UNIVERSIDADE ESTADUAL PAULISTA
"JÚLIO DE MESQUITA FILHO"
Campus de Bauru

CAIO CESAR POLICELLI AMALFI

Ferramenta de Análise e Projeto de Sistemas Instrumentados de Segurança em Automação Industrial

Bauru

2017

CAIO CESAR POLICELLI AMALFI

Ferramenta de Análise e Projeto de Sistemas Instrumentados de Segurança em Automação Industrial

Dissertação apresentada ao Programa de Pós-Graduação em Engenharia Elétrica da Faculdade de Engenharia Elétrica da Universidade Estadual Paulista “Júlio de Mesquita Filho” para obtenção do título de Mestre em Engenharia Elétrica.

Área de Concentração: Automação

Linha de Pesquisa: Mecatrônica

Orientador: Prof. Dr. Eduardo Paciência Godoy

Bauru – SP

2017

Policelli Amalfi, Caio Cesar.
Ferramenta de Análise e Projeto de Sistemas Instrumentados de Segurança em Automação Industrial / Caio Cesar Policelli Amalfi, 2017
186 f.

Orientador: Eduardo Paciência Godoy

Dissertação (Mestrado)–Universidade Estadual Paulista. Faculdade de Engenharia, Bauru, 2017

1. Automação. 2. Sistemas de Segurança. 3. Análise e Quantificação de Riscos. I. Universidade Estadual Paulista. Faculdade de Engenharia. II. Título.

UNIVERSIDADE ESTADUAL PAULISTA

Câmpus de Bauru

ATA DA DEFESA PÚBLICA DA DISSERTAÇÃO DE MESTRADO DE CAIO CESAR POLICELLI AMALFI, DISCENTE DO PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA ELÉTRICA, DA FACULDADE DE ENGENHARIA - CÂMPUS DE BAURU.

Aos 27 dias do mês de outubro do ano de 2017, às 14:00 horas, no(a) Instituto de Ciência e Tecnologia de Sorocaba-UNESP, reuniu-se a Comissão Examinadora da Defesa Pública, composta pelos seguintes membros: Prof. Dr. EDUARDO PACIÊNCIA GODOY - Orientador(a) do(a) Engenharia de Controle e Automação / Instituto de Ciência e Tecnologia/UNESP/Sorocaba, Prof. Dr. IVANDO SEVERINO DINIZ do(a) Engenharia de Controle e Automação / Instituto de Ciência e Tecnologia/UNESP/Sorocaba, Prof. Dr. DENNIS BRANDÃO do(a) Departamento de Engenharia Elétrica e da Computação / Universidade de São Paulo - São Carlos, sob a presidência do primeiro, a fim de proceder a arguição pública da DISSERTAÇÃO DE MESTRADO de CAIO CESAR POLICELLI AMALFI, intitulada **FERRAMENTA DE ANÁLISE E PROJETO DE SISTEMAS INSTRUMENTADOS DE SEGURANÇA EM AUTOMAÇÃO INDUSTRIAL**. Após a exposição, o discente foi arguido oralmente pelos membros da Comissão Examinadora, tendo recebido o conceito final: APROVADO _____. Nada mais havendo, foi lavrada a presente ata, que após lida e aprovada, foi assinada pelos membros da Comissão Examinadora.

Prof. Dr. EDUARDO PACIÊNCIA GODOY

Prof. Dr. IVANDO SEVERINO DINIZ

Prof. Dr. DENNIS BRANDÃO

AGRADECIMENTOS

Agradeço primeiramente a Deus por colocar diversas pessoas boas no meu caminho.

A meus pais Jeferson e Maria Helena que sempre acreditaram em mim e me deram todo apoio.

Aos meus amigos César Negri, Wesley Souza, Gabriel Policelli e Augusto Alonso por me ajudarem nos momentos difíceis durante a execução do meu trabalho de mestrado.

Ao meu orientador, professor doutor Eduardo Paciência Godoy, pela paciência, pelo apoio no desenvolvimento do projeto e por ter me dado a oportunidade de realizar um sonho de ser pós-graduando.

Agradeço, também, à CAPES pelo apoio financeiro que foi muito importante durante os períodos de pesquisa e revisão bibliográfica.

“Se o dinheiro for a sua esperança de independência, você jamais a terá. A única esperança verdadeira consiste numa reserva de sabedoria, de experiência e de competência”

Henry Ford

RESUMO

A alta complexidade atrelada às necessidades de segurança e confiabilidade dos processos industriais têm demandado a implantação de sistemas automáticos de segurança. Esse sistema, conhecido como Sistema Instrumentado de Segurança (SIS), é responsável pela segurança operacional do processo dentro de limites seguros através da monitoração de valores e parâmetros quando houver condições de risco. Os SISs são concebidos com diferentes Níveis de Integridade de Segurança (SIL) de acordo com o risco do processo. O desafio na implantação de um SIS é que seu procedimento de projeto é complexo e pouco difundido, além de existirem diversos métodos de cálculo e análise de riscos aceitos pelas normas de segurança. A motivação para este trabalho foi automatizar e auxiliar o projeto de SIS no que diz respeito à redução da quantidade de pessoas envolvidas e de tarefas manuais que podem causar erros, à padronização e simplificação dos procedimentos e cálculos necessários e também à diminuição do tempo de projeto, promovendo um aumento na eficiência e redução dos custos envolvidos. O objetivo é desenvolver uma ferramenta de análise e projeto de SIS, com programação voltada para Web, capaz realizar um estudo de riscos e falhas de um processo industrial e calcular um valor adequado para a seleção do SIL requerido para implantação de um sistema de segurança. A ferramenta é composta de quatro módulos: o Estudo de riscos e falhas usando a técnica HAZOP, a Quantificação dos riscos e criação de árvores de falhas; a Obtenção do SIL através da Análise da Árvores de Falhas (AAF) e a Definição de uma Função Instrumentada de Segurança (SIF) apropriada para o SIL calculado. A ferramenta desenvolvida é inovadora ao automatizar e combinar no mesmo ambiente todos os procedimentos necessários para a análise e projeto de SIS. Diversos casos de estudo de projeto de SIS, sendo um caso industrial real e outros da literatura, são utilizados para teste e validação dos módulos da ferramenta afim de demonstrar sua eficiência, flexibilidade de uso e exatidão dos resultados obtidos com a sua aplicação.

Palavras-chave: *Confiabilidade, Falhas, HAZOP, Função Instrumentada de Segurança (SIF), Nível de Integridade de Segurança (SIL).*

ABSTRACT

The high complexity tied to the reliability and security requirements of industrial processes has demanded the deployment of automatic safety systems. This system is known as Safety Instrumented Systems (SIS) and is responsible for the process operational safety within safe limits through the monitoring of values and parameters when there are conditions of risk. The SIS is designed with different Safety Integrity Levels (SIL) according to the process risk. The challenge in the deployment of SIS is that the design procedure is complex and not well known, and there are many calculation and risk analysis methods accepted by the safety standards. The motivation was automating and assisting in the design of SIS with regard to the reduction of people involved and manual tasks that may cause errors, the standardization and simplification of procedures and calculations needed and the reduction in project time, promoting an increase in efficiency and reducing the costs. The objective was developing an analysis and design tool for SIS, with web-based programming, capable of performing a study of the risks and failures of an industrial process and calculating an adequate value for the selection of the Safety Integrity Level (SIL) required for the implementation of the safety system. The tool is comprised of four modules: the Study of risks and failures using the HAZOP technique, the Quantification of risks and creation of fault trees; the SIL calculation through the Fault Tree Analysis (FTA) and the Definition of a Safety Instrumented Function (SIF) suitable for SIL calculated. The developed tool is innovative by systemizing and combining in the same environment all the procedures required for the analysis and design of SIS. Several case studies of SIS design are used for testing and validation of the tool modules, considering a real industrial case and others cases in the literature, in order to demonstrate the efficiency, flexibility of use, and accuracy of the results obtained with the tool application.

Keywords: *Reliability, Failures, HAZOP, Safety Integrity Function (SIF), Safety Integrity Level (SIL).*

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

AAF	*Análise de Árvore de Falhas*
AIChE	*American Institute of Chemical Engineers* (Instituto Americano de Engenheiros Químicos)
ANSI	*American National Standards Institute* (Instituto Nacional Americano de Normas)
APP	*Análise Preliminar de Perigo*
BCPS	*Basic Control Process System* (Sistema Básico de Controle de Processo)
BMS	*Burner Management System* (Sistema de Gerenciamento de Caldeiras)
CCPS	*Center for Chemical Process Safety* (Centro para Segurança de Processos Químicos)
DDCS	*Digital Distributed Control Systems* (SDCD – Sistemas Digitais de Controle Distribuído)
ESD	*Emergency Shutdown System* (Sistema de Parada de Emergência)
FAR	*Fatal Accident Rate* (Taxa de Acidente Fatal)
F&G	*Fire and Gas* (Sistema Fogo e Gás)
FMEA	*Failure Modes and Effects Analysis* (Análise de Modos de Falhas e Efeitos)
FMEDA	*Failure Modes, Effects and Diagnostic Analysis* (Análise de Modos de Falhas, Efeitos e Diagnósticos)
FS	*Functional Safety* (Segurança Funcional)
HAZOP	*Hazard and Operative* (Riscos e Operabilidade)
HFT	*Hardware Failure Tolerance* (Tolerância de Falha de Hardware)
IEC	*Internacional Electrotechnical Commission* (Comissão Eletrotécnica Iternacional)
ISA	*Internacional Society of Automation* (Sociedade de Automação Internacional)
NFPA	*National Fire Protection Association*(Associação Nacional de Proteção contra Incêndios)
PFD	*Probability of Failure on Demand* (Probabilidade de Falha em Demanda)
PSD	*Partial Shutdown System* (Sistema de Parada Parcial)
RRF	*Risk Reduction Factor* (Fator de Redução de Risco)
SFF	*Safe Failure Fraction* (Índice de Falha Segura)

SIF	*Safety Instrumented Function* (Função Instrumentada de Segurança)
SIL	*Safety Integrity Level* (Nível de Integridade de Segurança)
SIS	*Safety Instrumented System* (Sistema Instrumentado de Segurança)

SUMÁRIO

1 INTRODUÇÃO

1.1 JUSTIFICATIVA

A automação é uma realidade consolidada dentro de ambientes industriais, reduzindo os custos da produção e aumentando tanto a qualidade quanto a competitividade das empresas. Atualmente, devido à crescente utilização da automação dentro do ambiente industrial, sistemas de segurança específicos tornaram-se indispensáveis para assegurar o desempenho e integridade das plantas e das malhas de controle (CATELANI et al., 2012). Este sistema de segurança, comumente denominado de Sistema Instrumentado de Segurança (*SIS – Safety Instrumented System*), consiste em um conjunto de métodos de engenharia, hardware e software, especialmente desenvolvidos para prevenir e mitigar possíveis falhas e riscos capazes de afetar a integridade dos equipamentos, dos funcionários envolvidos e até mesmo do meio ambiente (IEC 61511-MOD, 2014).

Esta recente conscientização das indústrias a respeito do uso do SIS é resultante das tragédias ocorridas nas últimas décadas. Desde a catástrofe de Bhopal, em 1984 na Índia, na planta industrial de pesticidas da multinacional americana *Union Carbide*, com aproximadamente 15 mil mortos pelo vazamento de quarenta toneladas de gases tóxicos (GREENPEACE, 2002), as atenções foram voltadas ao SIS que poderia ter evitado o acidente. Atualmente, as discussões sobre o assunto focam no cumprimento das normas de segurança de processos industriais e de como tornar o projeto de tais sistemas de segurança, que possuem uma programação lógica com cálculos matemáticos complexos, mais simples ao projetista. A atitude empresarial com isso é alterada passando a valorizar o investimento em sistemas de segurança, agora responsáveis pela economia decorrente da prospecção preliminar de problemas eminentes (CASSIOLATO, 2010).

