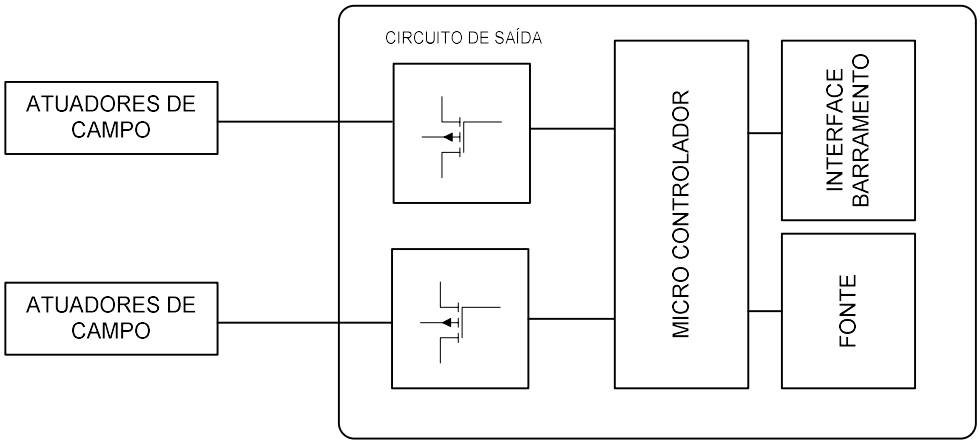


Fonte: do autor.

2.3.3 Módulos de Saídas Digitais

Os módulos de saídas digitais são compostos de conjuntos de saídas normalmente de 8 ou 16 pontos, possuem como elemento de acionamento das cargas externas transistores ou relés, de acordo com a aplicação final, e são formados por um circuito de interface de barramento e circuito digital similar ao módulo de entrada digital, conforme ilustrado na Figura 8.

Figura 8 - Diagrama simplificado de um módulo de saídas digitais.



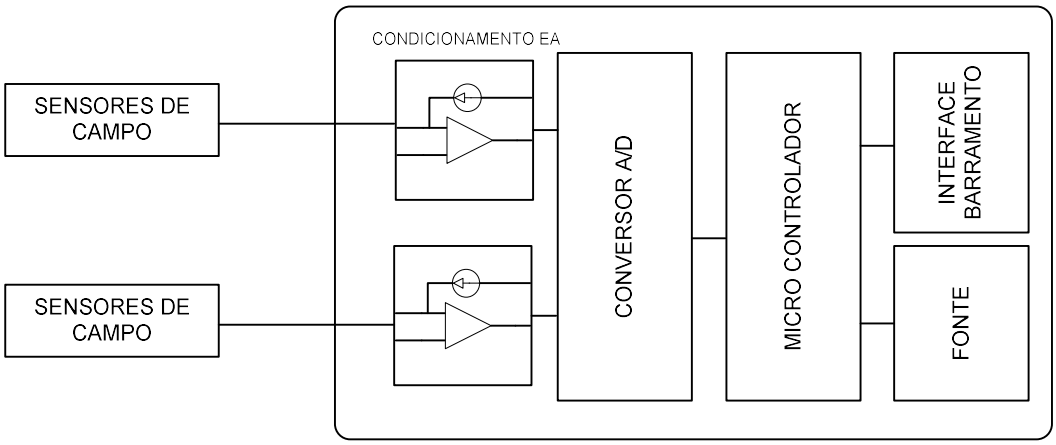
Fonte: do autor.

2.3.4 Módulo de Entradas Analógicas

Os módulos de entradas analógicas são compostos por 4 ou 8 entradas e possuem os sinais de leitura padronizados com a norma IEC-61131. Geralmente os sensores analógicos emitem sinais de corrente elétrica padronizados em 4 a 20mA alimentados pelo próprio módulo de entrada analógica ou por fonte externa, sinais de tensão entre -10 a 10V, além de termopares, RTD e sensores resistivos em geral, de acordo com sua aplicação. Existe uma gama de elementos sensores analógicos muito grande, por este motivo a norma estabelece a padronização do condicionamento dos sinais destes sensores para garantir a aplicação de qualquer fabricante de controlador de mercado.

Internamente, os módulos de aquisição de dados analógicos são compostos por um circuito de condicionamento e isolação do sinal de entrada, conversores analógicos/digitais – AD e circuito lógico microcontrolado com interface de barramento e fonte ou regulador de tensão conforme demais módulos já apresentados. Neste caso um mesmo canal de leitura analógica pode ser capaz de realizar a leitura de qualquer sinal de entrada padrão, desde que seja interligado e configurado da maneira correta. A Figura 9 ilustra o diagrama simplificado de um módulo de entrada analógico.

Figura 9 - Diagrama simplificado de um módulo de entradas analógicas



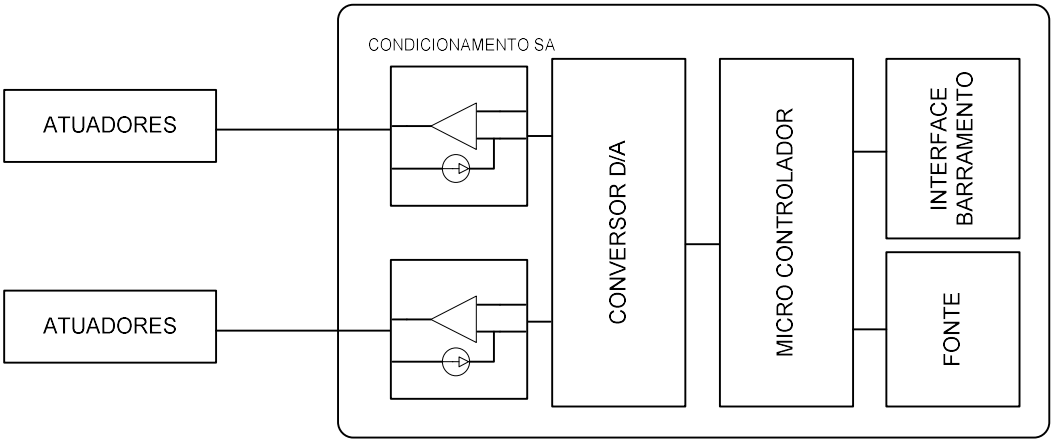
Fonte: do autor.

2.3.5 Módulo de Saídas Analógicas

Os módulos de saídas analógicas são normalmente compostos por 4 canais de saída padronizados a partir da IEC-61131 (os módulos de saída analógicas são projetados com 4 canais devido ao padrão da indústria e a capacidade de layout da placa do equipamento). Geralmente os transmissores analógicos recebem sinais de corrente elétrica padronizados em 4 a 20mA, 0 a 20mA e sinais de tensão entre -10 a 10V.

Internamente são compostos por uma interface de barramento, um circuito lógico com o microcontrolador, conversores digital/analógico – DA e driver de tensão e corrente elétrica para acionamento dos atuadores. Um diagrama básico deste módulo é apresentado na Figura 10.

Figura 10 - Diagrama simplificado de um módulo de saídas analógicas.



Fonte: do autor.

2.4 CARACTERÍSTICAS DOS CONTROLADORES SIL

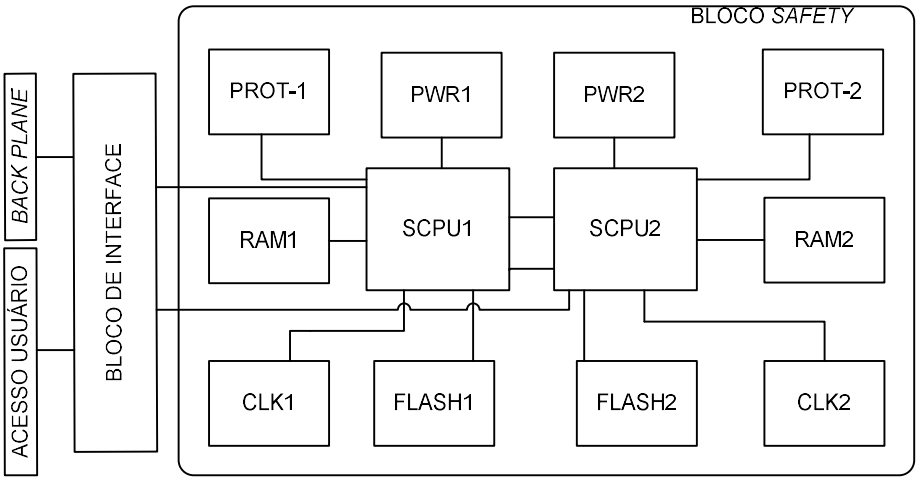
Os controladores SIL são equipamentos eletrônicos desenvolvidos para segurança de processos industriais, da mesma forma que os controladores standard, possuem processamento e comunicação em tempo real, porém utilizam biblioteca de lógicas limitadas aos projetos de segurança, ou seja, utilizam de instruções reduzidas a cada procedimento com a finalidade de

não sobrecarregar os processadores, memória de aplicativo, memória RAM além de possuírem componentes duplicados em seu projeto. Em alguns casos ainda são utilizados componentes triplicados em sua arquitetura formando a arquitetura de votação 2oo3, ou TMR (*Triple Modular Redundancy*).

2.4.1 CPU SIL

A CPU SIL, também chamada de *safety* CPU ou SCPU, é responsável pela execução do software aplicativo do cliente, interface de comunicação com demais sistemas e processamento dos sinais dos módulos de aquisição. Tipicamente a arquitetura de hardware da SCPU é dividida em três blocos distintos, sendo: fonte de alimentação, unidade de processamento e interface, como mostrado na Figura 11. Os componentes do hardware de um produto SIL são rigorosamente selecionados, alguns fabricantes possuem componentes já certificados para este tipo de projeto, mesmo assim, a utilização destes componentes não garante a certificação do equipamento, técnicas de layout, cálculo de confiabilidade devem comprovar tal capacidade.

Figura 11 - Diagrama de blocos safety CPU.



Fonte: do autor.

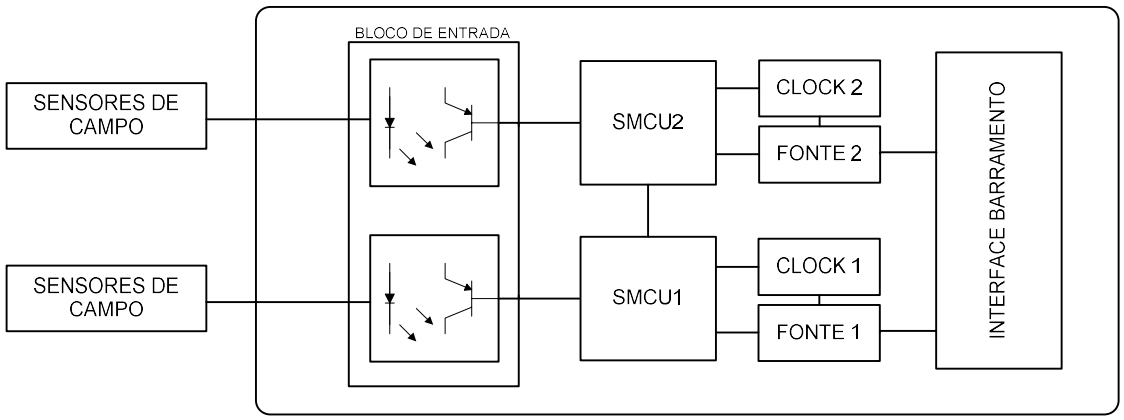
2.4.2 Módulo de Entradas Digitais SIL

Os módulos de entradas digitais possuem três blocos distintos e isolados: entrada, processamento e interface.

O circuito de entrada possui limitadores de tensão e corrente elétrica, filtro e acoplamento óptico para a transformação do sinal físico em sinal lógico a ser processado em cada SMCU (*Safety Microcontroller Unit*). As entradas digitais devem ter o limite de tensão e corrente, conforme definido na IEC 61131-2

O processamento interno é realizado através de dois microcontroladores denominados SMCU, responsáveis por todas as entradas de leitura e tratamento dos sinais internos e externos. O software interno possui um algoritmo que garante a concordância das mensagens das SMCUs para CPU. Este tipo de módulo possui duas fontes de alimentação independentes, uma para cada SMCU que além de alimentar as SMCUs, realizam isolamento entre a interface de barramento e o circuito de circuito de monitoração de tensão. A Figura 12 ilustra o diagrama de blocos do modulo de entrada digital.

Figura 12 - Diagrama de blocos módulo de entradas digitais.

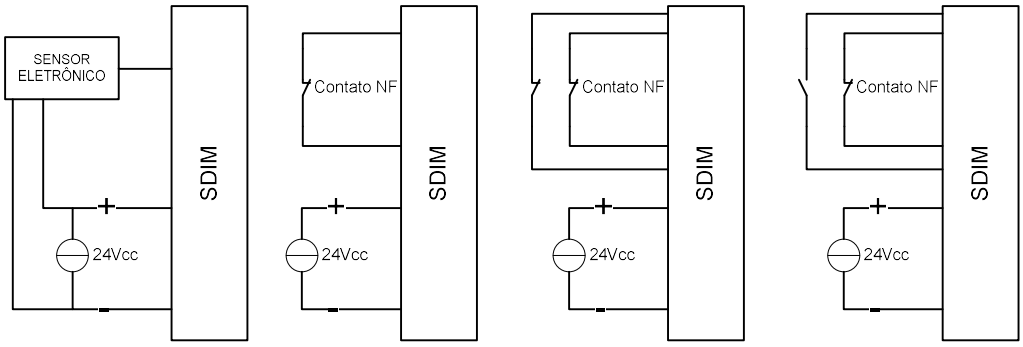


Fonte: do autor.