Um SIS tem por finalidade mitigar os riscos e implantar uma instrumentação e controle adicionais para segurança operacional em processos, tornando as plantas e suas malhas capazes de entrarem em falha segura, independente do sistema de controle tradicional (SUMERS, 2013). Essa responsabilidade é designada por alguns critérios como:

- Responder às condições perigosas que podem existir na planta;

- Se nenhuma ação for tomada pelo sistema de controle tradicional, agir imediatamente para evitar riscos maiores à integridade geral do processo;

- Se uma ação for tomada, atuar para prevenir outros riscos ou consequências.

Um SIS desencadeia ações automáticas para manter, ou fazer regressar, um processo ou instalação a um estado seguro, na presença de condições anormais. O SIS pode desencadear uma ou várias funções de proteção, contra os vários riscos de processo num processo ou planta. Os SISs são concebidos com diferentes Níveis de Integridade de Segurança (*SIL – Safety Integrity Level*), de acordo com o risco do processo. Quanto maior o SIL, maior a probabilidade de existirem componentes múltiplos e redundantes (por ex. mais que um sensor, controlador ou elemento final), testes mais rigorosos e exigentes requisitos de gestão. O SIL é calculado através de uma Probabilidade de Falha sob Demanda (PFD), isto é, a possibilidade de um sistema falhar quando o sistema de segurança necessitar ser usado por uma falha detectada. Para a aplicação de um SIS é fundamental o entendimento quanto aos riscos do processo e analisar os riscos baseados em consequência e probabilidade. Portanto, é necessário um estudo do processo de construção de um SIS, analisando todos os procedimentos descritos pelas normas, englobando todas as fases de desenvolvimento.

No entanto, o projeto e implementação de um SIS, por falta de investimentos e inovação, enfrenta algumas dificuldades e desafios como (SOKOLOV, 2015):

- O grande número de pessoas envolvidas pode causar confusão no desenvolvimento do SIS devido a uma interpretação diversa dos riscos do processo;

- O cálculo manual do nível de integridade de segurança pode gerar erros que influenciam diretamente na construção do SIS;

- A especificação e implantação do sistema de segurança requerido para atendimento do nível de segurança necessário;

- A manutenção do sistema de segurança funcional durante todo o ciclo de vida da planta.

Adicionalmente, é importante ressaltar que mesmo com toda tecnologia existente, a análise de riscos de um processo e o projeto do SIS ainda é feito, em sua maioria, separadamente e sem uso de ferramentas automáticas (NAIMAN, 2015). As poucas ferramentas computacionais existentes para auxílio na análise de riscos e projeto de SIS

são programas proprietários exclusivos, os quais não são distribuídos livremente, extremamente caros e de difícil acesso a projetistas de pequenas empresas. Tal fato tem norteado a exigência por uma nova abordagem para a análise e projeto de SIS, tendo em vista que se tratam de procedimentos normativos, envolvendo diversas pessoas e utilizando cálculos matemáticos que se não seguidos corretamente podem levar a uma implementação equivocada (NAIMAN, 2014).

Tendo isto como base, esta dissertação tem a intenção de gerar uma contribuição para a pesquisa brasileira dentro do escopo da automação industrial, através do desenvolvimento de uma ferramenta computacional que automatize as análises e os cálculos para construção desses sistemas de segurança. Essa ferramenta de análise e projeto de SIS auxilia principalmente no que diz respeito à redução da quantidade de pessoas envolvidas e de tarefas manuais que podem causar erros, à padronização e simplificação dos procedimentos e cálculos necessários e também à diminuição do tempo de projeto de um SIS, promovendo um aumento na eficiência e redução dos custos envolvidos com esta tarefa.

1.2 OBJETIVO

O objetivo deste trabalho foi desenvolver uma ferramenta de análise e projeto de SIS, com programação voltada para Web, capaz de realizar um estudo de riscos e falhas de um processo industrial e calcular um valor para a seleção do Nível de Integridade de Segurança (SIL). As principais tarefas realizadas por esta ferramenta são:

- Estudo de Riscos e Falhas usando a técnica HAZOP;
- Quantificação dos riscos e Criação de árvores de falhas com suas respectivas funções lógicas;
- Obtenção do Nível de Integridade de Segurança (SIL) através da Análise da Árvores de Falhas (AAF);
- Definição de uma Função Instrumentada de Segurança (SIF) apropriada para o SIL calculado.

1.3 ESTRUTURA E CONTEÚDO

A estrutura deste trabalho ficou dividida em 7 capítulos considerando esta introdução e desconsiderando as referências bibliográficas e os anexos.

O capítulo 2 trata da revisão conceitual, todos os conceitos importantes para o entendimento do trabalho, como as normas de segurança funcional, os estudos de falhas e riscos conhecidos, sistemas instrumentados de segurança, nível de integridade de segurança e função instrumentada de segurança.

O capítulo 3 traz a revisão bibliográfica, buscando as mais relevantes pesquisas que já foram publicadas acerca do tema, os métodos de análise de riscos existentes em estudo atualmente e as ferramentas computacionais disponíveis para o auxílio de projetos de sistemas instrumentados de segurança.

O capítulo 4 apresenta a proposta da ferramenta desenvolvida no trabalho, toda a arquitetura contendo as entradas e saídas de cada módulo, a metodologia utilizada para a criação do software e a demonstração de todos os cálculos envolvidos.

O capítulo 5 discorre sobre a descrição detalhada da ferramenta, como é o funcionamento, as telas, os dados a serem cadastrados. Aqui também é feita a validação da ferramenta Web desenvolvida utilizando para isso um projeto real anteriormente elaborado.

O capítulo 6, por sua vez, apresenta e discute os resultados obtidos com a aplicação da ferramenta de SIS desenvolvida para casos de estudo reais da indústria de processos disponíveis na literatura relacionado ao tema.

Por fim, o capítulo 7 apresenta as considerações finais e as conclusões obtidas com a elaboração do trabalho.

2 CONCEITOS FUNDAMENTAIS

2.1 NORMAS DE SEGURANÇA FUNCIONAL

Atualmente o conceito de segurança é de real importância para o projeto de sistemas automatizados, uma vez que tal definição expressa a ausência de riscos inadmissíveis causados por danos físicos, à saúde das pessoas direta e indiretamente, às propriedades e até mesmo ao ambiente (OLIVEIRA, 2003). A presença de situações perigosas no ambiente industrial estimula a crescente formação e treinamento dos trabalhadores para que estes saibam como agir no caso do acontecimento de eventos indesejados.

Neste contexto, a segurança funcional se encaixa também como um fundamento necessário para o meio industrial. A segurança funcional é a parte do aspecto de segurança da qual depende um sistema ou um equipamento em operação correta com relação às respostas e às entradas, objetivando sempre alcançar a completa não existência de riscos que podem ser causados por uma máquina e/ou sistema (SILVA, 2006).

Algumas aplicações industriais exigem o uso de equipamentos especialmente projetados para uma determinada funcionalidade, os quais diferem da especificação normal de um projeto. Nessas aplicações, locais onde a presença de gases, vapores, líquidos e pós inflamáveis podem gerar risco de incêndio ou explosão, pela existência de atmosferas potencialmente explosivas. Esses locais nas instalações industriais são chamados de áreas Classificadas (OLIVEIRA,2003).

Equipamentos de segurança são equipamentos utilizados em aplicações industriais de controle e automação onde a segurança funcional é o fator preponderante. A especificação de equipamentos para operação em áreas classificadas, depende primeiramente da análise do grau de risco dos locais de instalação dos equipamentos eletroeletrônicos. A segurança intrínseca procura garantir que instrumentos e circuitos de baixa tensão em áreas classificadas não liberem energia suficiente para a ignição de gases e elementos presentes nesta atmosfera.

Perdas de vidas humanas, de instalações, de equipamentos e de produção, bem como a contaminação do meio ambiente, contribuíram para a evolução das normas, de regulamentos e para o desenvolvimento de sistemas de segurança, segundo Finkel et al (2006). Além destes fatores, danos à imagem e eventuais multas representam elevados

custos que viabilizam os custos do ciclo de vida do SIS (GRUHN; CHEDDIE, 2006). O desenvolvimento de normas e padrões de segurança pela indústria tem como objetivo evitar a intervenção do governo e teve início após a ocorrência de vários desastres em plantas de processo americanas, nas décadas de 80 e 90. Destacam também os padrões utilizados pela indústria:

- *Programmable Electronic Systems In Safety Related Applications*, Parts 1 & 2, U.K. Health & Safety Executive: este foi o primeiro padrão sobre o tema, publicado em 1987;

- *Guidelines for Safe Automation of Chemical Process*, AIChE: este padrão cobre o projeto de Sistemas Digitais de Controle Distribuído (SDCD) e SIS, e foi elaborado pelo *Center for Chemical Process Safety – CCPS*, entidade criada pelo AIChE depois do acidente em Bopal, na India;

- *Boiler and Combustion Systems Hazard Code*, National Fire Protection Association NFPA 85: considerado como o padrão mais reconhecido no mundo para segurança de sistemas de combustão.

- *Recomended Practice for Instrumentation and Control Systems for Fired Heaters and Steam Generator*, API RP 556; o documento se apresenta como aplicável de forma integral em plantas químicas, plantas de gasolina e instalações similares.

- *Recommended Practice for Design, Installation and Testing of Basic Surface safety Systems for Offshore Production Platforms*, API RP 14C: práticas recomendadas prescritivas (*proven practices*) elaboradas para engenheiros de projeto e equipes de operação.

- *Process Safety Management of Highly Hazardous Chemicals* OSHA 29 CFR 1910.119: a OSHA reconheceu a ANSI/ISA-84.00.01-1996 como um conjunto de boas práticas para SIS e que a conformidade com este padrão equivale à aderência aos requisitos de Gerenciamento de Segurança de Processo da OSHA para SIS.

- *Standard Criteria for Safety Systems for Nuclear Power Generating Systems* IEEE 603-2009: estabelece os critérios mínimos de projeto e funcionamento para sistemas de segurança em centrais nucleares.

- *Identification of Emergency Shutdown Systems that are Critical to Maintaining Safety in Process Industry* ANSI/ISA 91.00.01-2001: este padrão inclui definições de

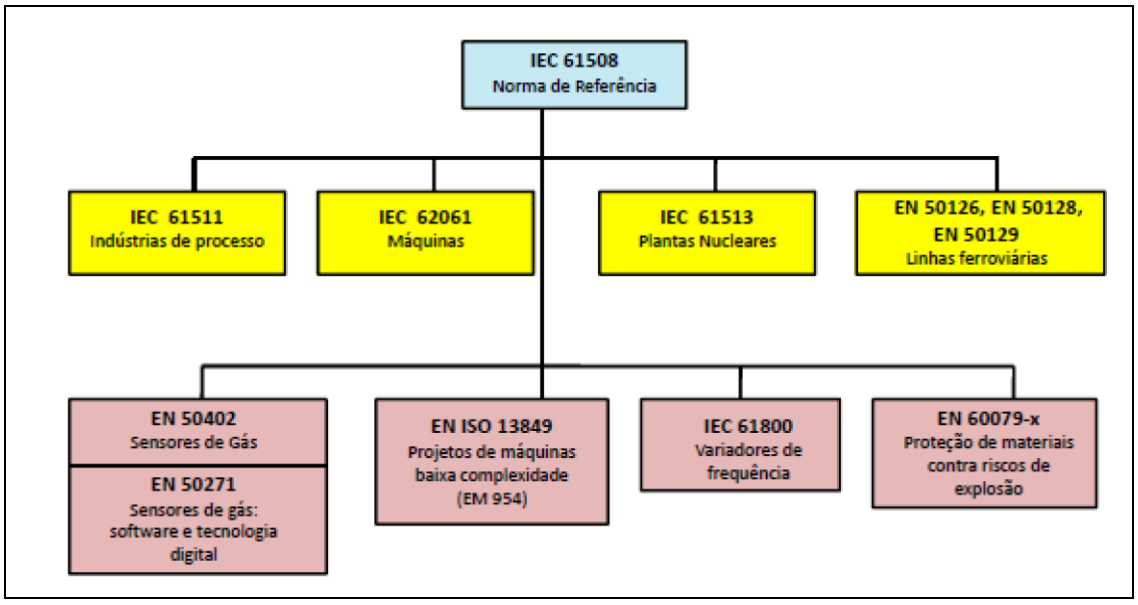
BPCS, sistemas de parada de emergência e controle crítico de segurança. Controles do tipo *Safety Critical Control* são aqueles que não possuem proteção de retaguarda, ou seja, cuja falha resultaria em evento perigoso.