Os canais de entrada deste módulo possuem bornes de conexão que permitem diversos modos de ligação, seja um simples contato, um sensor alimentado por fonte externa,

configuração para arranjos de contatos paralelos ou série para configuração de sensores com arquiteturas 1oo1, 1oo2, 2oo3 entre outros. Para ambos arranjos é permitido o monitoramento de cada canal de entrada. A Figura 13 ilustra alguns esquemas de ligação dos sensores no módulo de entrada digital monitorado SDIM (*Safety Digital Input Monitored*).

Figura 13 - Esquema de interligação de sensores nos módulos de entradas digitais.



Fonte: do autor.

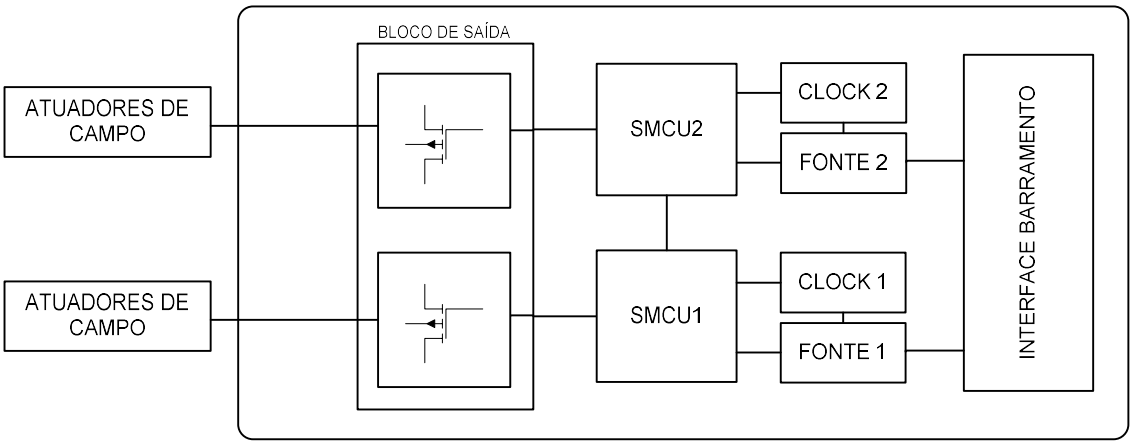
2.4.3 Módulo de Saídas Digitais SIL

Os módulos de saída digital SIL ou simplesmente SDOM (*Safety Digital Output Monitored*) são dispositivos aplicados à sistemas de segurança, concebido a partir dos requisitos da norma IEC-61508 e dividido em três blocos distintos, interface de comunicação, processamento e bloco de saídas.

As saídas digitais são os circuitos que fornecem corrente para um atuador. Neste caso, onde o requisito é segurança, cada canal de saída possui um driver de fonte de corrente positivo e um driver de coletor de corrente negativo. Ambos os SMCUs controlam cada parte da saída, com sinais complementares.

O SMCU1 é o único microcontrolador que se comunica com o ETHMCU. O software interno deve garantir que ambas as SMCUs “concordem” com o telegrama que está sendo recebido. A Figura 14 apresenta o diagrama de blocos do módulo de saída digital.

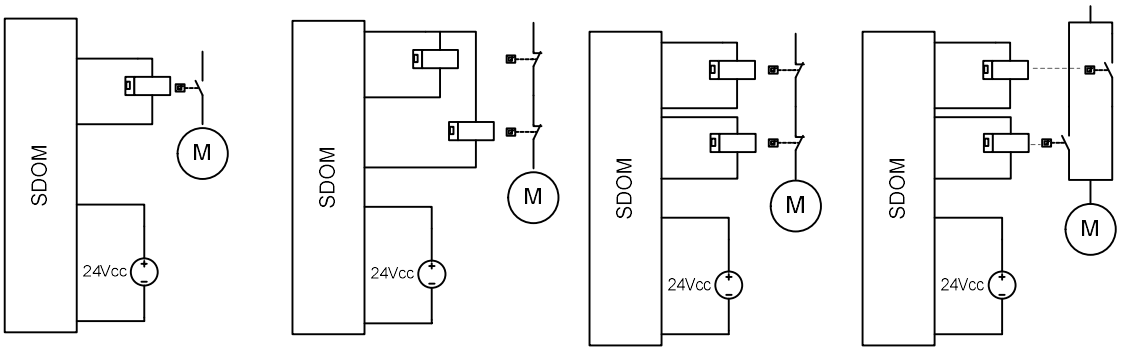
Figura 14 - Diagrama de blocos módulo SDOM.



Fonte: do autor.

Os canais de saída deste módulo possuem bornes de conexão que permitem diversos modos de ligação, desde uma saída simples, até arranjos série ou paralelo de acordo com a aplicação. Cada canal possui um circuito de monitoramento de corrente elétrica e um algoritmo de teste para cada canal com intervalo de tempo configurável. A Figura 15 ilustra alguns esquemas de ligação das cargas no módulo de saída digital monitorado SDIM.

Figura 15 - Exemplos de ligações de cargas no módulo SDOM.



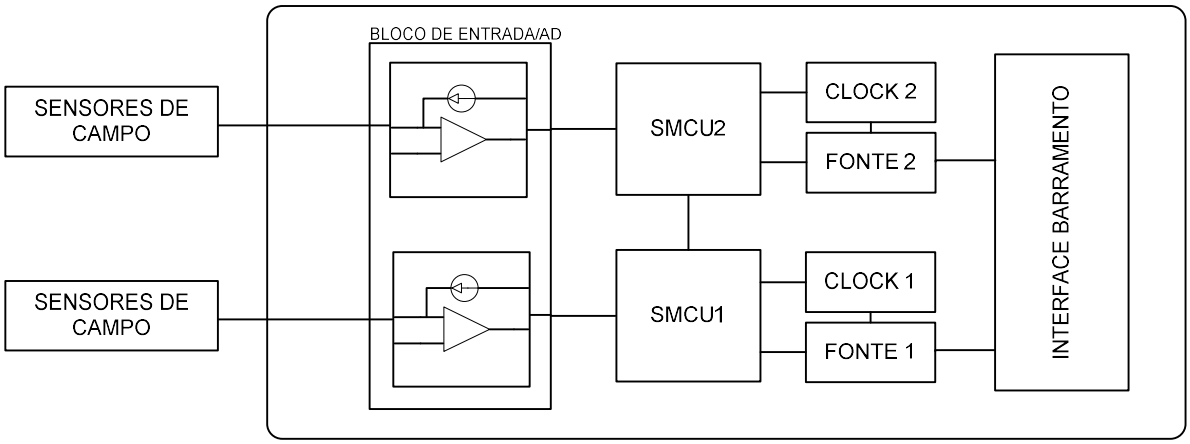
Fonte: do autor.

2.4.4 Módulo de Entradas Analógicas SIL

Os módulos de entradas analógicas são geralmente compostos por 4 canais e possuem os sinais de leitura padronizados com a norma IEC-61131, os sensores analógicos emitem sinais de corrente elétrica padronizados em 4 a 20mA alimentados pelo próprio módulo de entrada analógica ou por fonte externa, sinais de tensão entre -10 a 10V, além de entradas para termopares, RTD, e sensores resistivos, de acordo com sua aplicação.

Internamente, os módulos de aquisição de dados analógicos são compostos por um circuito de condicionamento e isolação do sinal de entrada, circuito de monitoramento dos canais de entrada, conversores analógicos/digitais – AD e duas unidades de processamento formada por processador, memória RAM, fonte e clock e a interface de barramento com conversor DC/DC. A Figura 16 ilustra o diagrama simplificado de um módulo de entrada analógico.

Figura 16 - Diagrama de blocos módulo de EA.



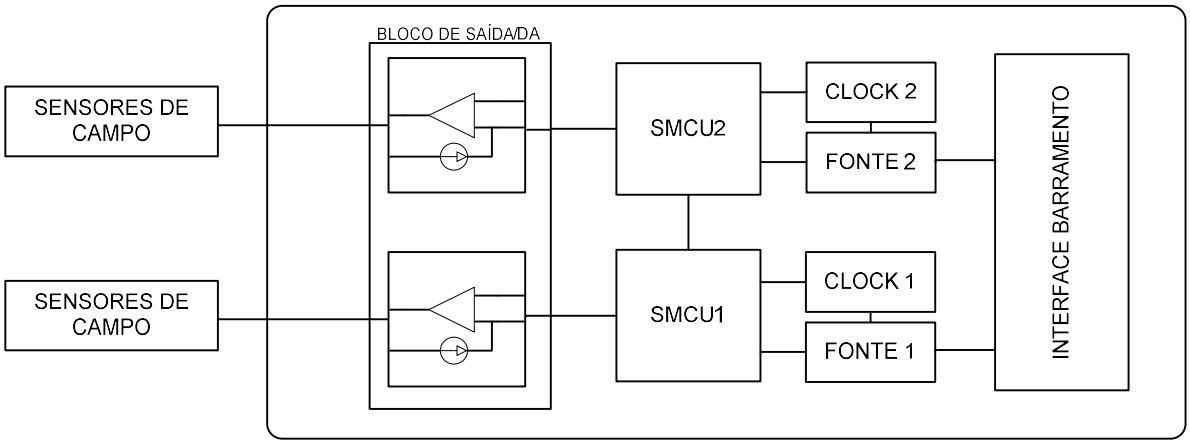
Fonte: do autor

2.4.5 Módulo de Saídas Analógicas SIL

Os módulos de saídas analógicas são normalmente compostos por 4 canais de saída padronizados a partir da IEC-61131. Geralmente os transmissores analógicos recebem sinais de corrente elétrica padronizados em 4 a 20mA, 0 a 20mA e sinais de tensão entre -10 a 10V.

São empregadas duas unidades de processamento formadas por processador, memória RAM, fonte e clock e a interface de barramento com conversor DC/DC. A Figura 17 ilustra o diagrama simplificado de um módulo de entrada analógico.

Figura 17 - Diagrama de blocos módulo de saídas analógicas.



Fonte: do autor.

2.5 PRINCIPAIS DIFERENÇAS ENTRE EP STANDARD E EP SIL

Um controlador programável consiste de uma arquitetura modular, onde os principais componentes são: bastidor, fonte, CPU, módulos de comunicação, módulos de aquisição de dados de sinais de campo e módulos de saída para controle de processo, constituídos de sinais digitais e analógicos padronizados por IEC-61131.

Sistemas dedicados à segurança funcional implicam na existência de uma série de técnicas para construção de hardware e software sustentadas por IEC-6508. Existe uma grande

diferença entre as duas soluções, em um controlador SIL, a segurança é prioridade, pois um EP SIL é projetado para atuar somente em caso de falha no processo, ao contrário dos controladores programáveis de processo onde exige-se muito do desempenho não desconsiderando a confiabilidade do sistema.

Quando se deseja que um controlador programável standard tenha características similares a um EP SIL, no ponto de vista das métricas de acordo com a tabela 2 sem comprometer o desempenho, existe a possibilidade de mesclar as técnicas construtivas conforme IEC-61131 e IEC-61508, tanto em hardware, quanto em software.

Como exemplo, o processador RM42L432 da *Texas Instruments* desenvolvido para SIL-3 possui arquitetura interna redundante e utiliza uma gama de diagnósticos embarcados no seu próprio firmware, garantindo um alto nível de confiabilidade. Desta forma, para aplicações de missão crítica com controladores programáveis Standard, são utilizadas técnicas similares, montando fontes, CPUs e até mesmo módulos de entrada e saída (I/O) em redundância. Para estes arranjos também é utilizada a técnica de aumento da gama de diagnóstico através de hardware e software no programa aplicativo. A elevação do custo da arquitetura redundante muitas vezes é inferior ao custo de desenvolvimento e certificação de equipamentos com selo SIL conforme a norma IEC-61508.

De acordo com IEC-61508 seção 6, diversos arranjos de interligação de componentes podem ser projetados para aumento de confiabilidade de um sistema. Estas técnicas podem ser adotadas em qualquer parte de uma malha de controle dos sistemas de segurança.

2.6 DIAGRAMA DE BLOCOS DE CONFIABILIDADE

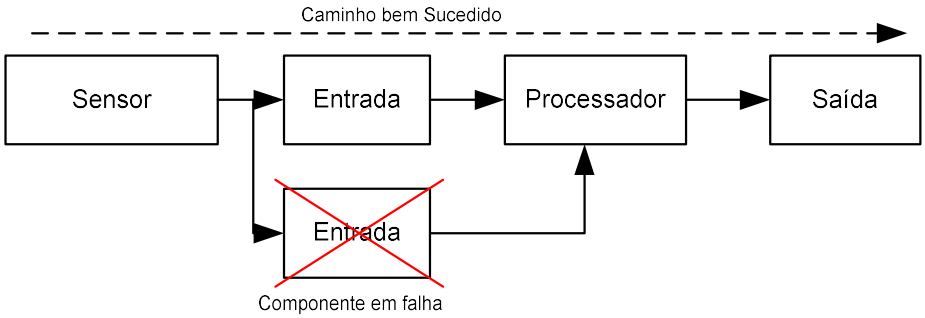
Conforme IEC 61508-6 anexo B e IEC 61131-6 o diagrama de blocos de confiabilidade RDB (*Reliability.Block Diagram*) é uma técnica utilizada para facilitar o cálculo de disponibilidade e probabilidade de falha de hardware de sistemas elétricos ou eletrônicos. A

técnica consiste em redesenhar cada módulo do sistema a ser calculado em formas de blocos, podendo ser representados em associações série, paralelo ou misto, seguindo um fluxo de acordo com sua interligação no sistema. No caso de leitura de um sinal, o fluxo ocorre do módulo de entrada até o elemento processador. Caso necessite-se uma sinalização, adicionam-se os componentes de sinalização, normalmente uma interface homem-máquina. No caso de um comando, adicionam-se os blocos que compõem a saída do sistema.

O RBD permite cálculo de confiabilidade de dois estados, sucesso ou falha, onde a resposta é bem sucedida caso seja possível encontrar um caminho de início a fim do fluxo não sendo obstruído por uma falha. Caso contrário, o caminho apresentou uma falha. Em sistemas redundantes, os componentes que são duplicados ou triplicados são tolerantes à falha de um ou mais módulos e demais componentes únicos não apresentam um caminho alternativo.

A Figura 18 ilustra um diagrama RBD com 2 canais de entrada duplicados e o restante dos componentes do sistema unitários.

Figura 18 - RBD de um controlador standard.

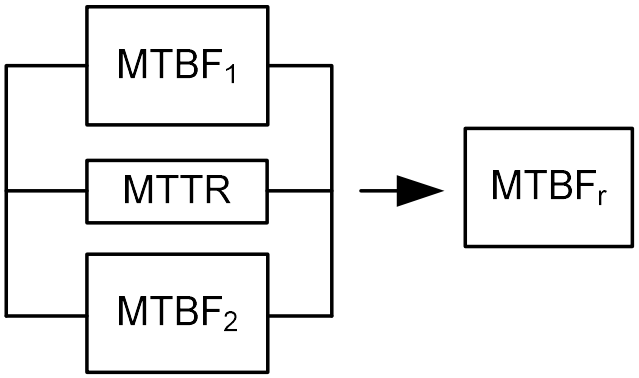


Fonte: IEC61508.

No exemplo da Figura 18 tem-se um sistema misto, onde os módulos de entrada estão em paralelo (realizando a leitura de um sensor através de um canal de cada módulo) e os demais componentes em série. Considerando os módulos de entrada do mesmo modelo, o primeiro

passo é calcular o resultado destes módulos em paralelo transformando-os em um componente com MTBF (*Mean Time Between Failures*) resultante e construindo então um circuito série para facilitar o cálculo. Neste cálculo, utiliza-se também o MTTR (*Mean Time to Repair*) que é o tempo médio de reparo, conforme Figura 19, o diagrama ilustra o MTBF resultante deste circuito paralelo. A forma de cálculo do MTBF resultante está descrita na Equação 1.

Figura 19 - Cálculo RBD paralelo.



Fonte: IEC 61508.

2.7 ARQUITETURAS DE VOTAÇÃO

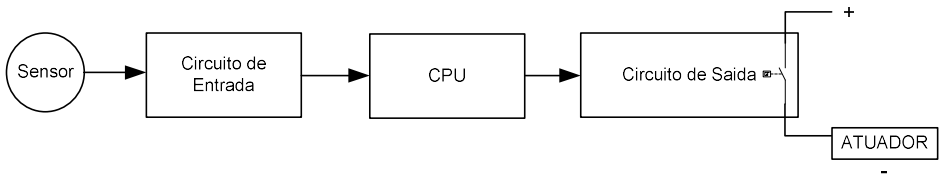
Conforme IEC 61508-6 anexo B as arquiteturas de votação MooN (D) (M *out of* N), referem-se à capacidade de votação e redundância do sistema, onde N indica o número de canais redundantes que executam a função, enquanto M indica quantos desses canais têm de estar disponíveis para funcionamento. A letra D se refere às capacidades de diagnóstico, ou seja, cada canal tem capacidade de executar testes de diagnóstico regulares para verificar o seu correto funcionamento e utilizar esses diagnósticos para adaptar o votador de saída de forma que o estado de saída global possa ser dado pelo(s) outro(s) canal(is). Saliente-se que os testes de diagnóstico somente reportam as falhas encontradas e não devem mudar nenhum dos estados de votação de saída.

Na ausência da letra D, os diagnósticos são utilizados também, mas apenas para alertar a existência de falhas diagnosticáveis.

As principais arquiteturas MooN são denominadas 1oo1, 1oo1D, 1oo2, 2oo2, 1oo2D, 1oo3 e 2oo3.

A arquitetura 1oo1 (diz-se “um-de-um”) consiste em um arranjo onde existe apenas um componente de entrada, um elemento de processamento e um elemento de saída. Nesta arquitetura nenhuma tolerância a falhas é fornecida nem proteção do modo de falha. Os circuitos eletrônicos podem falhar com segurança (saídas desenergizadas, circuito aberto) ou perigosamente (saídas energizadas ou curto-circuito). A Figura 20 ilustra a arquitetura 1oo1.

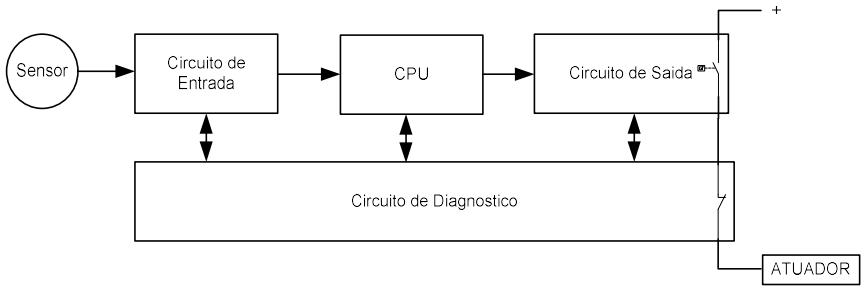
Figura 20 - Arquitetura 1oo1 de um controlador.



Fonte: IEC 61508.

A arquitetura 1oo1D é formada por um conjunto simples conforme a Figura 2, porém com um circuito de diagnóstico para o controlador. Neste caso, o circuito de diagnóstico implementa funções de segurança capazes de transformar uma falha perigosa em falha segura, por exemplo, a desenergização do circuito de saída. Como os efeitos dos diagnósticos on-line devem ser modelados, quatro categorias de falhas podem ser incluídas: λ_{DD} (*Dangerous, Detected Failure Rate*), λ_{DU} (*Dangerous, Undetected Failure Rate*), λ_{SD} (*Safe, Detected Failure Rate*), e λ_{SU} (*Safe, Undetected Failure Rate*). A Figura 21 ilustra a arquitetura 1oo1D.

Figura 21 - Arquitetura 1ooD de um controlador.

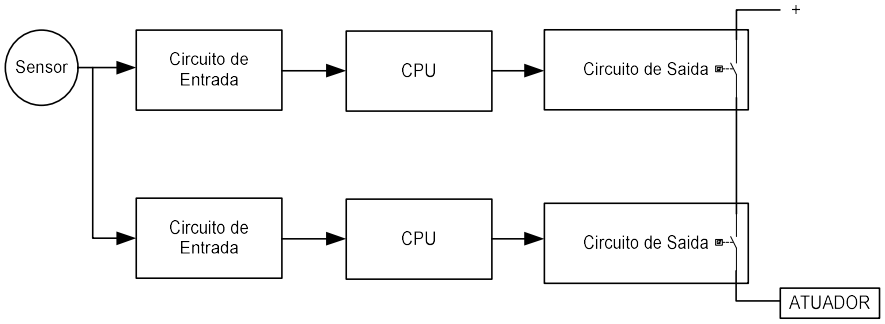


Fonte: IEC 61508.

A arquitetura 1oo2 consiste em dois controladores conectados em paralelo, onde as funções de segurança são processadas de forma independente, onde, desta maneira, deve ocorrer falha nos dois equipamentos para que ocorra uma falha da função de segurança. Esta configuração oferece baixa probabilidade de falha na demanda, mas aumenta a probabilidade de falha segura.

As saídas das funções de segurança são interligadas em série para garantir a segurança do processo. A Figura 22 ilustra a arquitetura 1oo2.

Figura 22 - Arquitetura 1oo2 de um controlador.

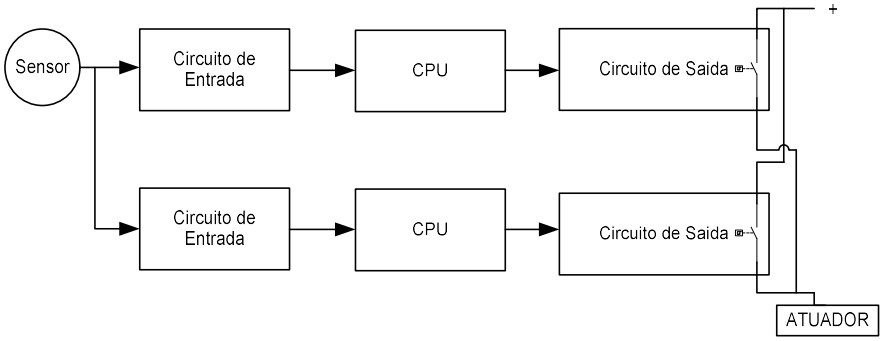


Fonte: IEC 61508.

Arquitetura 2oo2 é um conjunto idêntico ao circuito 1oo2, porém com as saídas interligadas em paralelo. É utilizada em situações onde não seja desejável falhar com as saídas desenergizadas, e, neste caso, se uma falha ocorrer em um dos componentes de um conjunto, o

outro que está ativo tem condições de assumir o controle. A Figura 23 representa a arquitetura 2oo2.

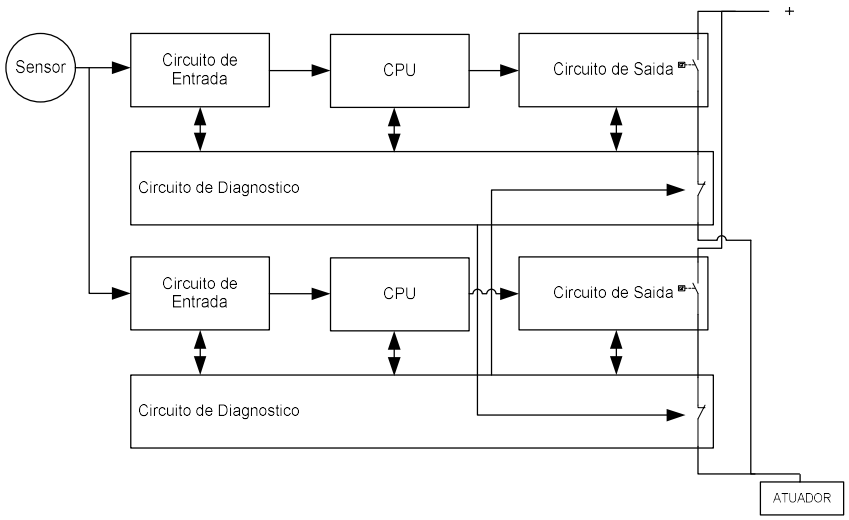
Figura 23 - Arquitetura 2oo2 de um controlador.



Fonte: IEC 61508.

A arquitetura 1oo2D consiste em dois conjuntos idênticos à arquitetura 1oo1D, onde o sensor é interligado e uma entrada de cada controlador, e suas saídas são respectivamente ligadas em série permitindo que uma unidade desligue a outra. A representação da arquitetura 1oo2D conforme Figura 24.

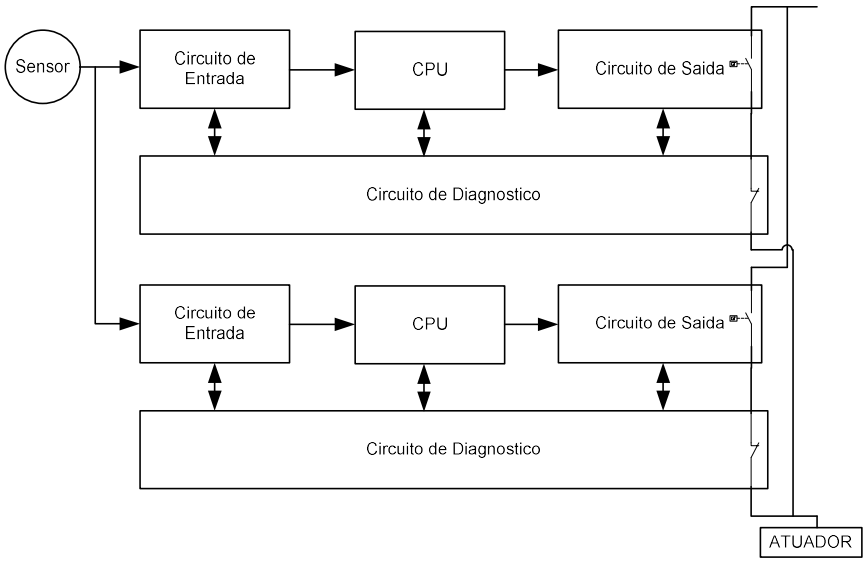
Figura 24 - Arquitetura 1oo2D de um controlador.