- *Functional Safety – Safety Related Systems*, IEC 61508: este padrão cobre o uso de relés, estado sólido e sistemas programáveis, incluindo dispositivos de campo. Este padrão se aplica a todas as indústrias (transportes, médica, nuclear, processo, etc) e foi elaborado para orientar o desenvolvimento de padrões específicos.

- *Functional Safety: Safety Instrumented Systems for the Process Industry Sector*, ISA 84.00.01-2004 Parts 1 &3 (IEC 61511 Mod). A IEC desenvolveu a IEC 61511 a partir da ANSI/ISA-84.01-1996. Posteriormente a ISA adotou a IEC 61511, acrescentando cláusulas regulatórias oriundas da versão escrita em 1996.

As duas principais normas utilizadas relacionadas à segurança funcional para regulamentar os processos industriais entre as demonstradas são a IEC 61508 e IEC 61511. Essas normas estabelecem critérios para o desenvolvimento de SIS. A Figura 1 mostra algumas normas de segurança, que utilizam a IEC 61508 como referência.

Figura 1 – Normas de Segurança Vigentes para segmentos industriais.



Fonte: Adaptado (FREIRE, 2013).

A norma internacional IEC 61508 é aplicada à segurança funcional de equipamentos elétricos, eletrônicos e eletrônicos programáveis (E/E/EP). Pode ser

chamada de documento padrão, pois normativas de segurança para segmentos industriais e aplicações derivam desta (SQUILLANTE, 2011). Esta norma é mais ampla, abrangendo processos industriais de inúmeras naturezas, fazendo com que os demais padrões se relacionem a este. Já a norma IEC 61511 ocupa relevância fundamental no momento em que se buscam produtos e certificados. É aplicável à integridade de SIS em indústria de processo (CRUZ-CAMPA & CRUZ-GOMEZ, 2009).

2.2 ESTUDOS DE FALHAS E RISCOS (HAZARD AND RISK)

Um método de estudo de perigos e riscos (*Hazard and Risk*) é requisitado pela norma para a construção de toda segurança em automação industrial, sendo um exame sistemático que deve ser adotado no início da elaboração do projeto (IEC 61511, 2003). Tal estudo é responsável por analisar e estudar os eventuais riscos que o processo ou sistema como um todo estão sujeitos (FREIRE, 2013). Os métodos de estudo mais relevantes usados atualmente pelas indústrias são o APP, FMEA, WHAT-IF e o HAZOP, definidos a seguir.

2.2.1 MÉTODO ANÁLISE PRELIMINAR DE PERIGOS (APP)

O método Análise Preliminar de Perigos, chamada na indústria pela sigla APP, refere-se a uma técnica básica de avaliação dos riscos perigos de um determinado processo (MESSIAS, 2015). Sua utilização poderá implicar na complementação da avaliação utilizando-se de outras técnicas adicionais, determinado pelo critério de aceitabilidade de riscos. Seu objetivo é mostrar os perigos, sejam eles com potencial para causar danos às instalações, aos operadores, ao público ou ao meio ambiente. A metodologia de APP compreende a execução das seguintes tarefas:

- Definição das fronteiras das instalações analisadas;
- Coleta de informações sobre as instalações e as características das substâncias perigosas envolvidas;
- Definição dos módulos de análise;
- Realização da APP propriamente dita (preenchimento da planilha para cada módulo de análise);

- Elaboração das estatísticas dos cenários por categorias de frequência e severidade, e da lista de sugestões gerados no estudo;

- Análise dos resultados e preparação do relatório.

O escopo da APP abrange todos os eventos perigosos, cujas causas tenham origem nas instalações analisadas, englobando tanto as falhas intrínsecas de componentes ou sistemas, como eventuais erros operacionais (erros humanos), principalmente aqueles decorrentes de falhas nos procedimentos ou na execução. Deverão ser consideradas unidades de processo, estocagem, dutos, terminais, subestações, utilidades entre outras instalações que possam representar risco à segurança e meio ambiente. Ficam excluídos da análise os eventos perigosos causados por agentes externos, tais como: quedas de aviões, helicópteros, meteoritos, ou terremotos e inundações. Tais eventos externos foram excluídos por terem ocorrências consideradas extremamente remotas. A realização da análise propriamente dita é feita através do preenchimento de uma planilha com as informações necessárias à avaliação de riscos para cada módulo de análise (SOUZA, 2012).

2.2.2 MÉTODO FMEA

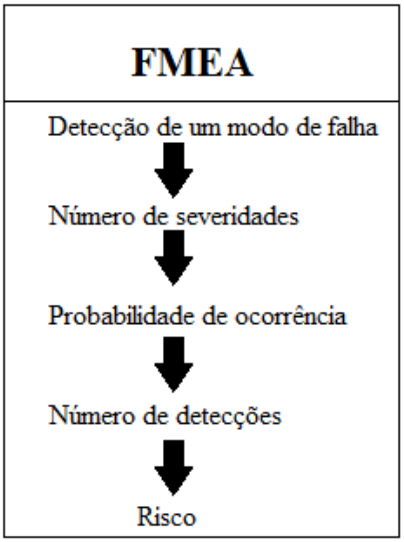
Entre os processos industriais que existem para evitar erros está o FMEA, que em inglês se refere *à Failure Mode and Effects Analysis*. No Brasil, a sigla foi traduzida como "Análise dos Modos de Falha e seus Efeitos" e funciona como um instrumento que tem o objetivo de evitar possíveis problemas num processo industrial aumentando assim confiabilidade já durante a fase de projeto (TAHARA, 2008).

Essas ações também podem objetivar aumentar a probabilidade de detecção dessas falhas, para que os produtos que apresentam inconformidades não cheguem ao cliente. Deste modo, é obtida uma lista de possíveis falhas, organizada por ordem do risco que elas representam e com respectivas ações a serem tomadas para mitigá-las. Tal lista auxilia na escolha de projetos alternativos com alta confiabilidade durante as etapas iniciais da fase de projeto, garantindo-se que todas as possíveis falhas de um projeto ou processo sejam consideradas e suas probabilidades de ocorrência minimizadas (quando se fizer necessário) (AMIGO, 2012).

A construção do FMEA consta de 4 etapas como mostrado na Figura 2:

- Detecção de modo de falha;
- Número de severidades que podem acontecer no processo ou sistema;
- Probabilidade de ocorrência do evento;
- Risco de o evento ocorrer.

Figura 2 – Método FMEA.

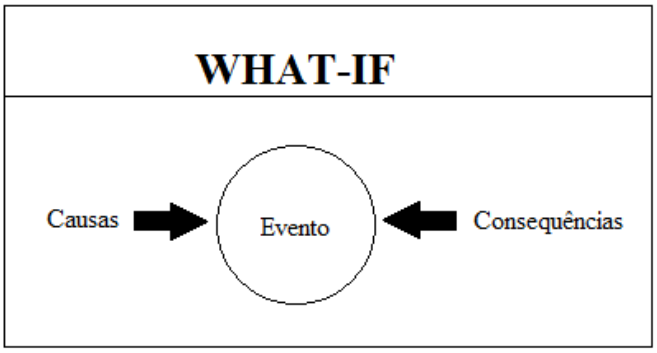


Fonte: (TAHARA, 2008).

2.2.3 MÉTODO WHAT-IF

What if é uma técnica qualitativa de cunho geral, de simples aplicação e muito útil como primeira abordagem, na identificação e detecção de riscos, em qualquer fase do projeto ou processo (STONNER, 2014). A aplicação desta técnica consiste em reuniões de uma equipe especializada, conhecedora do processo, que avalia o fluxo o processo, os subprocessos envolvidos, as entradas e saídas, e, com base no conhecimento de cada integrante, são levantadas questões do tipo “What if?”, ou, em Português, “E se?”, conforme Figura 3. Portanto ao responder à questão levantada, a equipe não precisa, necessariamente, ir fundo na pesquisa e identificação das causas e consequências. Eventualmente, estas causas e consequências podem ser melhor detalhadas, assim como as medidas de mitigação e prevenção.

Figura 3 – Método WHAT-IF.



Fonte: (STONNER, 2014).

Para realizar uma adequada análise “What if”, é importante um time multifuncional com experiência na planta e no processo, com um coordenador com capacidade de liderança, e realizar reuniões adequadamente conduzidas, iniciando com a apresentação da metodologia. É necessário também ter disponíveis o layout da planta, os fluxogramas de processo e de engenharia, especificações de equipamentos, variáveis do processo, diagramas de instrumentação (P&IDs) e outros documentos pertinentes. Percorre-se o fluxo de processo, buscando se colocar questões “What if” ao longo do percurso (STONNER, 2015).

2.2.4 MÉTODO HAZOP

O método de estudo HAZOP é o termo aplicado a um método detalhado de análise sistemática de um processo ou operação bem definida, seja este planejado ou existente. HAZOP é a abreviatura para *Hazard and Operability Study* (MACDONALD, 2004). Logo, o Estudo de Riscos e Operabilidade, é um exame criterioso, que deve ser elaborado durante o estágio inicial do detalhamento de engenharia de um projeto de segurança. Assim, os riscos inseridos no processo são identificados e avaliados. Inicialmente, o estudo contempla a coleta de dados das malhas de controle, relativo às ações envolvidas.

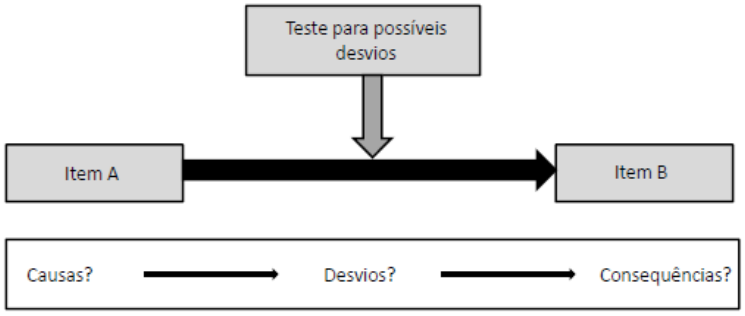
As malhas de controle são constituídas por diversos elementos, portanto se torna inviável a análise de todas as variáveis do sistema ao mesmo tempo. Sendo assim, o estudo indica que o sistema deve ser dividido em subsistemas, permitindo a análise detalhada de cada elemento. Desta maneira, é possível identificar possíveis falhas, consequências e as respectivas proteções necessárias. Esta divisão pode ser feita da seguinte forma:

- Os subsistemas menores são caracterizados por alta complexidade, envolvendo alto nível de risco;

- Os subsistemas maiores são simples, com baixo nível de riscos.

De posse dos subsistemas que compõe a malha de controle, as análises se restringem aos mesmos separadamente. Sendo assim, cada comunicação existente entre os elementos é analisada, desde a fonte até o seu destino. Isto permite quantificar e qualificar eminentes riscos. A análise que é feita da conexão entre dispositivos pelo HAZOP está representada na Figura 4.