Fonte: IEC 61508.

A arquitetura 2oo2D consiste num arranjo de dois conjuntos 1oo2D organizados de maneira semelhante ao sistema 2oo2. A solução 1oo1D protege o sistema contra falhas perigosas, onde, desta forma, duas unidades 1ooD em paralelo protegem o sistema contra desligamentos. Para esta solução ser confiável, os diagnósticos devem ser muito eficazes pois uma falha perigosa não detectada causará uma falha perigosa em todo o sistema. A Figura 25 ilustra a arquitetura 2oo2D.

Figura 25 - Arquitetura 2oo2D de um controlador.

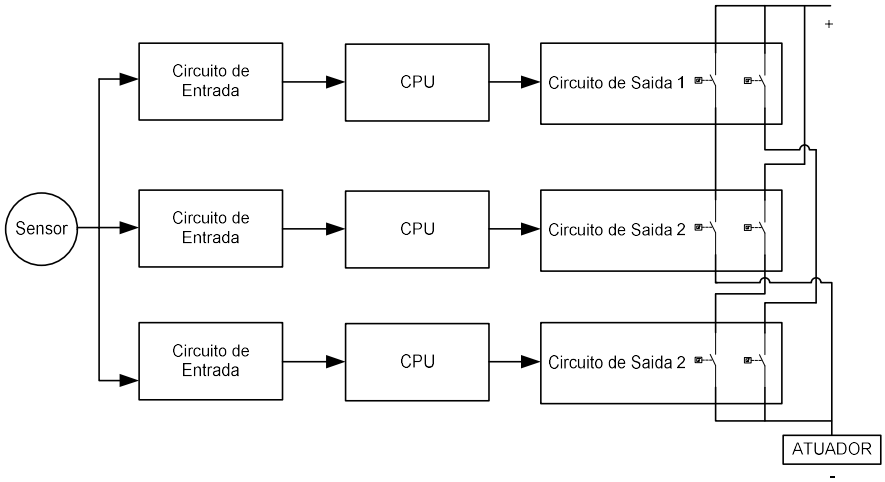


Fonte: IEC 61508.

Arquitetura 2oo3 é conhecida por tolerar falhas perigosas e falhas seguras (duas de três unidades devem estar em conformidade para o sistema operar) fornecendo alta disponibilidade. Duas saídas de cada unidade de controle são necessárias para cada circuito de saída, criando um sistema de votação onde o sistema acionará ou desligará a saída se no mínimo dois controladores forçarem este comando.

Uma análise detalhada do circuito de votação indica tolerância de uma falha de um dos modos de falha - perigoso (curto-circuito) ou seguro (circuito aberto). Quando uma unidade falha em circuito aberto, o sistema efetivamente se degrada para uma configuração de 1oo2. Se uma unidade falhar em curto-circuito, o sistema efetivamente se degrada para uma configuração 2oo2. Em ambos casos, o sistema permanece em operação. A arquitetura 2oo3 pode ser vista na Figura 26.

Figura 26 - Arquitetura 2oo3 de um controlador.



Fonte: IEC 61508.

A Tabela 3 apresenta resumidamente as principais funcionalidades de cada arquitetura apresentada identificando seus objetivos.

Tabela 3 - Quadro resumo de arquiteturas EP SIL.

ARQUITETURA	NUM. UNIDADES	NUM. SAÍDAS	OBJETIVO
1oo1	1	1	Unidade Básica
1oo2	2	2	Segurança
2oo2	2	2	Disponibilidade
1oo1D	1	2	Segurança
2oo3	3	6	Segurança e Disponibilidade
2oo2D	2	4	Segurança e Disponibilidade
1oo2D	2	4	Segurança e Disponibilidade + segurança

3 TRABALHOS RELACIONADOS

A análise dos trabalhos relacionados tem como objetivo uma pesquisa de trabalhos acadêmicos de maior relevância publicados em periódicos e revistas da área de sistemas de segurança com controladores dedicados a este fim, no entanto, a literatura não promove comparativos destas aplicações com controladores programáveis standard.

Segundo (Ždánsky et al., 2012), as funções de segurança de um controlador dedicado podem ser alcançadas por um controlador padrão de mercado, porém, este não possui reação predefinida no caso de falha, o que pode resultar em um valor arbitrário na saída do sistema de controle. Neste trabalho foi realizado um estudo de arranjos de arquitetura de funções instrumentadas de segurança comparando a aplicação de SIF com CLP SIL e CLP standard. Também foi analisada a influência do fator humano na atuação de sistemas automatizados de segurança concluindo que este é o fator mais provável que a falha perigosa.

Conforme (Rástočný et al., 2012), Sistemas de Controle Relacionados à Segurança - SRCS podem comprometer o nível de integridade de segurança - SIL do Sistema Instrumentado de Segurança - SIS devido à combinação de diagnósticos embarcados no controlador e sua devida integração com os diagnósticos e interpretações do SRCS desenvolvidos no programa aplicativo. Sugere-se a implementação de diagnósticos dos componentes da malha, como, monitoração de contatos de sensores e contatores no programa aplicativo, e utilização de demais componentes desta malha de segurança com certificação SIL desejada.

Conforme (Safety Reference Manual 1756-RM001O-EN-P, 2018) controladores Standard da série Controllogix® Rockwell Automation podem alcançar nível SIL 2 em suas aplicações dependendo da maneira em que os módulos do sistema são arranjados. Neste documento também é apresentado o memorial de cálculo para atingimento do SIL desejado pelo conjunto. Boas práticas de instalações mecânicas e elétricas dos controladores e seus componentes também são reforçadas neste manual.

De acordo com (Georgies et al., 2016), circuitos de entrada e saída digitais monitorados aplicados em sistemas de missão crítica podem atingir SIL4 a partir do circuito projetado e dos recursos de diagnósticos desenvolvidos e medidos através da probabilidade de falha por hora - PFH. Circuitos de condicionamento de sinais de saída compatíveis com o tipo 2 da IEC-61131 incluindo sinais de teste e feedback de status para monitoramento de circuitos podem atingir valores suficientes para atingimento de SIL4.

Conforme (Bukoswki et al, 2009), funções instrumentadas de segurança – SIF podem sofrer alterações de resultado de probabilidade média de falha na demanda PFD_{avg} (*Average Probability of dangerous Failure on Demand*) quando submetidos ao intervalo de testes de prova - PTI menor que 100% e completude menor que 100% pode sofrer degradação do nível SIL ao longo do tempo. O trabalho propõe uma correção destes resultados através da inserção de probabilidade de completude e da probabilidade de correção do intervalo de teste de prova.

De acordo com (Rástočný et al., 2016), o projeto de um SIS deve ser observado o dimensionamento das funções de segurança-SIF para garantir o tempo de atuação de uma determinada SIF quando demandada. Funções de segurança projetadas pelo usuário quando mau dimensionadas podem levar a degradação da segurança de todo o sistema.

Segundo (Sammarco, 2007), sistemas ESD (*Electronic Shutdown System*) aplicados em máquinas de mineração estão sendo realizados através de PLC (*Programmable Logic Controllers*), antes realizados através de fiação e lógica fixa (*Wardwired*). O trabalho compara a utilização dos sistemas ESD realizados através de *hardwired*, PLC e S-PLC (*Safety PLC*). Os testes realizados concluíram que ESD com *wardwired* atingiu SIL 2 com arquitetura 1oo1 e SIL 3 com arquitetura 1oo2. O ESD com a utilização de PLC atingiu apenas SIL 1 com arquitetura 1oo1 sendo o mesmo equipamento utilizado para o controle da máquina, enquanto o S-PLC independente do processo atingiu SIL 3 utilizando arquitetura 1oo2D.

De acordo com (Rástočný et al., 2017) controladores lógicos programáveis de segurança estão sendo utilizados para controle de processos devido aos requisitos de segurança em hardware por garantir uma reação segura em caso de detecção de falha e devido ao alto grau de diagnósticos por software que este tipo de equipamento proporciona. o trabalho analisou a influência dos parâmetros nativos no controlador de segurança combinados com os diagnósticos implementados no software aplicativo destes controladores para a cobertura dos sensores e atuadores da função de segurança e o comprometimento da integridade desta função de segurança devido à possíveis falhas de desenvolvimento do programa aplicativo.

Conforme (Torres et al., 2019) uma metodologia para avaliação de integridade de EP é proposto utilizando arquitetura de votação 2oo3 e análise através de modelo de Markov. A escolha por modelo Markov segundo Torres deve-se por considerar as taxas de falhas perigosas detectáveis, não detectáveis e aplicáveis em sistemas de baixa e alta demanda, onde cálculos estatísticos não realizam uma cobertura completa quanto apresentada pelo autor.

Segundo o autor, as normas IEC 61508, a IEC 61511 e a ISA TR 84.00.02 recomendaram diferentes métodos analíticos para quantificar a probabilidade de falha e o SIL necessário. Embora os padrões IEC e o relatório ISA sejam amplamente utilizados na indústria, esses padrões não fornecem uma abordagem abrangente dos métodos, nem especificam qual técnica deve ser aplicada com base nas características operacionais do sistema relacionado à segurança.

Embora o estudo comparativo tenha elencado lacunas no método utilizando equações simplificadas, o modelo de confiabilidade apresentado obteve mesmo resultado de desempenho (SIL2) em ambos os casos amostrados. O autor sugere ampliação do estudo utilizando através de falhas sistemáticas provenientes de erros de projetos, instalações e falhas de software.

Conforme (Torres et al., 2020) uma metodologia para avaliação de integridade de segurança de IEDS de proteção de rede elétrica é proposto através de modelo de Markov. O

artigo realiza comparação com método RBD alertando que o mesmo não contempla causas potenciais de falhas.

Torres realiza intervalos de teste de prova de um a cinco anos e verifica a degradação de SIL 3 para SIL 2 a partir de três anos de operação e reforça que o EP possui a maior influência no desempenho total do sistema composto por sensores, EP e atuadores.

Segundo Torres, em instalações industriais com arranjos de proteção, existem cenários de risco como consequência de qualquer aplicação incorreta mostrada neste documento. Um evento não controlado, particularmente no estudo de caso, uma falha de sobrecorrente nesses sistemas pode criar efeitos nocivos às pessoas, dispositivos e meio ambiente. A verificação SIL com IEDs sobre os arranjos de proteção fornece segurança e confiabilidade à operação de sistemas de energia industriais e comerciais em configurações complexas.

Este trabalho se diferencia dos demais por aproximar a metodologia de projeto dos controladores standard com os controladores de segurança comparando-os através de MTBF, disponibilidade, probabilidade de falhas, fator de redução de risco, fração de falhas seguras entre outras métricas não menos importantes. O trabalho propõe a aplicação dos controladores standard em funções de segurança onde certificações SIL não são exigidas, além disso a utilização de técnicas estudadas para emprego em sistemas de missão crítica com intuito de mitigação de possíveis falhas e melhoria de performance de segurança. Tornar esta metodologia mais popular pode significar a redução do índice de falhas em sitemas de automação de acordo com o gráfico da Figura 1.

A Tabela 4 - apresenta uma breve comparação entre os principais trabalhos relacionados.

Tabela 4 - Comparativo dos trabalhos relacionados.

Autor	Funções Segurança CLP Std	Monitoramento sensores	Ciclo de Vida	Arq Votação	CLP SIL Processos	RBD
Ždánsky, 2012	X					
Rástočný,2012		X				
Georgies,2016		X				
Rástočný, 2016			X			
Sammarco, 2007	X			X		
Rástočný, 2017				X	X	
Torres, 2019				X		
Torres, 2020						X
Juliano, 2020	X	X	X	X		X

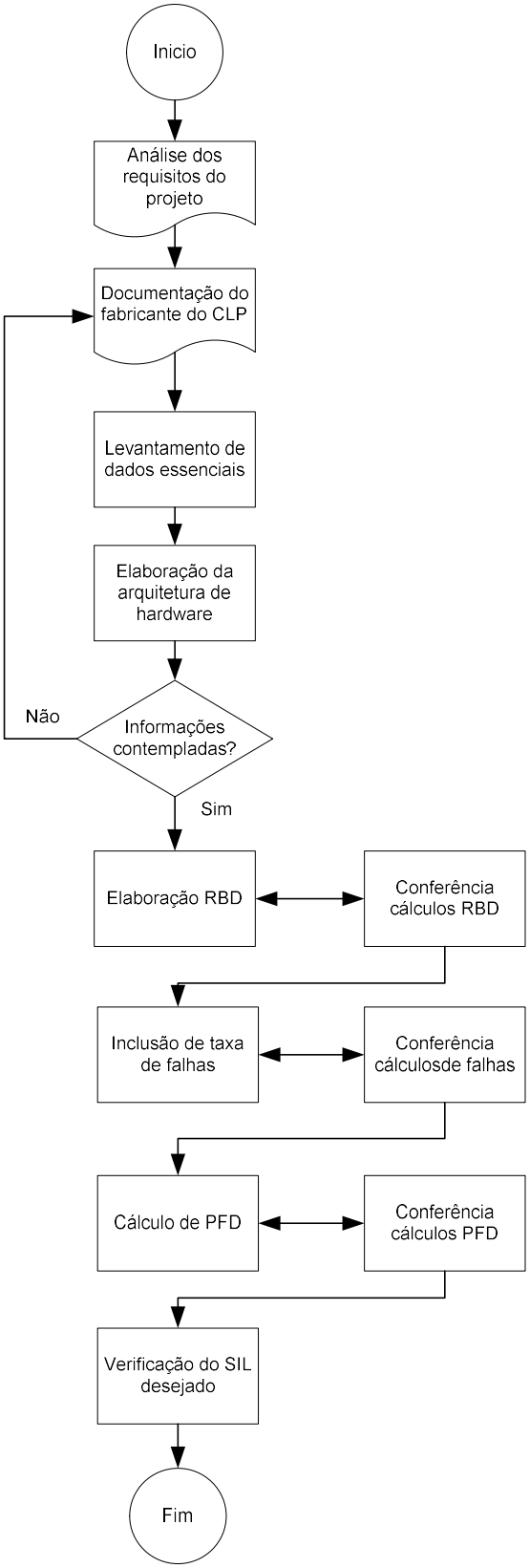
4 METODOLOGIA DE CÁLCULO DE CONFIABILIDADE

Pela avaliação das arquiteturas típicas dos EPs de segurança apresentadas na seção anterior, percebe-se que cada caso possui uma aplicação específica, seja ela relacionada com disponibilidade, tolerância à falhas ou fator de redução de riscos. Com base nestas arquiteturas, os controladores programáveis standard, que por sua concepção de projeto escalar, podem ser arranjados de formas similares aos EPs de segurança com o objetivo de atingirem métricas SIL.

Os controladores standard são tipificados por sua disponibilidade e não por sua tolerância a falhas como os controladores de segurança, porém, na prática o resultado é semelhante, a diferença está forma de cálculo que deve ser utilizada, apresentada nesta dissertação. Para obter os resultados em controladores standard, utiliza-se dos dados dos fabricantes que disponibilizam MTBF e Tempo Médio de Reparo - MTTR como as principais fontes de consulta. Em controladores de segurança utilizam-se taxas de falhas, análise através de árvore de falhas e Monte Carlo, dentre as principais técnicas.

Conforme fluxograma de cálculo da Figura 27 abaixo, os métodos RBD e cálculos probabilísticos foram escolhidos para o desenvolvimento deste trabalho por conta da facilidade de compreensão e versatilidade de aplicação em qualquer linha de controladores standard com características modulares.

Figura 27 - Fluxograma de cálculo de PFD.



Fonte: do autor.

A primeira etapa do projeto é a leitura da especificação técnica do projeto do sistema instrumentado de segurança onde devem constar os requisitos técnicos necessários, relação das malhas das funções instrumentadas de segurança com as informações de SIL desejado em cada malha de segurança. Estas especificações geralmente são realizadas através do estudo HAZOP, parte-se do princípio de que este estudo já foi realizado, pois não faz parte do estudo deste trabalho.

De posse desta documentação deve ser estudada documentação do fornecedor do controlador para avaliar como este equipamento será instalado e sua flexibilidade de arranjos de arquiteturas conforme apresentado no item 2.7 deste trabalho. Os dados essenciais para preparação dos cálculos de confiabilidade são: MTBF de cada componente de hardware, MTTR e MRT do conjunto, informações do fabricante do controlador que possibilite a levantamento da cobertura de diagnósticos – DC da solução.

Para a elaboração da arquitetura deve-se observar a flexibilidade, características elétricas, mecânicas e boas práticas contidas nos manuais do fabricante possibilitando que alguma das arquiteturas de votação apresentadas possam ser implementadas.

Após e elaboração da arquitetura, deve-se verificar se todas informações obrigatórias estão contempladas e então deve-se projetar o diagrama de blocos de confiabilidade – RBD conforme item 4.1 deste trabalho.

Concluído o RBD e os cálculos de disponibilidade para a arquitetura desenvolvida a próxima etapa é a inclusão das taxas de falhas conforme item 4.2 deste trabalho. Importante salientar a tabela de cobertura de diagnósticos, conforme IEC 61508 apresentada na tabela 4, esta é uma análise quantitativa realizada a partir das características construtivas dos componentes e do projeto de layout do circuito eletrônico do produto estudado.

A última etapa após a verificação das taxas de falhas são os cálculos de probabilidade média de falha na demanda - PFDavg de acordo com a equações 14 a 17 para arquiteturas 1oo1

e 1oo2 objetos de estudo deste trabalho. A finalização dos cálculos de todos os luxos RBD exigem a comparação dos resultados obtidos com os requisitos solicitados nas especificações do projeto do sistema de segurança.

4.1 CÁLCULOS RBD

Conforme Goble et al, algumas formas de cálculo de disponibilidade e tolerância a falhas são sugeridas, dentre elas, a técnica escolhida para o comparativo do controlador SIL com o controlador standard foi a RBD.

Conforme o item 2.4 o método RBD permite a simplificação dos componentes do sistema de forma que cada componente ou módulo seja associado à arquitetura a fim de garantir melhores métricas de confiabilidade do sistema.

Para componentes idênticos em paralelo, calcula-se o MTBF resultante a partir do MTBF e do MTTR fornecidos pelo fabricante do componente conforme Equação 1 abaixo:

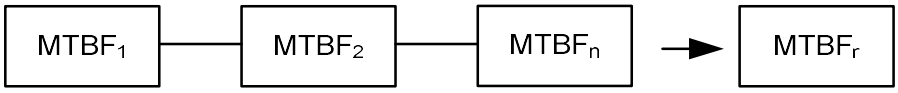
$$MTBF_R = \frac{MTBF^2}{2 * MTTR} \quad (1)$$

Ou, de outra forma, calcula-se a partir das taxas de falhas, conforme Equação 2:

$$\lambda_R = 2 * \lambda^2 * MTTR \quad (2)$$

Calculando o MTBF do sistema em paralelo, tem-se um sistema em série conforme a Figura 27.

Figura 28 - Método de cálculo RBD resultante.



Fonte: IEC 61508.

Para o caso de um sistema série, as equações de MBTF e taxa de falhas seguem abaixo com as equações 3 e 4 respectivamente:

$$MTBF_R = 1/(^1/_{MTBF_1} + \ ^1/_{MTBF_2} + ^1/_{MTBF_n}\ ) \quad (3)$$

Do ponto de vista da taxa de falhas (λ):

$$\lambda_R = \lambda_1 + \lambda_2 + \lambda_n \quad (4)$$

Existe uma forma de calcular sistemas redundantes genéricos, onde existem N equipamentos redundantes idênticos, dos quais M devem estar funcionando para que o sistema esteja em operação (1 <= M <= N). Este método é denominado redundância MooN, calculado a partir da Equação 5.

$$MooN = \frac{\lambda^{-1}}{(n-m)!\, m\left(\frac{n}{m}\right)} \left(\frac{\mu}{\lambda}\right)^{n-m} \quad (5)$$

Observa-se que:

- λ = taxa de falhas (falhas por hora);
- μ = taxa de reparos;
- D = disponibilidade (%);

A taxa de falhas deve ser calculada a partir da Equação 6.

$$\lambda = \frac{1}{MTBF} \quad (6)$$

A taxa da reparos é igual ao inverso do tempo médio para reparos conforme Figura 7

$$\mu = \frac{1}{MTTR} \quad (7)$$

A disponibilidade é calculada a partir da Equação 8.

$$D = \frac{MTBF_r}{(MTBF_R + MTTR)} * 100 \quad (8)$$

4.2 Cálculos de Probabilidade de Falhas

Para refinamento dos cálculos, foi incluída neste capítulo a forma de cálculo de probabilidade de falhas nos controladores standard para efeito comparativo das arquiteturas 1oo1 e 1oo2 nos controladores standard pesquisados.

De acordo com a norma IEC 61508 abaixo segue a forma de cálculo dos termos comuns às duas arquiteturas estudadas. Quando se deseja incluir taxas de falhas em controladores standard se utiliza na prática que metade da taxa de falhas é segura e a outra metade é perigosa, assim tem-se:

λ - taxa de falhas*;*

λs - taxa de falhas segura;

λd – taxa de falhas perigosa;

A Equação 9 corresponde à taxa de falhas seguras:

$$\lambda s = \frac{\lambda}{2} \tag{9}$$

O cálculo de taxa de falhas perigosas é realizado através da Equação 10.

$$\lambda d = \frac{\lambda}{2} \tag{10}$$

A cobertura de diagnóstico DC (*diagnostic coverage*) é um fator medido em percentual obtido através de um checklist de acordo com as normas IEC-61508-2, anexos A e C, e IEC-61508-6, anexo C, onde deve ser realizada uma análise detalhada a partir de diagramas de blocos e esquemas elétricos para verificar quais foram as técnicas de segurança empregadas no projeto. Neste caso é realizada uma estimativa em função dos componentes, layout de placa e esquema elétrico dos circuitos empregados no projeto. Quando o nível de informações sobre estes parâmetros é baixo devido à falta de informações do fabricante, aplica-se a tabela de baixa cobertura de diagnósticos. A tabela 4 apresenta um exemplo para apoio de cobertura de diagnósticos dos controladores, fonte IEC 61508-6 anexo C.

Tabela 5 - Cobertura de diagnósticos e eficácia para diferentes elementos.

Componente	DC Baixo	DC Médio	DC Alto
CPU	total inferior a 70%	Total inferior a 90%	
Registrador, RAM	50 a 70%	85 a 90%	99 a 99,99%
codificação e execução incluindo *"flag register"*	50 a 60%	75 a 95%	-
Cálculo de endereço	50 e 60%	85 a 98%	-
Contador de programa, *"stack"*, ponteiro	50 a 70%	60 a 90%	85 a 98%
Barramento			
Unidade de gerenciamento de memória	50%	70%	90 a 99%
Arbitragem de barramento	50%	70%	90 a 99%
Interrupção	40 a 60%	60 a 90%	85 a 98%
Clock (cristal)	50%	-	95 a 99%
Monitoramento de programa			
temporal	40 a 60%	60 a 80%	-
lógico	40 a 60%	60 a 90%	-
temporal e lógico	-	65 a 90%	99,99%
Memória invariável	50 a 70%	99%	99,99%
Memória variável	50 a 70%	85 a 90%	90 a 99,99%
Hardware Discreto			
Digital I/O	70%	90%	99%
Analógico I/O	50 a 60%	70 a 85%	99%
Fonte de Alimentação	50 a 60%	70 a 85%	99%
Comunicação e armazenamento em massa	90%	99,90%	99,99%
Dispositivos eletromecânicos	90%	99%	99,90%
Sensores	50 a 70%	70 a 85%	99%
Elementos finais	50 a 70%	70 a 85%	99%

Após obtenção da cobertura de diagnóstico calcula-se a taxa de falhas perigosas e detectáveis, λ_{dd}, a partir da Equação (11).

$$\lambda dd = \lambda d * DC \tag{11}$$

A fração de falha segura SFF (*safe Failure Fraction*) é um fator obtido através das taxas de falhas seguras e perigosas detectáveis, conforme (12).

$$SFF = \frac{(\lambda s + \lambda dd)}{\lambda} \quad (12)$$

A taxa de falhas perigosas e não detectadas é obtida da Equação (13).

$$\lambda du = \frac{\lambda}{2} * (1 - DC) \quad (13)$$

A probabilidade média de falha na demanda - PFDavg é calculada a partir da taxa de falhas perigosas e não detectadas e o intervalo de teste de prova, conforme Equação (14). No caso, PTI (*Proof test Interval*) medido em horas (h). tipicamente realizado em períodos de 1, 2, 5, 10 e 20 anos

$$PFDavg = \frac{\lambda du * PTI}{2} \quad (14)$$

Para arquiteturas 1oo2 foram utilizadas as equações de tempo de inatividade equivalente ao canal de entrada ou saída, de acordo com o fluxo RBD e tempo de inatividade equivalente ao sistema como um todo:

Tempo de inatividade equivalente ao canal – TCE (*Channel Equivalent Down Time*), conforme Equação (15).

$$TCE = \frac{\lambda du}{\lambda d} * \left({}^{PTI}/_{2} + MRT\right) + \left({}^{\lambda dd}/_{\lambda d} * MTTR\right) \quad (15)$$

- Onde MRT (*Mean Repair Time*)

Tempo de inatividade equivalente ao sistema – TGE (*System Equivalent Down Time*), conforme Equação (16).

$$TGE = \frac{\lambda du}{\lambda d} * \left({}^{PTI}/_{3} + MRT\right) + \left({}^{\lambda dd}/_{\lambda d} * MTTR\right) \quad (16)$$

Probabilidade média de falha na demanda para arquitetura 1oo2, conforme Equação (17).

$$PFDavg = 2 * [(1 - \beta d) * \lambda du]^2 * TCE * TGE + (\beta d * MTTR) + \beta * \lambda du * \left({}^{PTI}/_{2} + MRT\right) \quad (17)$$

Através deste método, é possível realizar uma aproximação mais detalhada do nível de integridade de segurança - SIL que um controlador Standard pode atingir.

5 ESTUDO DE CASO

O estudo de caso em referência aplica-se aos sistemas de Shutdown e Fogo e Gás – F&G de plataformas de petróleo, locais onde a segurança do meio ambiente, pessoas e processo é fundamental.