Figura 4 – Percurso de uma tarefa dentro da malha de controle HAZOP.



Fonte: (FREIRE, 2013).

Os desvios devem ser considerados como elementos ou parâmetros. Os tipos mais comuns de desvios podem ser listados como um conjunto de palavras-chave (MACDONALD, 2004). A Tabela 1 a seguir expõe as principais palavras-chave utilizadas na elaboração do estudo HAZOP, e seus respectivos significados.

Tabela 1 – Palavras-Chave para Elaboração do HAZOP.

Palavras-Chave	**Significado**
Não	A intenção do projeto não é alcançada.
Mais	Aumentando quantitativamente.
Menos	Diminuindo quantitativamente.
Assim como	Modificação qualitativa.
Parte de	Apenas uma parte da intenção do projeto é alcançada.
Reverso	Oposição lógica à intenção do projeto.
Exceto	Substituição completa.

Fonte: (MACDONALD, 2004).

Na sequência, o estudo HAZOP é manipulado através da investigação de uma série de questões a cerca deste possível desvio. A Tabela 2 ilustra estas questões que devem ser respondidas afim de caracterizar um eminente risco.

Tabela 2 – Questões para cada desvio.

Palavras-Chave	Significado
É possível ocorrer?	Decidir Sim ou Não, baseado em regras simples.
Causas	Devem ser estabelecidas as causas. Se as consequências do desvio forem triviais, causas detalhadas não são necessárias.
Consequências	Devem ser consideradas categorias, incluindo, prejuízos às pessoas, ao meio-ambiente, danos aos equipamentos, perda de qualidade e produção.
Proteção	Devem ser expostas proteções existentes no projeto ou nos métodos de operação. Proteções devem incluir procedimentos de operação, alarmes e trips.
Risco Aceitável	Esta decisão não precisa necessariamente ser tomada no estudo.
O que pode ser feito	Os estudos corretivos devem indicar soluções óbvias que devem ser acordadas ao término do mesmo;
Ação	As ações necessárias que devem ser estabelecidas.

Fonte: (MACDONALD, 2004).

Resumidamente, o preenchimento destas questões presentes na Tabela 2 representam uma base de dados da análise de riscos da planta. As ações e recomendações expostas pelo HAZOP indicam quais equipamentos e procedimentos devem ser implementados pela equipe projetista e de manutenção da planta afim de que os riscos sejam mitigados.

As análises existentes e apresentadas aqui como as principais utilizadas dentro do cenário industrial podem ser comparadas através de suas vantagens e desvantagens como mostrado pela Tabela 2.

Tabela 3 – Vantagens e Desvantagens dos Métodos de Análise de Riscos.

Métodos	Vantagens	Desvantagens
FMEA	Aumenta a probabilidade de detecção das falhas; Amplo - detecção de falhas inclusive nos produtos.	Extremamente complicado para quem nunca trabalhou com o mesmo.
WHAT-IF	Técnica Simples de Análise - Busca respostas através da pergunta “E SE?”; Ao responder à questão levantada, a equipe não precisa, necessariamente, ir fundo na pesquisa e identificação das causas e consequências.	Pela simplicidade de sua realização pode deixar de ver falhas intrínsecas ao processo; Alguns detalhes podem ser deixados de lado, ou seja, não é um exame profundo.

HAZOP	Análise sistemática de um processo ou operação bem definida; Elaborado durante o estágio inicial do detalhamento de engenharia de um projeto de segurança. Assim, os riscos inseridos no processo são identificados e avaliados; O estudo indica que o sistema deve ser dividido em subsistemas, permitindo a análise detalhada de cada elemento.	Bem longo de ser preenchido; Até este ponto do projeto não foi encontrada nenhuma ferramenta automática que realizasse o procedimento.

Fonte: Autoria Própria.

2.3 FALHAS ALEATÓRIAS E SISTEMÁTICAS

Um sinistro ocorre quando um dispositivo em algum nível (um sistema, uma unidade, um módulo, ou um componente) falha ao cumprir a sua função desejada (GOBLE & CHEDDIE, 2005). Todavia, a falta de sucesso na realização de uma atividade por um equipamento ou sistema pode ser de responsabilidade de algum ou ambos fatores:

- Falhas Aleatórias ou Físicas: Falhas aleatórias são relativamente bem compreendidas. Uma falha aleatória é quase sempre permanente e atribuível a algum componente ou módulo (GOBLE & CHEDDIE, 2005);
- Falhas Sistemáticas ou Funcionais: Uma falha sistemática ocorre quando o sistema é capaz de operar, porém não desempenha a sua função desejada. Fontes de falhas sistemáticas são quase sempre erros de projeto, geralmente devido à procedimentos ou treinamentos inadequados (GOBLE & CHEDDIE, 2005).

Logo, falhas físicas estão diretamente relacionadas à erros de hardware, enquanto que as falhas funcionais se referem às ações indevidas tomadas pela equipe de operação e engenharia do sistema.

Mensurar a taxa de probabilidade de ocorrência de falhas sistemáticas e aleatórias é um tema complexo, e que envolve rigorosos investimentos por partes das maiores empresas do mundo. Prever esta probabilidade é um fator de projeto importante, visto que os sistemas instrumentados de segurança devem ser implementados afim de mitigar os potenciais riscos decorrentes destas falhas (FREIRE, 2013).

Uma das bases de dados mais populares que apresenta a taxa de falha é o banco de dados OREDA. OREDA significa "*Offshore Reliability Database*". Este livro, referência para os projetistas , apresenta uma análise estatística detalhada sobre os vários tipos de equipamentos de processos. Muitos engenheiros a utilizam como uma fonte de dados para

as taxas de falhas, afim de realizar cálculos de verificação de segurança (GOBLE & CHEDDIE, 2005).

2.4 SISTEMAS INSTRUMENTADOS DE SEGURANÇA (SIS)

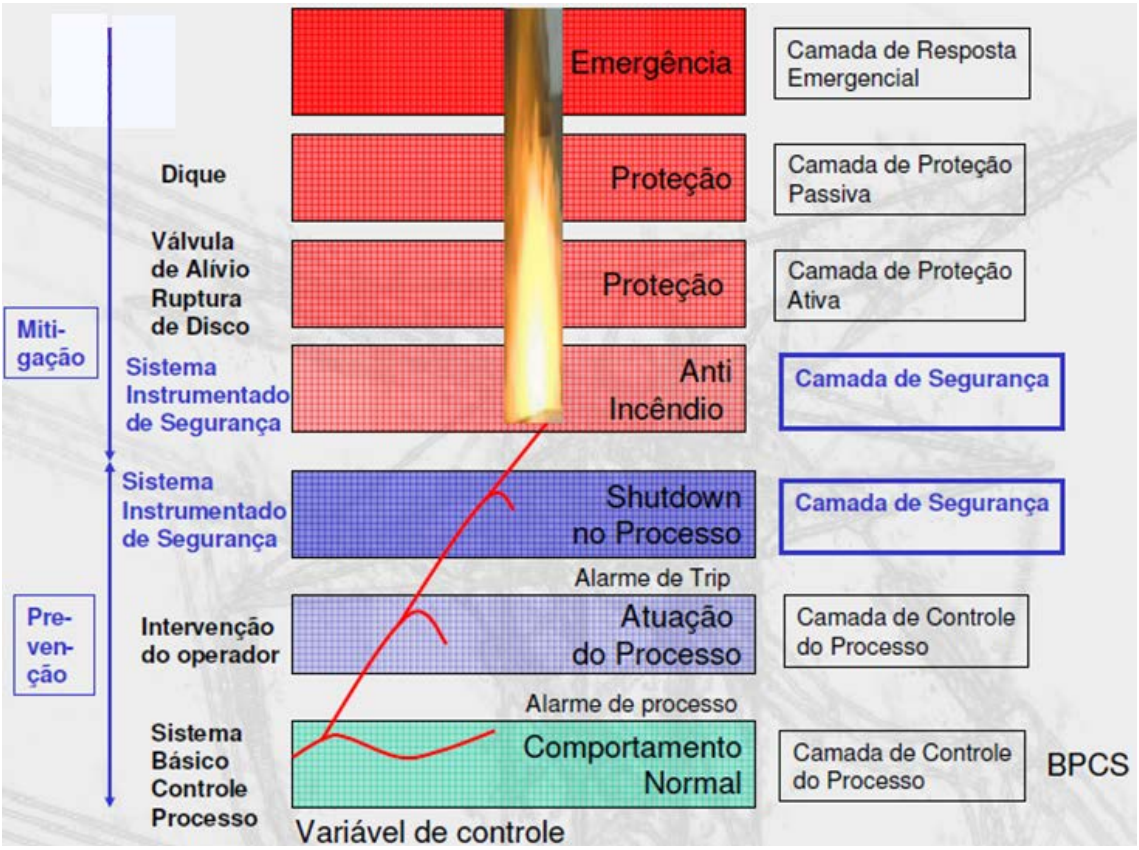
2.4.1 ANÁLISE DE CAMADAS DE PROTEÇÃO

Sistema de segurança é o termo utilizado para descrever sistemas que desempenham uma função ou funções específicas que garantam que os riscos sejam mantidos em um nível aceitável (MINORU, 2015). Os sistemas de segurança são subdivididos de acordo com suas aplicações, interagindo com os processos e buscando coibir supostos problemas iniciais que estejam ocorrendo, além de procurar a redução das consequências que estes problemas possam gerar. A Figura 5 mostra as camadas de proteção possíveis a fim de se reduzirem riscos eminentes. O sistema básico de controle do processo (BCPS) fornece a segurança com o projeto apropriado do controle do processo. Este nível consiste em controles básicos, em alarmes, e em supervisão do operador. O Sistema Instrumentado de Segurança opera independente do sistema básico de controle do processo para fornecer um pouco mais de segurança que o controle do processo. Executa ações da parada programada quando as camadas precedentes não podem resolver uma emergência.

- *Prevenção:* Caracterizado pelos sistemas que buscam coibir o início dos problemas. Esta classificação contém o Sistema Digital de Controle Distribuído (SDCD), os Alarmes e posteriores intervenções dos operadores, além do próprio Sistema Instrumentado de Segurança.

- *Mitigação:* Nestes casos mais críticos, eventuais distúrbios na planta já ocorreram. Desta forma, os Sistemas de Detecção e Combate ao Fogo e Gás são utilizados para reduzir as consequências.

Figura 5 – Camadas de Proteção.



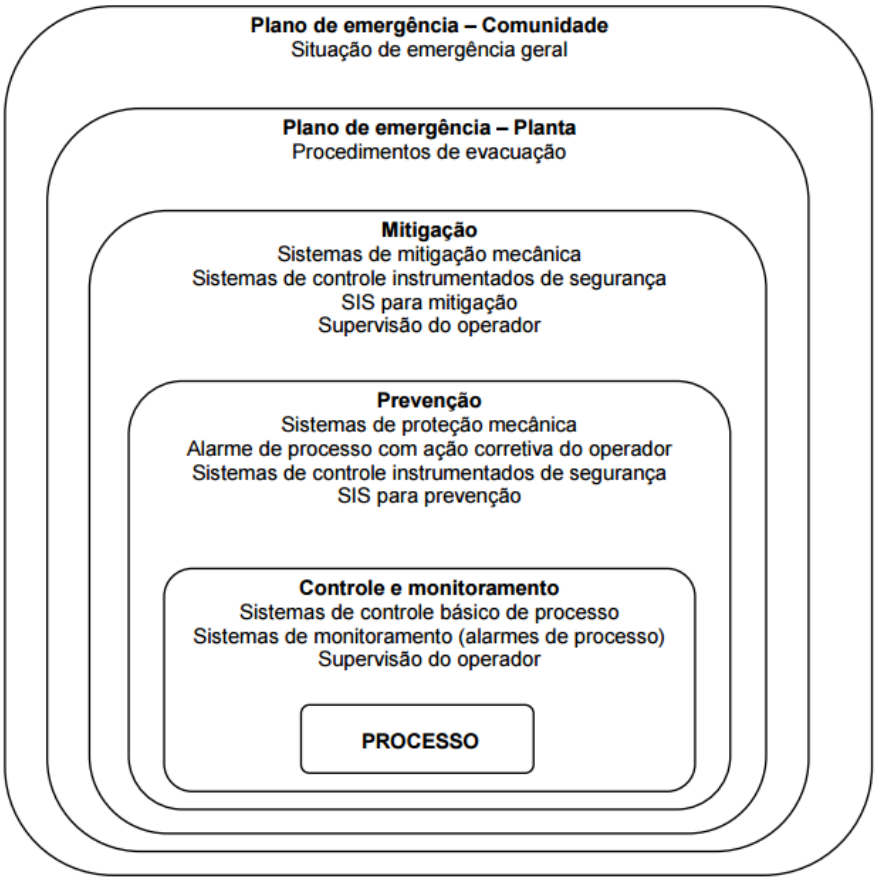
Fonte: (CASSIOLATO, 2012).

Acidentes ocorrem quando eventos com reduzida probabilidade são combinados. A prevenção pode ser obtida pelo uso de camadas de proteção independentes que dificultam a propagação de eventos perigosos e reduzem o risco do processo para níveis aceitáveis. Aumentar o número de camadas de proteção reduz a probabilidade de acidentes, porém é mais efetivo investir no aumento da segurança intrínseca do processo (GRUHN; CHEDDIE, 2006). Grandes máquinas e equipamentos são projetados para serem inerentemente seguros, terem alta confiabilidade e onde necessário são protegidos por camadas de proteção compatíveis com os riscos. Devido às solicitações dinâmicas em períodos de instabilidade do processo ou paradas abruptas, mecanismos de falhas são iniciados ou acelerados.

A metodologia *Layer of Protection Analysis*, conhecido por LOPA, foi desenvolvida para determinar se existem camadas independentes de proteção (IPLs) suficientes para os cenários acidentais identificados na análise de riscos, considerando a frequência dos eventos iniciadores, severidade das consequências e probabilidade de

falha das IPLs (LASSEN, 2008). As camadas de proteção devem ser efetivas em prevenir ou mitigar as consequências de um evento perigoso, ser independentes de outras IPLs associadas com o perigo identificado e devem ser projetadas para facilitar validações regulares das funções de proteção (LASSEN, 2008). Na Figura 6 são mostradas camadas de proteção típicas, conforme a IEC 61511 (2003).

Figura 6 – Métodos Típicos de Redução de Riscos em Processos.



Fonte: (SILVA, 2012).

2.4.2 SIS DEFINIÇÃO

O Sistema Instrumentado de Segurança ou mais comumente SIS que se encaixa nesse conceito de sistema de segurança pode ser explicado como a técnica de mitigar riscos e implantar instrumentação e controle operacional em processos, tornando a planta e suas malhas capazes de entrarem em falha segura ou *shutdown*, independente do sistema de controle, caso ocorra um acidente, protegendo assim os equipamentos, pessoas e até mesmo o meio ambiente (IEC 61511, 2003). O SIS é construído para aplicar um conjunto

de funções de controle específicas para a segurança do processo quando ocorre uma falha inaceitável ou extremante perigosa. Esses sistemas englobam elementos como sensores ou indicadores, unidades lógicas e elementos finais (atuadores) para realização de uma ou mais funções de segurança e são totalmente independentes de outros sistemas a fim de que sua funcionalidade não seja comprometida (IEC 61508, 2010). Também é relevante que o SIS permanece "dormente" durante operação normal somente atuando quando requisitado.

A maneira com a qual o SIS atua na planta industrial varia de acordo com as necessidades da aplicação, recebendo as respectivas classificações:

- *Partial Shutdown System* (PSD) ou Sistema de Parada Parcial: Caracterizada como uma prevenção, o princípio desta funcionalidade é, depois de constatado um eminente problema em uma determinada área de processos, desativar todos os dispositivos que de alguma forma estão relacionados a esta área. Entretanto, as outras áreas de processos que não possuem ligação direta com este distúrbio continuam a exercer suas funcionalidades normalmente.

- *Emergency Shutdown System* (ESD) ou Sistema de Parada de Emergência: Diferentemente do caso do PSD, existem casos nos quais os distúrbios são influenciáveis por vários fatores e impactantes em mais de uma área de processos simultaneamente. Sendo assim, torna-se inviável que a lógica de atuação do SIS possa prevenir maiores problemas desativando apenas uma parte da planta. Nestes casos, faz-se necessário desligar todas as áreas de processos ao mesmo tempo, de uma maneira suave e segura, caracterizando uma *trip* da planta. Obviamente, estes casos são mais complexos, e representam o limiar entre a prevenção e a mitigação.

- *Burner Management System* (BMS) ou Sistema de Gerenciamento de Caldeiras: As caldeiras industriais são caracterizadas pelas altas temperaturas atingidas durante os processos. Estes níveis de calor devem ser controlados, e caso atinjam valores acima de um determinado nível seguro, a segurança de processos, que neste caso específico é conhecida como BMS, deve agir afim de evitar a ocorrência de acidentes.

- *Fire and Gas System* (F&G) ou Sistema de Fogo e Gás: Nestas aplicações, a intenção é reduzir as consequências dos distúrbios ocorridos. Estes sistemas irão atuar quando o risco eminente não foi reduzido à níveis seguros em tempo hábil, e os acidentes já ocorreram, podendo estar associados ao fogo e a emissão de gases tóxicos. Desta forma,

o sistema é baseado em sensores, atuadores e demais dispositivos com a finalidade de detectar estes focos iniciais e combatê-los.

2.4.3 SIS: CONCEITOS FUNDAMENTAIS

- *Estado de Parada Segura:* Recentemente, com a difusão da utilização dos SIS, existem vários conceitos incorretos que são amplamente difundidos (FINKEL et al., 2006). Um deles por exemplo afirma que, para uma condição segura, o SIS agirá cortando toda forma de alimentação elétrica, porém isso não é verdade já que pode ser necessária para atuação no processo a ação de algum equipamento visando a eliminação de alguma substância tóxica no processo. Dessa forma, a IEC 61511 (2003) determina que deve ser identificado um estado seguro no qual os riscos indesejáveis foram eliminados, fato este que é estabelecido previamente na fase de projeto do sistema de segurança;

- *Confiabilidade:* A confiabilidade de um sistema é dada como a habilidade do mesmo realizar sua função dentro dos limites e condições operacionais dentro de um espaço de tempo definido (SAINI et al., 2017). A confiabilidade é quantificada de acordo com o tempo médio entre as falhas que ocorrem no sistema;

- *Disponibilidade:* Mede a proporção de tempo em que o instrumento trabalha sem falhas. A disponibilidade é uma função não somente de confiabilidade, mas é também uma função de manutenção. A Tabela 4 mostra a relação entre a confiabilidade, manutenção e disponibilidade. Nota-se que, nesta tabela, um aumento na capacidade de manutenção implica em uma diminuição no tempo que leva para realizar ações de manutenção;

Tabela 4 – Relação entre Confiabilidade, Manutenção e Disponibilidade.

Confiabilidade	**Manutenção**	**Disponibilidade**
Constante	Diminui	Diminui
Constante	Aumenta	Aumenta
Diminui	Constante	Aumenta
Aumenta	Constante	Diminui

Fonte: (CASSIOLATO, 2010).

- *Probabilidade de Falha em Demanda* (PFD)*:* Atributo de confiabilidade que indica qual a probabilidade de um componente falhar em cumprir uma ação previamente especificada no momento da sua requisição (HILDEBRANDT, 2007). É o indicador apropriado para sistemas de segurança;

- *Fator de Redução de Riscos* (RRF)*:* Matematicamente é o inverso do PFD e expressa a magnitude da redução de risco que pode ser alcançada com a inserção de uma determinada função de segurança (GANDY, 2013);

- *Diagnósticos:* São necessários para identificar falhas perigosas que podem impedir o SIS de realizar suas atribuições. Assim, a capacidade de um sistema de detecção de falhas automaticamente representa a cobertura do diagnóstico que é estimado usando a técnica desenvolvida para tal e conhecida como *Failure Modes, Effects and Diagnostic Analysis* – FMEDA (GRUHN; CHEDDIE, 2006).

2.5 NÍVEL DE INTEGRIDADE DE SEGURANÇA (SIL)

2.5.1 SIL DEFINIÇÃO

Uma vez definido o SIS e seus conceitos principais, vale discursar sobre uma parte relevante ao projeto de sistemas de segurança realizada após a análise de riscos que é a quantificação dos mesmos. O SIL, sigla para *Safety Integrity Level* em inglês, ou “Nível de Integridade de Segurança” é uma unidade de medida utilizada para quantificação da redução de riscos (MCLENDON, 2013). Este nível é a representação estatística da integridade de um SIS, quando uma demanda de processo ocorre, sendo também usada para medir a confiabilidade do SIS. As normas ANSI/ISA-S84.01 (2011) e IEC 61508 (2003) possuem os mesmos três primeiros níveis de integridade: SILs 1, 2 e 3. A IEC também inclui um nível adicional, SIL 4, que a ISA não possui. Quanto maior o SIL, mais confiável ou eficiente é o sistema (OLIVEIRA, 2012).

Os SIL estão relacionados à probabilidade de falha na demanda (PFD), que é equivalente à indisponibilidade de um sistema no momento da demanda de processo e à consequência/criticidade no evento desta indisponibilidade. A relação 1/PFD conhecida como fator de redução de risco, mais comumente conhecida em inglês por *Risk Reduction Factor* ou RRF, se relaciona diretamente com o SIL. A Tabela 5 mostra essa relação.

Tabela 5 – Relação entre SIL, PFD e RRF.

SIL	Probabilidade Média de Falha em Demanda	Redução de Risco
4	$\geq 10^{-4}\ a\ < 10^{-5}$	$> 10000\ a\ \leq 100000$
3	$\geq 10^{-4}\ a\ < 10^{-3}$	$> 1000\ a\ \leq 10000$
2	$\geq 10^{-3}\ a\ < 10^{-2}$	$> 1000\ a\ \leq 1000$
1	$\geq 10^{-2}\ a\ < 10^{-1}$	$> 10\ a\ \leq 100$

Fonte: (FREIRE, 2013).