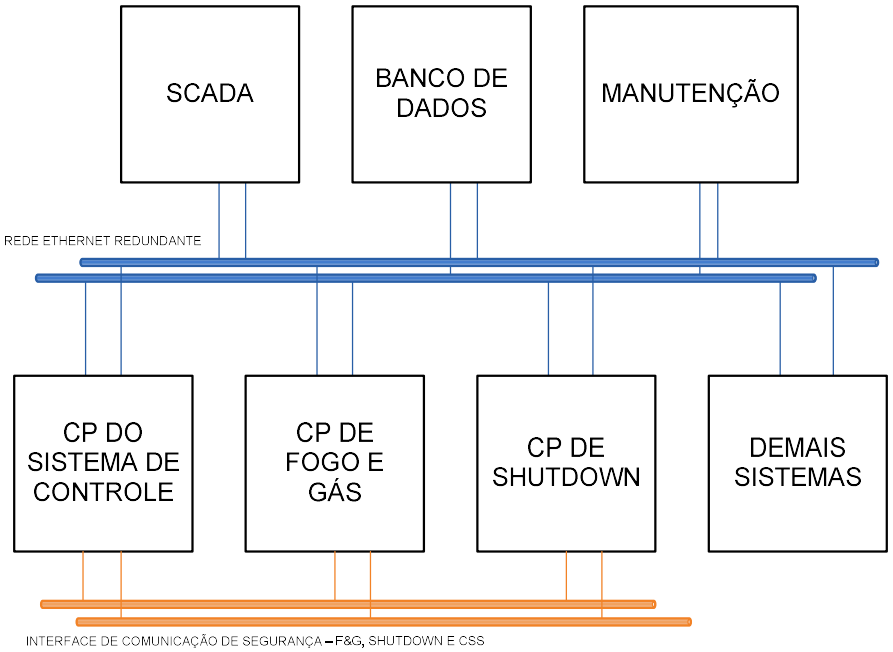
Sistemas de shutdown consistem em realizar o desligamento seguro de processos industriais em caso de falhas em equipamentos e ou processos, neste caso, plataformas de petróleo em alto mar. Nestas instalações, estes sistemas são divididos em shutdown dos sistemas de utilidades composto por geração de energia, tratamento de água, ar condicionado, controle de água de lastro, entre outros, situados no casco – *Hull* da embarcação, e shutdown do processo produtivo – *Top Side*, composto por tratamento primário do óleo, separação água/óleo, tratamento de água, sistema de carregamento de navio entre outros.

Sistemas de fogo e gás - F&G são responsáveis pela detecção e alarme de incêndio, combate à incêndio por água ou CO_2, sistemas de exaustão de segurança, sistema de alarme de abandono, onde os sistemas de shutdown trabalham em sincronismo com o de F&G, pois um sinistro qualquer pode acarretar um desligamento parcial ou total de uma planta industrial.

Tipicamente estes sistemas de segurança requerem equipamentos certificados com marcação SIL1, SIL2 ou SIL3, em alguns casos não existe a exigência da certificação, mas utilizam-se equipamentos com tais marcações por estes equipamentos serem projetados e certificados para segurança funcional. Além das exigências de segurança funcional, é exigida alta disponibilidade nestas aplicações, nó mínimo 99,5%, sendo requerida redundância entre demais técnicas para aumento de confiabilidade destes conjuntos. Estes conjuntos de controladores são divididos por função, ou seja um conjunto para operar o sistema de controle, um conjunto para operar o sistema de fogo e gás e o terceiro para operação do sistema de Shutdown, ambos possuem processamento isolado mas se comunicam em uma rede de controle

de alta velocidade com canais de comunicação dedicados entre si utilizando sistemas SCADA como interface com operadores. A Figura 28 ilustra a simplificação deste sistema.

Figura 29 - Arquitetura típica de um sistema de controle de plataforma de petróleo.



Fonte: do autor.

5.1 LISTA DE PONTOS SIF

De acordo com o estudo de caso, as funções instrumentas de segurança correspondentes aos sistemas de fogo e gás e shutdown de uma plataforma de petróleo, tipicamente são compostas de uma grande quantidade de entradas e saídas discretas e uma pequena quantidade se entradas e saídas analógicas, pois são compostos geralmente de chaves de alarme e comandos digitais de abertura, fechamento ou desligamento provenientes de níveis alto e muito alto das variáveis do processo.

A lista de pontos de entradas e saídas – I/O abaixo é uma média das funções instrumentadas de segurança de plataformas de petróleo de médio porte, a origem das informações não pode ser revelada por questões estratégicas da empresa fornecedora dos dados.

Tabela 6 - Lista de pontos de sistemas de segurança de uma plataforma de petróleo.

SIL Requerido	DI-SEG	DO-SEG	AI-SEG	AO-SEG	%
Total de pontos	1651	1496	205	70	
SIL 3	67	60	9	3	4%
SIL 2	331	300	41	14	20%
SIL 1	661	599	82	28	40%
Não classificado	592	537	73	25	36%

Nota-se uma grande concentração de pontos com níveis de classificação até SIL 2 devido ao esforço de projetar medidas compensatórias levantadas nos estudos iniciais LOPA e HAZOP na tentativa de mitigar riscos que envolvam pessoas, processos e ambiente, neste caso 96% das funções instrumentadas de segurança são classificadas até SIL 2.

5.2 ESTIMATIVA DE CUSTO DO SISTEMA DE SEGURANÇA

O levantamento de custo foi realizado a partir de lista de preços de mercado dos principais fornecedores de controladores programáveis standard e de segurança atuantes no mercado nacional, entre eles, Altus, Siemens, Hima, Rockwell. Foram estudadas as arquiteturas de hardware de cada fabricante e foram projetadas arquiteturas equivalentes dos equipamentos de cada fabricante. De posse das listas de preço, foram realizadas as médias de preço para as arquiteturas de votação 1oo1, 1oo2 e 1oo1D destes fabricantes para manter o sigilo de valor individual de cada solução.

As arquiteturas 1oo1 e 1oo2 foram projetadas com os controladores standard, e a arquitetura 1oo1D com a plataforma certificada destes fabricantes com nível de integridade de segurança até SIL 3 conforme o quantitativo e classificação apresentados na lista de pontos da tabela 6.

As listas de preços foram orçadas em setembro de 2018 com cotação em dólar americano e foi realizada uma atualização monetária desta moeda para a data atual deste trabalho.

A tabela 7 apresenta a média de valor dos fabricantes de referência para a arquitetura 1oo1.

Tabela 7 - Relação de valor do CLP standard com arquitetura 1oo1.

Componente	Descrição	Quantidade	Custo total
B09	Backplane	1	
PWR	Power	1	
CPU	CPU	1	
PBM	PROFIBUS Master	1	
ETH	Ethernet Card	1	
PBS	PROFIBUS Slave	23	
DI	Digital Input	104	
AI	Analog Input	26	
DO	Digital Output	94	
AO	Analog Output	10	
			$ 136.374,72

A Tabela 8 apresenta a média de valor dos fabricantes de referência para a arquitetura 1oo2.

Tabela 8 - Relação de valor do CLP standard com arquitetura 1oo2.

Componente	Descrição	Quantidade	Custo total
B09	Backplane	2	
PWR	Power	2	
CPU	CPU	2	
PBM	PROFIBUS Master	4	
ETH	Ethernet Card	4	
PBS	PROFIBUS Slave	92	
DI	Digital Input	208	
AI	Analog Input	52	
DO	Digital Output	188	
AO	Analog Output	20	
			$ 456.581,85

A Tabela 9 apresenta a média de valor dos fabricantes de referência para a arquitetura 1oo1D.

Tabela 9 - Relação de valor do CLP SIL com arquitetura 1oo1D.

Componente	Descrição	Quantidade	Custo total
B09	Backplane	2	
PWR	Power	2	
CPU	SCPU	2	
PBM	PROFISAFE Master	4	
ETH	Ethernet Card	4	
PBS	PROFISAFE Slave	23	
DI	Digital Input	104	
AI	Analog Input	26	
DO	Digital Output	94	
AO	Analog Output	10	
			$ 794.186,22

Conforme apresentado nas tabelas 7 a 9 existe uma diferença significativa de custo em relação às arquiteturas estudadas, ,onde o projeto do CLP SIL para atendimento até SIL 3 apresentou custo superior a cinco vezes a arquitetura 1oo1 com controlador standard e maior que setenta por cento superior a arquitetura 1oo2 com controladores standard conforme apresentado na Tabela 10.

Tabela 10 - Comparativo de custo CLP standard versus CLP SIL.

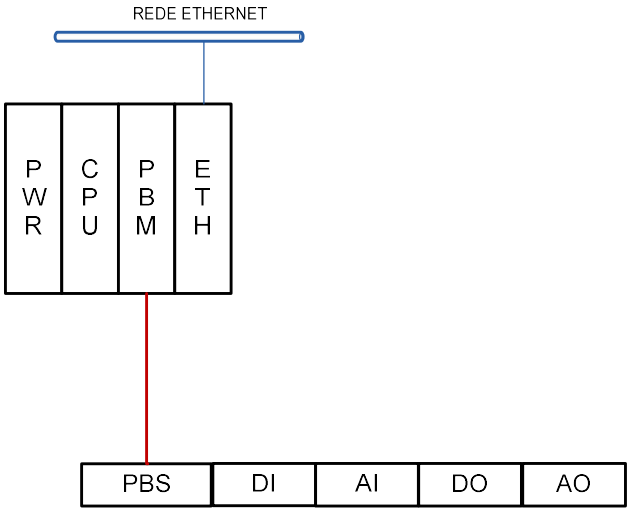
Arquitetura	Custo Total	Diferença
1oo1	$ 136.374,72	83%
1oo2	$ 456.581,85	43%
1oo1D	$ 794.186,22	

5.3 TESTES REALIZADOS

De acordo com os cálculos de probabilidade de falhas foram analisados dois cenários de arquiteturas de um determinado controlador standard de um fabricante nacional com o objetivo de aplicação nos sistemas Shutdown e fogo e gás de FPSOs, um com uma arquitetura 1oo1 e sistema de I/O distribuído interligado ao chassi de processamento e comunicação através de protocolo PROFIBUS DP, conforme Figura 30 e o segundo cenário com o mesmo modelo de equipamento, porém com redundância do tipo *Hot Standby* de CPU, fontes, módulos de

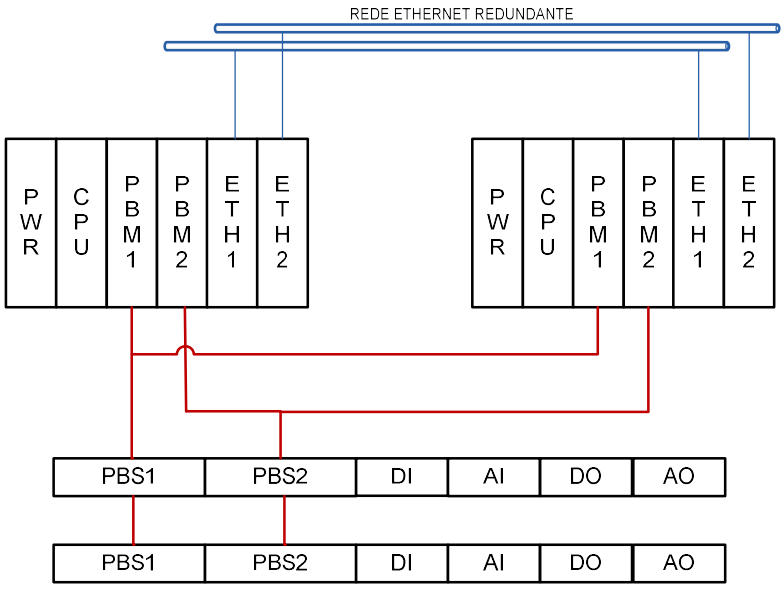
comunicação em chassis separados e arquitetura 1oo2 para os canais de I/O, conforme Figura 31.

Figura 30 - Controlador standard com arquitetura 1oo1.



Fonte: do autor.

Figura 31 - Controlador standard com arquitetura 1oo2.

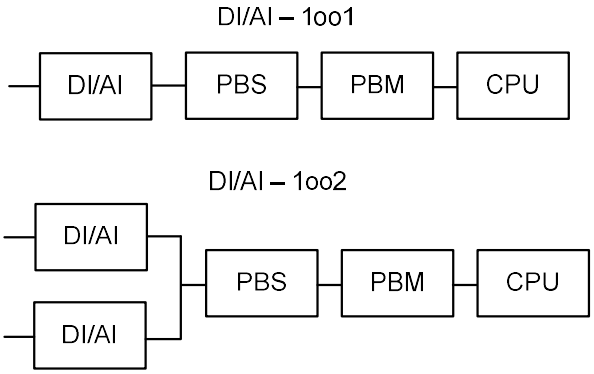


Fonte: do autor.

De acordo com o capítulo 5 deste trabalho foram realizados os cálculos PFDavg para ambos os casos com intervalos de teste de um, dois, cinco, dez e vinte anos, conforme IEC 61508.