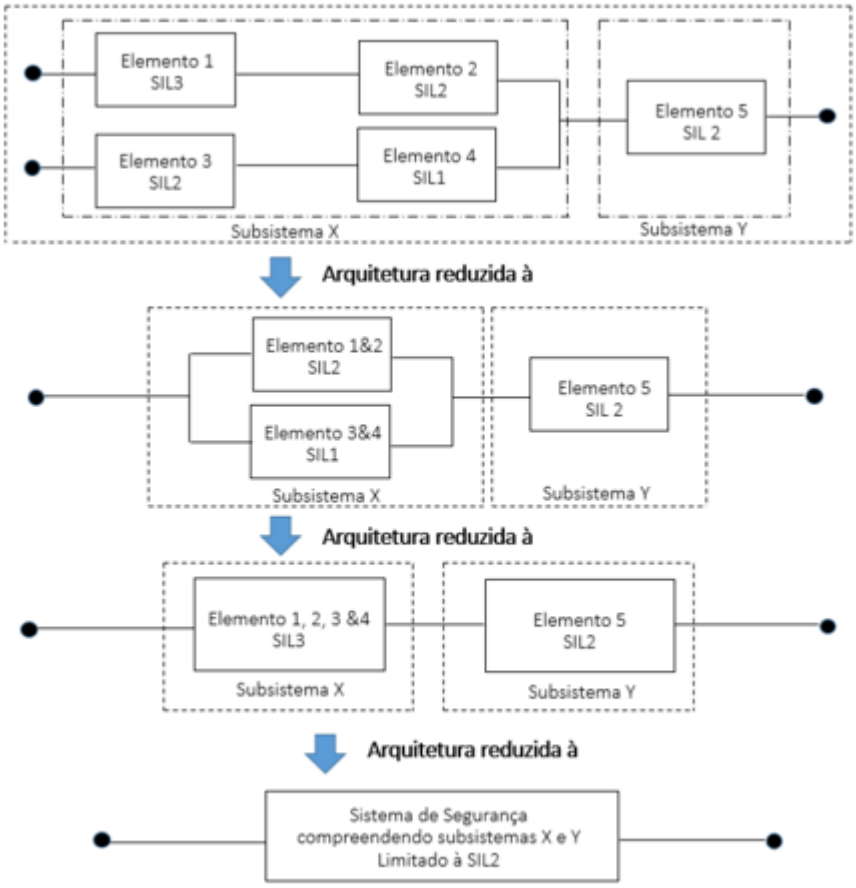
2.5.2 DETERMINAÇÃO DO SIL REQUERIDO

Para se determinar o nível de integridade desejado para um SIS, os seguintes parâmetros devem ser considerados:

- O grau de severidade das consequências, se a função de proteção pertencente ao instrumento não operar em demanda;
- A probabilidade de existência de seres humanos expostos ao perigo;
- Existência de fatores alternativos que poderão reduzir o impacto das consequências do risco;
- A frequência em que a função de proteção do instrumento é chamada para operar.

É possível também que em uma mesma malha tenha elementos ou subsistemas com diferentes níveis de integridade de segurança. A IEC 61508 (2010) demonstra como se deve proceder para as relações lógicas entre os subsistemas. Para arquiteturas em série o valor do nível de integridade de segurança resultante é obtido comparando-se as arquiteturas e selecionando-se o menor valor entre eles. Por exemplo duas arquiteturas em série uma SIL 3 e a outra SIL 2, o SIL resultante então é o SIL2. Já arquiteturas em paralelo se comportam de forma diferente, tais arquiteturas são somadas com limite máximo de SIL 4. Por exemplo duas arquiteturas em paralelo, uma SIL 1 e outra SIL 2, o valor resultante é SIL 3. A Figura 7 apresenta como é feita a redução das arquiteturas.

Figura 7 – Determinação do SIL máximo por uma arquitetura compreendida por dois subsistemas.



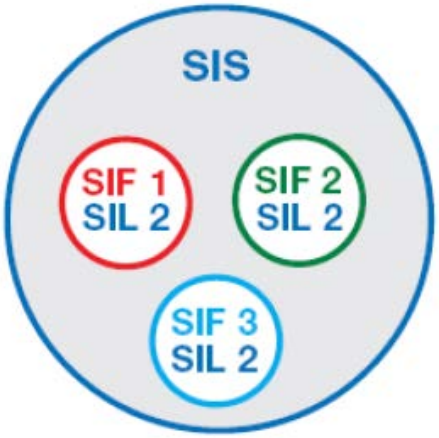
Fonte: (IEC 61508, 2010).

2.6 FUNÇÃO INSTRUMENTADA DE SEGURANÇA (SIF)

A *Safety Instrumented Function*, SIF, sigla em inglês que significa “Função Instrumentada de Segurança” é uma função com um nível específico de segurança, um SIL, que é implementada e colocada em execução pelo Sistema Instrumentado de Segurança (SIS), representando um conjunto de decisões que protegem o sistema contra um único perigo específico (GOMES, 2014). Apesar de geralmente o sistema de segurança de uma planta ser integrado e operado em uma estação de operação e engenharia única, as malhas de segurança de processos se diversificam. Isto deve-se ao fato que cada malha possui um SIL específico, que foi obtido através das análises de avaliação do risco. E consequentemente, as características destas malhas são especificadas de acordo com o risco potencial que cada uma delas deve mitigar.

A relação que une SIF, SIL e SIS é apresentada na Figura 8. Cada Sistema Instrumentado de Segurança (SIS) possui uma (ou mais) Função Instrumentada de Segurança (SIF) com um Nível de Integridade de Segurança (SIL) específico.

Figura 8 – Relação SIF, SIL e SIS.



Fonte: (GOMES, 2014).

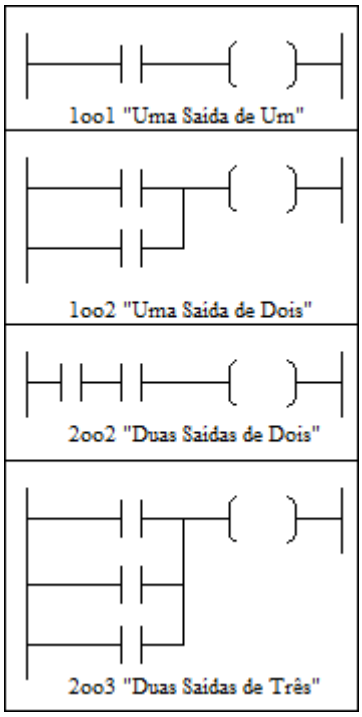
A fração de falha segura mede a tendência natural de um instrumento em falhar de forma segura ou de detectar falhas perigosas. O resultado é sempre um número entre zero e um, sendo que um número mais próximo de um é bom (CROWL & LOUVAS, 2002). Logo, o índice fração de falha segura, ou *Safe Failure Fraction* (SFF), é um fundamento implícito à SIF que os instrumentos utilizados em sistemas de segurança devem possuir. Quanto maior foi o SFF de um elemento, mais seguro é este dispositivo, e consequentemente possuirá qualificações para atuar em malhas que requerem níveis de integridade elevados.

Outro aspecto importante na definição dos elementos que irão compor uma malha de segurança é o atendimento ao índice tolerância à falha de hardware, ou *Hardware Fault Tolerance* (HFT). Uma tolerância a falhas de hardware de N significa que N+1 é o número mínimo de falhas que podem causar uma perda da função de segurança (IEC 61508, 2010).

A arquitetura de uma SIF é decidida pela tolerância de falhas de seus componentes, (HFT) e pelo nível de redundância de seus componentes. A utilização de redundância de hardware (ou de equipamentos) é um dos recursos mais empregados quando tolerância a falhas é requerida. Maior tolerância a falhas corresponde a maior disponibilidade da

planta e maior segurança funcional. As arquiteturas SIF mais comuns, mostradas na Figura 9, são:

Figura 9 – Arquiteturas SIF.



Fonte: Autoria Própria.

- Simplex ou Votação 1oo1: O princípio de votação 1oo1 envolve um sistema de canal único sem redundância (sensor – controlador – atuador), e normalmente é projetado para aplicações de segurança de baixo nível. A ocorrência de falha num dos equipamentos imediatamente resulta na perda da função de segurança ou o encerramento do processo.
- Duplex ou Votação 1oo2 ou 2oo2: O princípio de votação 1oo2 foi desenvolvido para melhorar o desempenho de integridade de segurança de sistemas de segurança baseados em 1oo1. A solução possui dois canais em paralelo (redundância de sensores e atuadores), de forma que se ocorre uma falha num canal, o outro ainda é capaz de desenvolver uma função de segurança.
- 2oo2: Nesta votação há a duplicação de canais (sensor – controlador - atuador) numa configuração serie, de forma que ambos os canais têm de falhar para que a função de segurança seja perdida ou o processo encerrado. Essa configuração reduz significativamente a probabilidade da perda da função de segurança. Por outro lado, o

sistema tem a desvantagem de que a probabilidade de falha por demanda é duas vezes mais elevada do que a de um único canal.

- Triplex ou Votação 2oo3: Nesta votação há três canais em paralelo (redundância de sensores e atuadores), de forma que dois deles precisam ser funcionais a fim de funcionar e cumprir com as funções de segurança. O princípio de votação 2oo3 é melhor aplicada quando há uma separação física completa de microprocessadores. No entanto, isto requer que estejam localizados em três módulos diferentes. Embora os sistemas mais recentes têm um nível mais elevado de diagnóstico, sistemas de segurança com base na votação 2oo3 ainda mantêm a desvantagem de probabilidade de falha sob demanda, que é aproximadamente três vezes maior que os dos sistemas baseados em 1oo2.

A HFT é uma variável importante na definição da característica de uma malha de segurança. Todavia, este parâmetro, que pode variar de 0 a 2, está diretamente relacionado com a redundância dos equipamentos. A Tabela 6 ilustra a relação entre o HFT e a votação dos equipamentos.

Tabela 6 – Tolerância à Falha de Hardware de acordo com a votação.

Votação	**Definição**	**HFT**
1oo1	Apenas 01 módulo de processamento independente, sem diagnóstico.	0
1oo1D	Apenas 01 módulo de processamento independente, com diagnóstico.	0
1oo2	02 módulos de processamentos independentes, sem diagnóstico.	1
1oo2D	02 módulos de processamentos independentes, com diagnóstico.	1
2oo2	02 módulos de processamentos sem módulo de diagnóstico, porém são dependentes, e o sistema depende de ambos energizados.	0
2oo2D	02 módulos de processamentos com módulo de diagnóstico, porém são dependentes, e o sistema depende de ambos energizados.	0
2oo3	03 módulos de processamento, porém são dependentes e ao menos 02 módulos precisam estar em funcionamento.	1
1oo3	03 módulos de processamento independentes.	2

Fonte: (CROWL & LOUVAS, 2002).

3 REVISÃO BIBLIOGRÁFICA

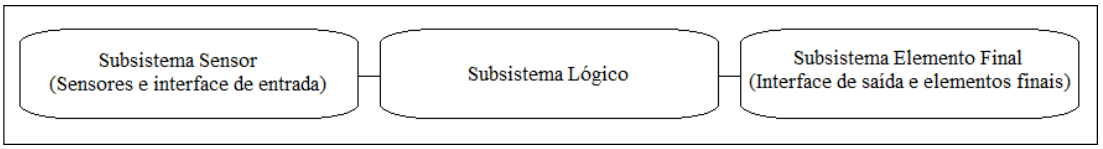
Analisando as bibliografias existentes acerca dos temas relacionados ao projeto de SIS, envolvendo análise e quantificação de riscos, cálculo do SIL e fundamentação da SIF, é possível verificar que a maioria da literatura recente (após 2005) têm focado em desenvolvimentos mais específicos sobre SIS. Novos métodos de análise e quantificação de riscos ou métodos que consideram a existência de falhas com características específicas em determinados processos têm sido propostos. O mesmo foi verificado na literatura referente aos trabalhos para cálculo e obtenção do SIL e SIF. Em contrapartida, e considerando a disponibilidade de literatura nacional sobre o tema de SIS, a proposta e revisão deste trabalho contemplaram um estudo mais básico sobre o tema. Este trabalho focou no estudo de métodos tradicionais para análise e quantificação de riscos, cálculo do SIL e fundamentação da SIF e na sistematização de um procedimento de projeto de SIS usando tais métodos, e compatível para a implementação computacional em ambiente Web conforme requerido na proposta do trabalho.

3.1 MÉTODOS DE ANÁLISE DE RISCO E CÁLCULO DO NÍVEL DE INTEGRIDADE DE SEGURANÇA

O projeto e especificação de SIS pode ser feita utilizando diversos métodos aceitos pelas normas de segurança. Nesse sentido, diversas metodologias de projeto de SIS diferentes têm sido propostas buscando facilitar as etapas de análise de riscos, os cálculos e a definição dos níveis de segurança (SILVA, 2012). Metodologias baseadas na análise de risco como FMEA (*Failure Modes and Event Analysis*), técnica What-if, Fuzzy e estudo HAZOP têm sido usadas no projeto de SIS (SOUZA et al., 2013).

A norma IEC 61508 (2010) fornece uma noção para validação e verificação de sistemas de segurança. Apesar de existirem diversos métodos de projeto de SIS, a norma sugere um procedimento em particular através da avaliação da probabilidade de falha por demanda (PFD) para o cálculo do SIL. Tal metodologia sugere a decomposição do SIS em três subsistemas, Subsistema Sensor, Lógico e Elemento final como visto na Figura 10.

Figura 10 – Subsistemas para elaboração do SIS.



Fonte: (IEC 61508, 2010).

- Subsistema Sensor (S): compreende os sensores reais e quaisquer outros componentes e cabeamento, mas não incluindo os componentes em que os sinais são primeiramente combinados por voto ou outro processo;
- Subsistema Lógico (LS): compreende os componentes em que os sinais são primeiramente combinados e todos os outros componentes necessários para isso incluindo o sinal final apresentado ao subsistema elemento final;
- Subsistema Elemento Final (FE): compreende todos os componentes e cabeamento que processam o sinal final do subsistema lógico incluindo o componente final de atuação.

Após essa divisão, fica mais simples ao projetista usar a soma do PFD de todos os subsistemas e assim calcular o SIL para o sistema como um todo.

Com relação às análises de risco, Bartolozzi et al. (2000) descrevem o uso de modelos qualitativos em um sistema de suporte para análises HAZOP, em conjunto com um algoritmo para encontrar as causas e as consequências de desvios variáveis. Os modelos usam várias estruturas de representação entre as quais árvores constituem o mais importante do ponto de vista funcional-lógico. Boonthum et al. (2014) criaram a combinação de uma análise HAZOP com um modelo estrutural que foi introduzido para obter um procedimento de identificação de risco e operações malsucedidas.

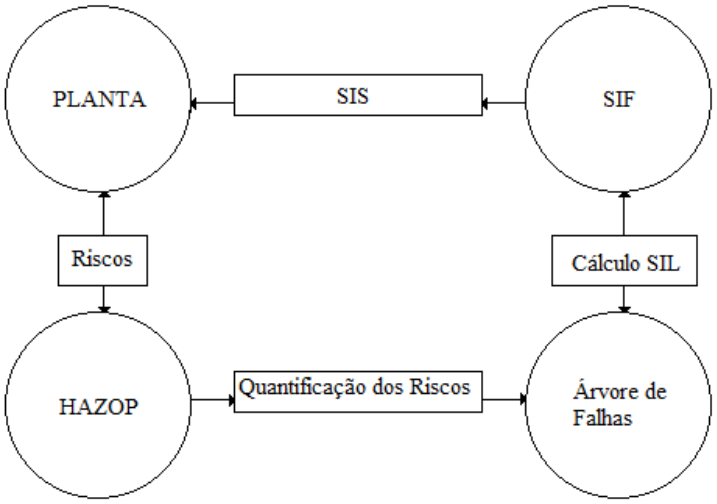
Cui et al. (2012) propõem uma nova estrutura de integração que combina HAZOP, análise de camada de proteção (LOPA), especificação de requisitos de segurança (SRS) e validação de nível de integridade de segurança (SIL) para o projeto de SIS. No trabalho, essa nova estrutura resulta numa plataforma de software inteligente chamada HASILT, capaz de realizar o armazenamento dos dados de histórico em uma base de casos central, usada para ajudar a resolver novos problemas a partir de casos antigos semelhantes.

Por sua vez Mansoori et al. (2016) demonstram experimentalmente que o HAZOP pode ser aplicado a um estudo de caso de experimentos de segurança de rede para medir

de forma confiável o comportamento de rastreamento de IP de sites mal-intencionados usando um honeypot de cliente de baixa interação.

Freire (2013) utiliza uma malha de controle de um Processo de Desbutanização, parte de uma Unidade de Processamento de Gás Natural (UPGN), um segmento da indústria de óleo e gás, para exemplificar a quantificação e qualificação dos eminentes riscos presentes no mesmo. Através do estudo HAZOP, o autor expõe as causas, consequências e ações preventivas para os eventuais riscos envolvidos no processo, tanto os inerentes ao processo quanto os externos. A partir dos riscos calculados, elabora uma árvore de falhas, a qual representa um método que fornece uma detalhada interpretação da quantificação dos riscos partindo de eventos inerentes ao processo juntamente com eventos que podem ser causados externamente e de externas para compor a taxa de fatalidades e assim se obter um valor adequado para o SIL. Usando como base o valor do SIL calculado, é possível a especificação de uma SIF eficiente visando à mitigação dos perigos estimados que poderiam causar danos ao sistema. Na Figura 12 pode ser visto o diagrama utilizando as técnicas expostas por Freire (2013).

Figura 11–Diagrama do procedimento adotado por Freire (2013).



Fonte: (Freire, 2013).

Zorzan et al. (2013) discorrem sobre a metodologia FMEA como ferramenta de análise de riscos, tratando-a como uma antecipação de falhas perigosas em qualquer sistema industrial e assim levantando as prioridades na hora de decidir quais ações serão tomadas para extinguir ou minimizar danos. O levantamento é feito com o auxílio de um formulário padrão de Análise dos Modos de Falha e seus Efeitos, os dados são inseridos

na tabela mostrada pela Figura 11. Essa tabela especifica o tipo de falha, suas causas e também o grau de severidade dos eventos em estudo.

Figura 12– Formulário usado pelo FMEA

Sistema: _____ **FMEA - Análise de Modos de Falhas e Efeitos** FMEA Nº: _____ ☐ Projeto

Sub-Sistema: _____ Responsável: _____ Folha: ____ de ____ ☐ Processo

Componente: _____ Data(Início): _____ Data(Origem): _____ Revisão: _____

Equipe: _____

Processo / Função	MODO de Falha	EFEITOS da Falha	Severidade	CAUSAS da Falha	Ocorrência	Meios e Métodos de Controles	Detecção	NPR	Açoes Recomendadas	Responsáveis e Prazos	Ações Tomadas	Severidade	Ocorrência	Detecção	NPR

Fonte: (Zorzan et al., 2013).

Ayaz e Tesik (2017) afirmam que a análise de modos e efeitos de falhas (FMEA) é uma ferramenta de qualidade poderosa e proativa para definir, detectar e identificar possíveis modos de falha e seus efeitos em processos. No entanto, o processo convencional de FMEA às vezes é difícil de implementar devido à carga de trabalho necessária e à subjetividade das avaliações realizadas. Assim, o trabalho usou algoritmos baseados em dados, como a análise de associação, para avaliar objetivamente as falhas e eliminar a subjetividade, e implementando essa técnica FMEA através de um aplicativo para servidores de computador.

Já Catelani, Ciani e Luongo (2012) acreditam que o aumento dos requerimentos de confiança, disponibilidade e segurança no contexto do processo industrial força continuamente os projetistas a enfrentarem desafios de especificação técnica para o

projeto de SIS. A proposta deles se preocupa na introdução de um modelo confiável para o cálculo do SIL afim de clarificar os aspectos de segurança tanto para os usuários finais como também para os técnicos não intrinsicamente envolvidos com problemas de segurança. Essa proposta se baseia na metodologia de Diagrama de Blocos de Confiabilidade, *Reliability Block Diagram* (RBD), que entra como método de quantificação de acidentes ao invés da árvore de falhas. O RBD é uma representação gráfica da funcionalidade requerida mostrando de fato a conexão lógica dos componentes necessários para completar uma função especifica do sistema. O procedimento sugere uma arquitetura lógica da função de segurança, identificando o SIL para cada componente envolvido com a função de segurança.

Uma pesquisa realizada na China por Wang e Tai (2011) afirma que a avaliação de segurança e redução de risco é comumente ligada a métodos probabilísticos, como a Análise da Árvore de Falhas (AAF), Diagrama de Blocos de Confiabilidade (RBD), Análise de Markov (MA) e equações simplificadas. Porém, as atividades de teste e de manutenção do SIS, que são potencial de risco, são pesquisadas através de métodos de otimização.. A pesquisa apresenta uma otimização da análise de falhas e quantificação para o cálculo do SIL, criando uma alternativa que mantém o equilíbrio entre segurança e disponibilidade e que alcança otimização do projeto do SIS no que diz respeito a exatidão matemática do SIL e da votação necessária para a SIF. A otimização é calculada para a concepção do SIS através da definição de variáveis de projeto, como configuração redundante, taxas de falhas, manutenções periódicas e testes frequentes que funcionam como fatores de controle que compõe o conjunto de variáveis de decisão para o cálculo do SIL e posterior definição da SIF.

A verificação do nível de integridade de segurança (SIL) é um passo crítico no ciclo de vida de segurança dos sistemas de segurança. Dessa maneira, Ding et al. (2017) apresentam um novo método para a verificação do SIL de um SIS com diferentes redundâncias com base na degradação do sistema. A ideia-chave do método é calcular a probabilidade média de falha perigosa em demanda (PFDAVG) em cada estágio de degradação do sistema, que é causado por falhas de canais redundantes. Para validar o método proposto, os autores aplicam no sistema de parada de segurança da Central de Controle de Energia Nuclear, e o resultado numérico é comparado com o modelo de AAF.

A alta complexidade dos sistemas produtivos atuais e os possíveis impactos negativos nos seres humanos, equipamentos e meio ambiente em caso de falha desses

sistemas demandam o desenvolvimento de soluções de controle de SIS que sejam estáveis, seguros e de acordo com as normas de segurança industriais. Uma forma de melhoria da confiabilidade desses programas de controle, que também é requisito das normas IEC 61508 (2010) e IEC 61511 (2003), é a utilização do ciclo de desenvolvimento de programas de segurança, ou modelo-V, de SIS. Ferrarezi et al. (2014) apresentam um framework para o desenvolvimento de programas de SIS baseados no modelo-V da norma IEC 61511. Cada componente desse framework foi desenvolvido para fornecer métodos e ferramentas compatíveis com a implementação de cada fase do modelo-V, de forma que o projeto do SIS seja realizado em total conformidade com as normas.

Almaw et al. (2016) discorrem que na maioria dos processos industriais, a resposta desejada no caso de uma falha é o desligamento do processo. Os SIS são projetados para que esse estado seja alcançado em resposta a falhas de itens específicos ou perda de energia. O efeito colateral desse projeto de segurança pode ser que o SIS seja propenso a uma ativação espúria, o que significa que o funcionamento normal do processo pode ser interrompido de forma intempestiva. Na concepção de um SIS, é importante quantificar a taxa de ativação espúria e verificar a necessidade de medidas adicionais para assegurar uma operação estável e segura do processo. Assim os autores apresentam novas fórmulas para cálculo do SIL considerando a ativação espúria e a propagação de falhas em um SIS. As fórmulas propostas são comparadas com as existentes para arquiteturas selecionadas, discutindo-se as diferenças entre elas.

3.2 FERRAMENTAS COMPUTACIONAIS

Apesar da disponibilidade de técnicas e do surgimento de novos métodos para a realização das etapas necessárias para o projeto de SIS, ainda é deficiente e existe uma grande demanda por ferramentas computacionais que automatizam qualquer uma dessas etapas, tendo em vista que muitas destas até hoje são feitas manualmente. Wang e Tai (2010) garantem que com o desenvolvimento das tecnologias de informática, os métodos de simulação e os algoritmos genéticos, a realização de tais etapas se tornarão mais simples e otimizadas.