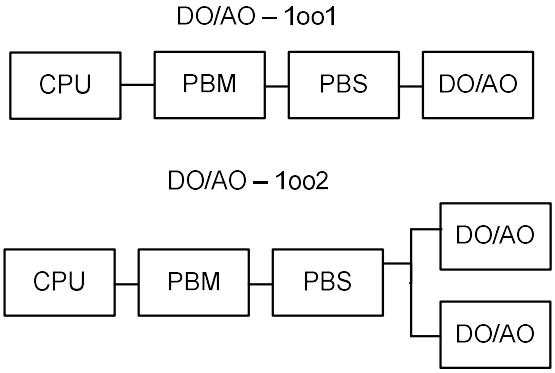
Para obter os resultados, os circuitos foram subdivididos por circuito de entrada e circuito de saída, tanto para os canais de entradas digitais e analógicos - DI/AI quanto para canais de saídas digitais e analógicas - DO/AO, em ambos arranjos, 1oo1 e 1oo2, a Figura 32 ilustra o diagrama RBD do sistema para leitura dos canais de entrada e a Figura 33 o mesmo diagrama para os canais de saída.

Figura 32 - Diagrama RBD para circuitos DI/AI com arquitetura 1oo1 e 1oo2.



Fonte: do autor.

Figura 33 - Diagrama RBD para circuitos DO/AO com arquitetura 1oo1 e 1oo2.



Fonte: do autor.

De posse de todos os diagramas RBD foram calculados todos os parâmetros de cada módulo do sistema e dos conjuntos 1oo1 e 1oo2 para os circuitos de entrada e saída digitais e analógicos. No caso da arquitetura "*Hot-Standby*" dos chassis de processamento e comunicação, foram considerados como arranjo 1oo1 pois os mesmos não utilizam-se da técnica de votação, ou seja, as informações são processadas somente no equipamento que está

ativo, em modo *"Hot"* enquanto o chassi que está em modo *"Standby"*, coleta informações de sincronismo, diagnósticos e estados dos canais de entrada e saída mantendo-se pronto para assumir o processo em caso de falha crítica de algum componente do conjunto que está operante. Este tipo de arquitetura aumenta a disponibilidade do sistema, mas não eleva seu nível de integridade de segurança. Este arranjo é considerado "tolerante a falhas".

Inicialmente foram calculados todos os parâmetros de confiabilidade e taxa de falhas de cada módulo do sistema de acordo com a metodologia descrita no capítulo 5. A Tabela 11 apresenta o resultado de cálculo de todos os módulos comuns ao sistema nos dois arranjos.

Tabela 11 - Memorial de cálculo dos módulos utilizados no estudo de caso.

Componente	Descrição	MTBF (h)	λ	λs, λd	DC(%)	λdd	β(%)	SFF	λdu
B09	Backplane	2436960	4,10E-07	2,05E-07	0	0,00E+00	10	0,50000	2,05E-07
PWR	Power	44483976	2,25E-08	1,12E-08	60	6,74E-11	10	0,50300	4,50E-09
CPU	CPU	15255816	6,55E-08	3,28E-08	60	1,97E-10	10	0,50300	1,31E-08
PBM	PROFIBUS Master	8886990	1,13E-07	5,63E-08	60	3,38E-10	10	0,50300	2,25E-08
ETH	Ethernet Card	36203064	2,76E-08	1,38E-08	60	8,29E-11	10	0,50300	5,52E-09
PBS	PROFIBUS Slave	41693078,4	2,40E-08	1,20E-08	60	7,20E-11	10	0,50300	4,80E-09
DI	Digital Input	46341216	2,16E-08	1,08E-08	70	7,55E-11	10	0,50350	3,24E-09
AI	Analog Input	112302024	8,90E-09	4,45E-09	60	2,67E-11	10	0,50300	1,78E-09
DO	Digital Output	32331928	3,09E-08	1,55E-08	70	1,08E-10	10	0,50350	4,64E-09
AO	Analog Output	40189944	2,49E-08	1,24E-08	60	7,46E-11	10	0,50300	4,98E-09

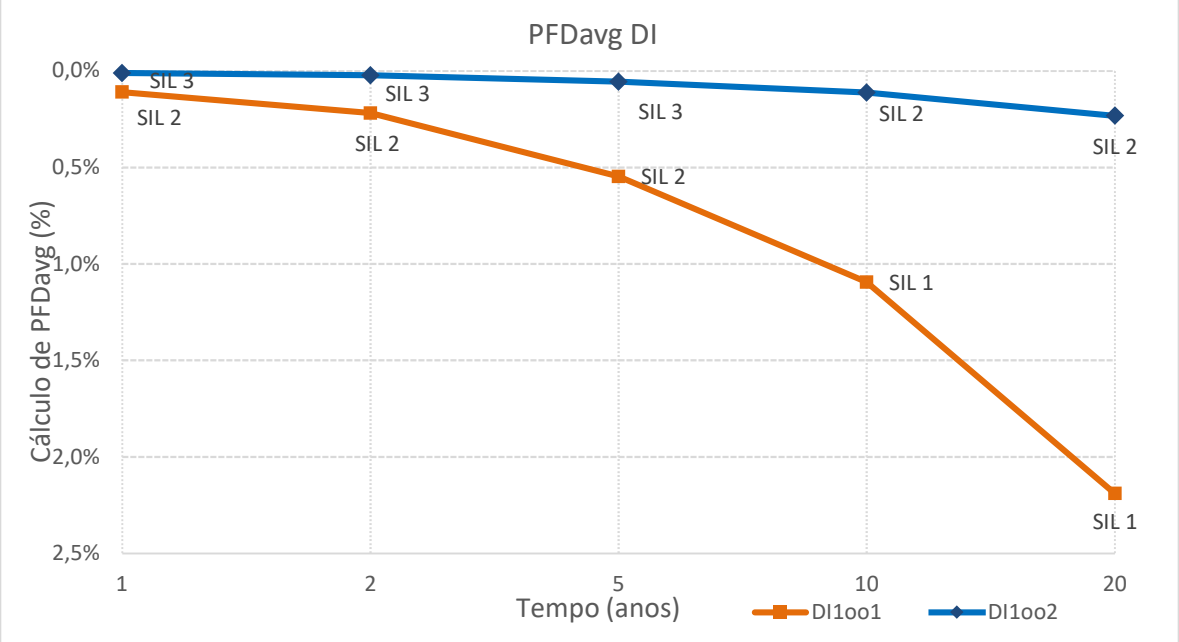
Após o cálculo dos módulos comuns foi desenhado o RBD do circuito de entrada digital até o a CPU do sistema nos arranjos 1oo1 e 1oo2 e calculada as probabilidades de falhas na demanda para intervalos de testes de 1 a 20 anos conforme tabela 12.

Tabela 12 - PFD_{avg} para DI arranjos 1oo1 e 1oo2.

Tempo	1 ano	2 anos	5 anos	10 anos	20 anos
Componente	**PFD_{avg1}**	**PFD_{avg2}**	**PFD_{avg5}**	**PFD_{avg10}**	**PFD_{avg20}**
DI1oo1	1,09E-03	2,19E-03	5,47E-03	1,09E-02	2,19E-02
DI1oo2	1,10E-04	2,21E-04	5,58E-04	1,13E-03	2,33E-03

Conforme Figura 34 o comparativo dos arranjos 1oo1 e 1oo2 nos intervalos de testes até vinte anos, o a arquitetura 1oo1 parte de SIL 2 e degrada-se para SIL 1 a partir de dez anos, enquanto em uma arquitetura 1oo2 parte de SIL 3 e degrada-se para SIL 2 a partir de 10 anos.

Figura 34 - Gráfico PFD_{avg} DI para intervalos de testes de 1, 2, 5 10 e 20 anos.



Fonte: do autor.

Concluído os cálculos para DI foram calculados os mesmos parâmetros para os circuitos de saídas digitais - DO com a mesma metodologia. Os resultados estão apresentados na tabela 13.

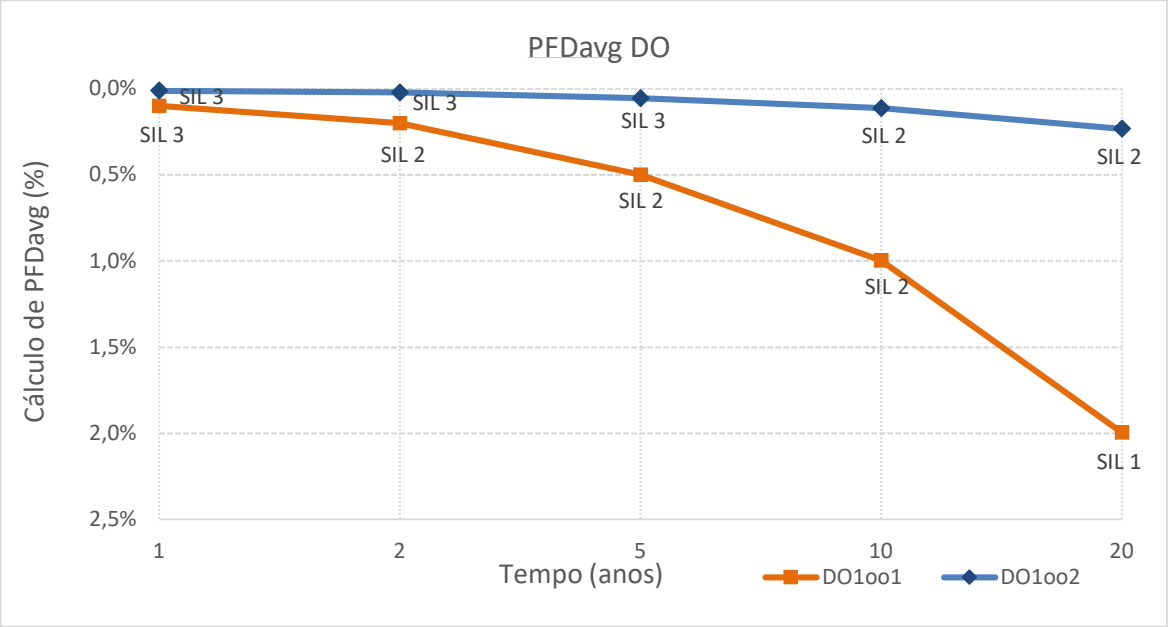
Tabela 13 - PFD_{avg} para DO arranjos 1oo1 e 1oo2.

Tempo	**1 ano**	**2 anos**	**5 anos**	**10 anos**	**20 anos**
Componente	**PFD_{avg1}**	**PFD_{avg2}**	**PFD_{avg5}**	**PFD_{avg10}**	**PFD_{avg20}**
DO1oo1	9,98E-04	2,00E-03	4,99E-03	9,98E-03	2,00E-02
DO1oo2	1,10E-04	2,21E-04	5,58E-04	1,13E-03	2,33E-03

Conforme gráfico da Figura 35, o comparativo das arquiteturas para os circuitos de saída digital apresentou desempenho de SIL 3 para SIL 2 em um ano, SIL 2 até 10 anos e SIL 1 para

20 anos de intervalo de testes no arranjo 1oo1. Em arranjo 1oo2 apresentou degradação de SIL 3 para SIL 2 a partir de 10 anos de PTI.

Figura 35 - Gráfico PFD_{avg} DO para intervalos de testes de 1, 2, 5 10 e 20 anos.



Fonte: do autor.

Repetindo os cálculos para os circuitos de entrada analógica – AI, tem-se os resultados conforme a tabela 14.

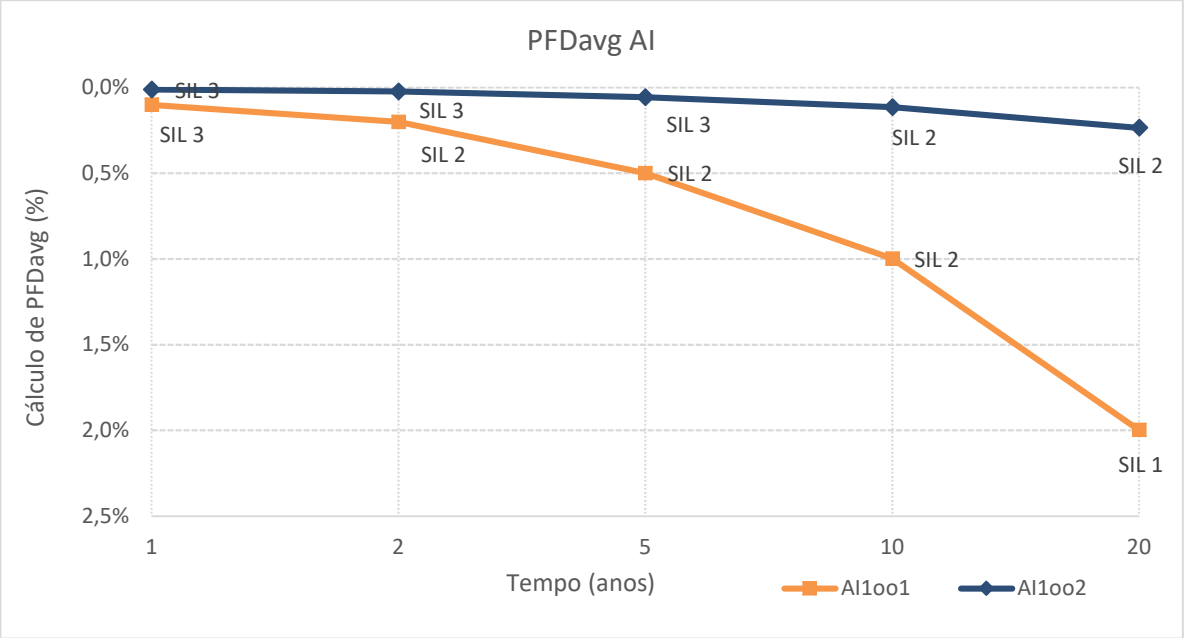
Tabela 14 - PFD_{avg} para AI arranjos 1oo1 e 1oo2.

Tempo	**1 ano**	**2 anos**	**5 anos**	**10 anos**	**20 anos**
Componente	**PFD_{avg1}**	**PFD_{avg2}**	**PFD_{avg5}**	**PFD_{avg10}**	**PFD_{avg20}**
AI1oo1	9,99E-04	2,00E-03	4,99E-03	9,99E-03	2,00E-02
AI1oo2	1,11E-04	2,23E-04	5,62E-04	1,14E-03	2,34E-03

De acordo com o gráfico da Figura 36, o comparativo das arquiteturas para os circuitos de entrada analógica - AI apresentou desempenho de SIL 3 para SIL 2 em um ano, SIL 2 para

10 anos e SIL 1 para 20 anos de intervalo de testes para arranjo 1oo1. Em arranjo 1oo2 apresentou degradação de SIL 3 para SIL 2 a partir de 10 anos de PTI.

Figura 36 - Gráfico PFD_{avg} AI para intervalos de testes de 1, 2, 5 10 e 20 anos.



Fonte: do autor.

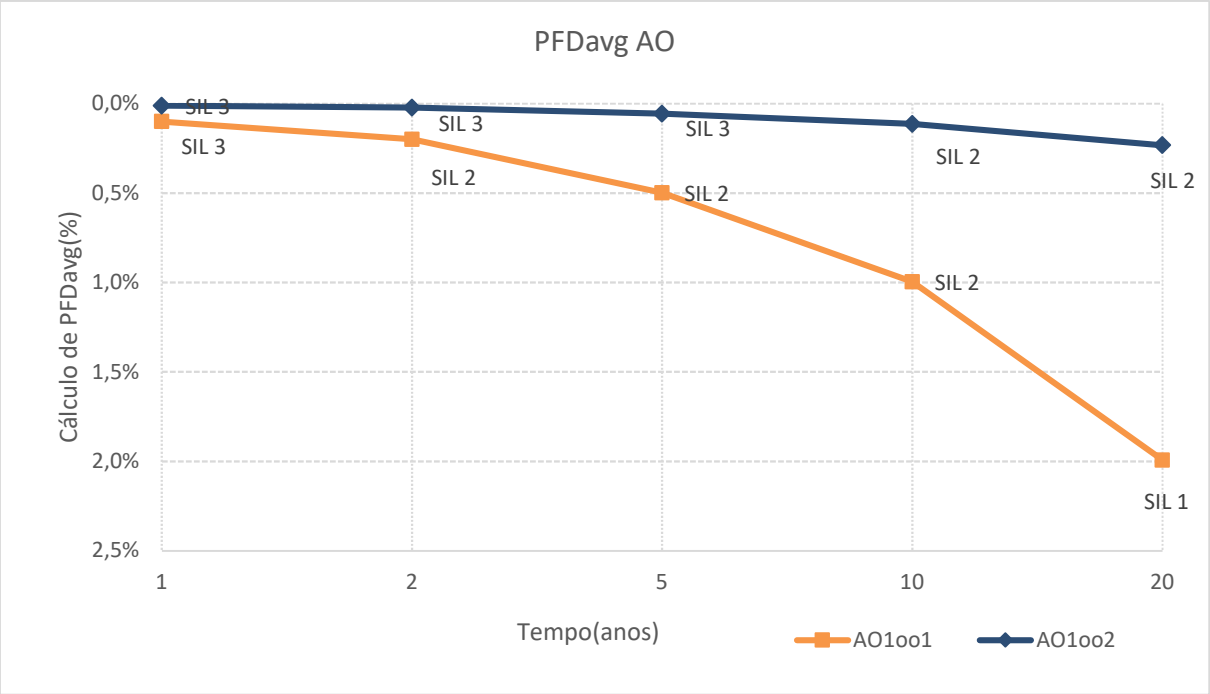
Aplicando os cálculos para os circuitos de saída analógica – AO, tem-se os resultados conforme a tabela 15.

Tabela 15 - PFD_{avg} para AO arranjos 1oo1 e 1oo2.

Tempo	**1 ano**	**2 anos**	**5 anos**	**10 anos**	**20 anos**
Componente	**PFD_{avg1}**	**PFD_{avg2}**	**PFD_{avg5}**	**$PFDa_{vg10}$**	**PFD_{avg20}**
AO1oo1	9,96E-04	1,99E-03	4,98E-03	9,96E-03	1,99E-02
AO1oo2	1,10E-04	2,21E-04	5,58E-04	1,13E-03	2,33E-03

De acordo com o gráfico da Figura 37, o comparativo das arquiteturas para os circuitos de saída analógica - AO apresentou desempenho de SIL 3 para PTI de um ano, SIL 2 para dez anos e SIL 1 para 20 anos de intervalo de testes para arranjo 1oo1. Em arranjo 1oo2 apresentou desempenho SIL 3 para PTI 5 anos e SIL 2 a partir de 10 anos.

Figura 37 - Gráfico PFD_{avg} AO para intervalos de testes de 1, 2, 5 10 e 20 anos.



Fonte: do autor.

Conforme resultados de probabilidade média de falha na demanda PFDavg dos canais digitais e analógicos apresentados nas figuras 34 a 37 pode-se concluir que ambos apresentam resultados similares de desempenho SIL nos intervalos de testes de referência da IEC 61508 devido as características do projeto dos módulos da família de produtos testados e os arranjos de arquitetura ao qual os equipamentos foram submetidos.

6 CONCLUSÕES

Os controladores programáveis dedicados à segurança de processos industriais são projetados para atuação somente em caso de falhas, diante deste fato, sua concepção de projeto exige tolerância a falhas, alta gama de diagnósticos e lógicas de controle simplificadas, onde o desempenho não é a exigência principal.

Controladores Standard possuem alta flexibilidade de arquiteturas, são projetados para possuir alto desempenho, execução de lógicas complexas e alto índice de disponibilidade.

Analisando as diferenças entre concepções de cada projeto, pode-se verificar ainda semelhanças nas soluções pois os dois tipos de controladores, apoiam-se na mesma norma no requisito conceitual (IEC61131).

Dentre as principais diferenças entre os dispositivos, pode-se destacar por parte dos controladores de segurança: maior esforço para especificação e desenvolvimento de projeto, seleção de componentes, maior preocupação por apontamento de diagnósticos e algoritmos para predição de falhas, menor gama de lógica para os programas aplicativos no intuito de redução de risco de erro de projeto de software aplicativo por parte do usuário final.

Os fabricantes utilizam métricas diferentes para validação de seus projetos nos dois casos, por exemplo, em manuais dos controladores standard são indicados os dados de confiabilidade como MTBF e MTTR assim como melhores práticas de aplicação do produto. Nos controladores de segurança a indicação por taxas de falhas e análise de probabilidade é muito mais destacada.

Neste trabalho foram utilizadas as técnicas de diagramas de blocos de confiabilidade – RBD, arquiteturas de votação, cálculos estatísticos de probabilidade média de falha na demanda PFD_{avg} como principais meios de obtenção dos resultados. Conforme os cálculos de desempenho SIL realizados na família de controladores programáveis standard comercial com arranjos de arquitetura 1oo1 e 1oo2 foram alcançadas métricas SIL 2 nos intervalos de testes -

PTI de vinte anos em todos os casos, resultados que podem contribuir para aumento de confiabilidade e mitigação de riscos de acidentes em processos de missão crítica onde a certificação pode não ser a exigência principal. A popularização desta metodologia pode contribuir com a sociedade no intuito de aumento de segurança de plantas industriais que possam adotar este trabalho como base de estudo de segurança de sua base instalada.

Para continuidade deste trabalho propõe-se buscar uma aproximação maior destes dois tipos de controladores com o objetivo de comprovar que controladores standard são capazes de executar lógicas de segurança sem comprometer determinado processo, adotando as mesmas práticas de diagnose, e verificação de análise de possíveis falhas conforme é projetado nos controladores certificados para área de segurança de processo utilizando a práticas recomendadas na IEC 61508-6 anexo C.

REFERÊNCIAS

BUKOSWKI, J.; BEURDEN, I. Impact of proof test effectiveness on safety instrument system performance. **IEEE Annual Reliability and Maintainability Symposium**, Fort Worth, v.1, n.6, p. 157-163, Jan 2009.

BRITISH STANDARDS INSTITUTION. **PD CEN ISO/TR 12489**: petroleum, petrochemical and natural gas industries: reliability modelling and calculation of safety systems. London: BSI Standards, 2016.

GOBLE, W.; CHEDDIE, H. **Safety instrument systems verification:** practical probabilistic calculations. 1st ed. Durhan: International Society of Automation, 2005.

HEALTH AND SAFETY EXECUTIVE. **Out of control:** why control systems go wrong and how to prevent failure. 2nd ed. Sheffield: HSE, 2003. Disponível em: https://www.hse.gov.uk/pubns/priced/hsg238.pdf. Acesso em: 10 mai. 2018.

GEORGIES, O.; YANG, H.; REINDL, L. Type-2 digital input and output signal conditioning circuits for industrial safety applications. *In*: IEEE INTERNATIONAL MULTI-CONFERENCE ON SYSTEMS, SIGNALS & DEVICES (SSD). 13., 2016, Leipzig. **Proceedings[…]** IEEE, 2016, p.393-400.

INTERNATIONAL ELECTROTECHNICAL COMMISSION. **IEC 61511-1 a 3**: functional safety – safety instrumented systems for the process industry sector. Geneva: IEC Publisher, 2010.

INTERNATIONAL ELECTROTECHNICAL COMMISSION. **IEC 61508-1 at 7**: functional safety of electrical/electronic/programmable electronic safety-related systems. Geneva: IEC Publisher, 2010.

INTERNATIONAL ELECTROTECHNICAL COMMISSION. **IEC 61131-1 at 9**: programmable controllers. Geneva: IEC Publisher, 2004.

INTERNATIONAL SOCIETY OF AUTOMATION. **ISA-TR84.00.02**: Safety integrity level -SIL check of safety instrumented functions. Durhan: International Society of Automation, 2015.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO 13849**: safety of machinery - safety-related parts of control systems. Geneva: Multiple, 2015.

LUNDTEIGEN, M.; RAUSAND, M. Architectural constraints in IEC 61508: do they have the intended effect? **Reliability engineering and system safety**, [S.1], v.94, n.2, p.520-525, Feb. 2009.

MANZINI, R.; REGATTIERI, A. **Maintenance for industrial systems**: Springer series in reliability engineering. 11th ed. London: Springer-Verlag, 2010.

MIYAGI, P. **Controle programável**: Fundamentos do controle de sistemas a eventos discretos. 5.ed. São Paulo. Edgard Blucher, 2015.

RÁSTOČNÝ, K.; ZDANSK, J. Specificities of safety PLC based implementation of the safety functions. **International Conference on Applied Electronics**, Bohemia, v.1, n.1, p.229-231, Sept. 2012.

RÁSTOČNÝ, K.; ŽDÁNSKY, J.; BALÁK, J. *et al*. Diagnostics of an output interface of a safety-related system with safety PLC. **Springer-Verlag Journal**, [S.1], v.99, p.1169–1178, July 2017.

RÁSTOČNÝ, K. Effects of diagnostic on the safety of a control system realised by safety PLC. **Elektro Proceedings of 11th International Conference**, Strbke Pleso, v.1, n.4, p. 462-467, July 2016.

ROCKWELL AUTOMATION. **Using ControlLogix in SIL 2 Applications**, Rev. P, 09/2018. Disponível em: https://literature.rockwellautomation.com/idc/groups/literature/documents/rm/1756-rm001_-en-p.pdf. Acesso em: 25 out. 2019.

SAMMARCO, J. Programmable electronic and hardwired emergency shutdown systems: A quantified safety analysis. **IEEE transactions on industry applications**, [S.1], v.43, n.4, p 1061-1068, 2007.

ŽDÁNSKY, J.; NAGY, P. Influence of the control system structure with safety PLC on its reliability and safety. **Elektro Proceedings of 9th International Conference**, Rajeck Teplice, v.1, n.1 May 2012, p1061 – 1068.

TORRES, E.; SRIRAMULA, S.; CELEITA, D.; RAMOS, G. Model for assessing the safety integrity level of electrical/ electronic/programmable electronic safety-related systems. **IEEE Industry Applications Society Annual Meeting**, Baltimore, v.54, n.1, p.713-720, Sept. 2019.

TORRES, E.; SRIRAMULA, S.; CELEITA, D.; RAMOS, G. Safety integrity level verification model for IED protection schemes. **IEEE Transactions on Industry Applications**, [S.1], v.1, n.1, p.1-8, Mar. 2020.

TEXAS INSTRUMENTS, **RM42L432 16 and 32 Bit RISC Flash Microcontroller**, Rev. B, 06/2015.
Disponível em: http://www.ti.com/lit/ds/symlink/rm42l432.pdf?ts=1588511436900. Acesso em: 13 jul. 2019.

YOE, C. **Principles of risk analysis**. Boca Raton: CRC Press, 2012.