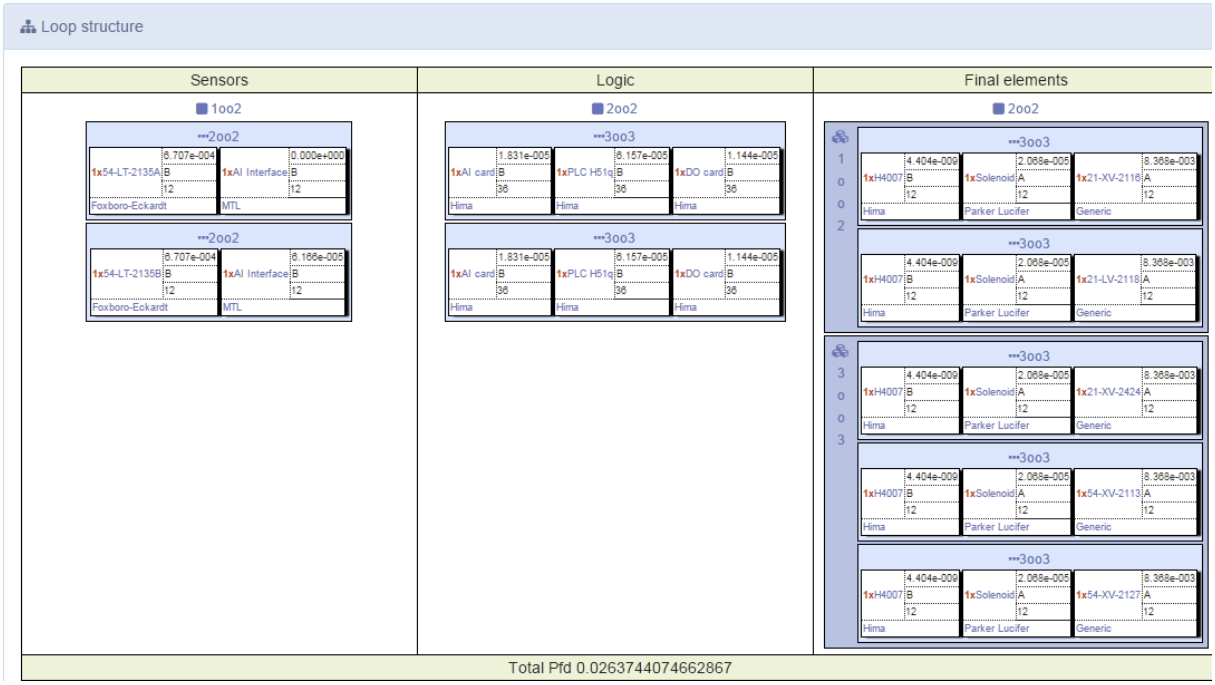
Diversas empresas relacionadas, e que possuem sistemas relacionados, à área de controle e automação industrial como Emerson (2015) utilizam softwares de inserção de dados como Word e Excel para criar planilhas personalizadas e estruturadas dos riscos em estudo nos processos e para cálculo dos níveis de segurança requeridos. Tais

ferramentas, apesar de auxiliarem no desenvolvimento da análise e cálculo realizado, exigem longos períodos de tempo para serem concluídas.

Uma empresa de pesquisa norueguesa, a MIDT (2015), lançou um software teste programado em linguagem específica para Internet com o objetivo de simplesmente utilizar as metodologias oferecidas pelas normas para funções de segurança afim de se obter um valor para o SIL. O ponto forte dessa ferramenta é a facilidade e rapidez no cálculo do SIL, porém o ponto fraco se refere ao fato de que para se usar o programa é necessário ter em mãos todo o estudo de riscos previamente realizado para inserção dos dados, já que a aplicação não oferece esse recurso.

A Figura 13 apresenta os subsistemas separando-os em sensor, lógico e elemento final, nos quais estão alocados os equipamentos que serão avaliados para cálculo do SIL.

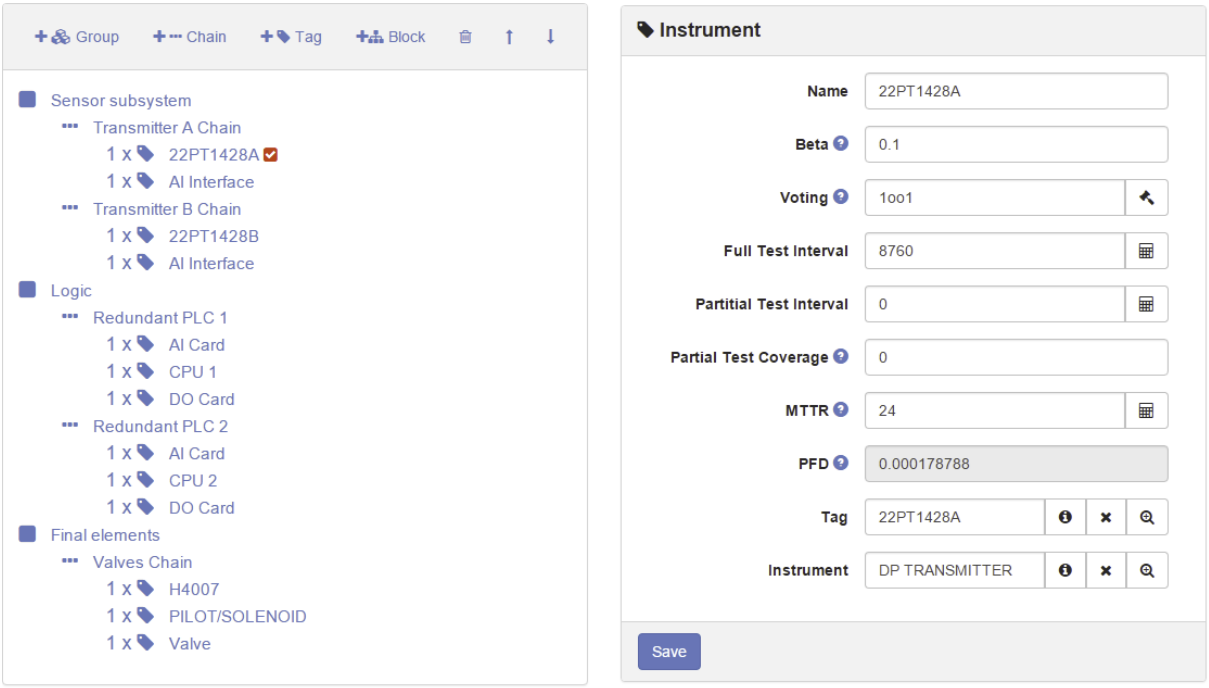
Figura 13 – Subsistemas Sensor, Lógico e Elemento Final (MIDT, 2015).



Fonte: (http://sil.midt.no/Home/HowItWorks, 2017).

A Figura 14 demonstra as variáveis utilizadas por essa ferramenta para o cálculo do nível de integridade de segurança (SIL).

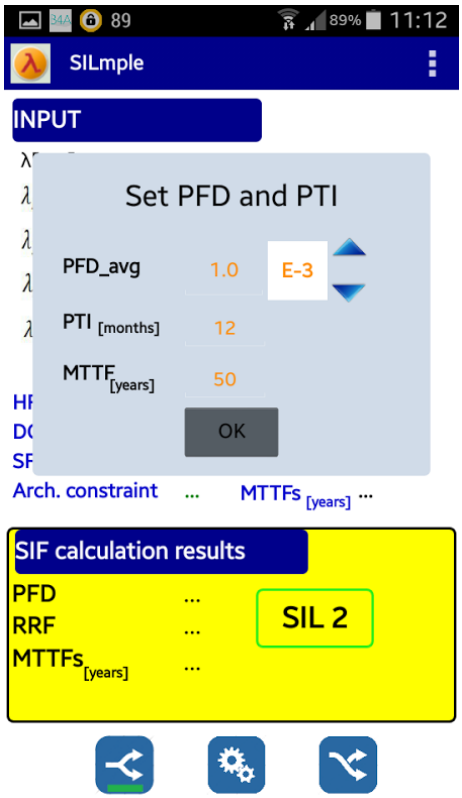
Figura 14– Tela de inserção de dados para cálculo do SIL para cada equipamento (MIDT, 2015).



Fonte: (http://sil.midt.no/Home/HowItWorks, 2017).

Outra ferramenta que também faz o cálculo do SIL foi liberada para dispositivos móveis do tipo Android (GIGIOSOFT, 2016). Chamado de *SILmple*, este aplicativo permite também que através do SIL, seja obtido a definição da SIF para o mesmo. O aplicativo calcula também os tempos médios de falhas, HFT e SFF, as restrições arquitetônicas para apoiar as normas IEC 61508 (2010) e IEC 61511 (2003). A Figura 15 apresenta uma imagem do aplicativo Android *SILmple*.

Figura 15 – Aplicativo Android para Cálculo do SIL (GIGIOSOFT, 2016).



Fonte: (https://lh3.googleusercontent.com/uu, 2017).

As análises de risco como a APP e o estudo HAZOP também possuem softwares próprios como o da EXIDA (2017) chamado *exSILentia*, um software muito utilizado no ambiente industrial, próprio, criado em linguagem de programação fechada e vendido a altos preços. Tal aplicação permite a inserção de dados de risco e, através do método APR, os quantifica gerando uma matriz de perigos que posteriormente é utilizada para o cálculo do SIL. A Figura 16 mostra parte desse sistema.

Considerando softwares proprietários relacionados ao projeto de SIS como o EXIDA, existe também o *SIL Selection Tool* da Pepperl Fuchs (PEPPERL +FUCHS, 2017) que serve obtenção de um SIL adequado aos equipamentos de um SIS, o *PAScal Safety Calculator* da Pilz (PILZ, 2017) que seleciona o SIL de acordo com EN/IEC 62061 e o *SIL CALCULATOR* da ProSIS (PROSIS, 2017) que verifica o SIL utilizando a árvore de falhas.

Figura 16 – Ferramenta própria para cálculo do SIL (EXIDA, 2017).

Fonte: (http://www.exida.com/exSILentia, 2017).

Entretanto é necessário ressaltar que apesar de existirem diferentes ferramentas computacionais para realização de análises e de cálculos relacionados ao projeto de SIS, não foi encontrada na literatura nenhuma ferramenta que integrasse todas as etapas de projeto do SIS. Ou seja, as partes separadas mostram um avanço no que diz respeito a automatização, porém o tempo de um projeto ainda é longo pois as etapas complementares devem ser realizadas manualmente.

Dessa maneira pode-se afirmar que a criação de uma ferramenta que integre todos os procedimentos envolvidos, conforme proposta neste trabalho, torna-se importante e gera contribuições tanto acadêmicas para os pesquisadores dessa área quanto técnica para os projetistas, técnicos e engenheiros da indústria. A Tabela 7 mostra uma comparação entre as principais ferramentas computacionais especificadas neste capítulo.

Tabela 7 – Comparação das Ferramentas Desenvolvidas.

Ferramenta	Vantagens	Desvantagens
MIDT	Ferramenta de cálculo do SIL; Cálculo do PFD; Oferece uma sugestão de configuração da votação para cada subsistema; Online; Facilidade de Operação; Banco de dados vasto.	Não faz nenhuma análise de risco, apenas os cálculos como se análise tivesse ainda que ser feita manualmente; Operação em ambiente Web.

SILmple	Cálculo do SIL; Cálculo do PFD; Aplicativo de Celular.	Não funciona adequadamente; Falha na inicialização; Não faz nenhuma análise de risco do processo.
Exida	Software completo; Permite análise de riscos; Cálculo do SIL; Cálculo do PFD; Banco de dados vasto; Oferece uma sugestão de configuração da votação para cada subsistema; Conexão entre todos os módulos	Extremamente caro; Funciona especificamente para certos fabricantes; Poucas funções são usadas no Brasil; Feito em linguagem de programação C/C++/C# para operação em computadores locais; Sem suporte Web.
SIL Selection Tool	Cálculo do SIL	Extremamente caro; Funciona especificamente para certos fabricantes; Poucas funções são usadas no Brasil; Feito em linguagem de programação C/C++/C# para operação em computadores locais; Sem suporte Web.
PAScal Safety Calculator	Cálculo do SIL; Cálculo do PFD;	Feito em linguagem de programação Pascal para operação em computadores locais; Sem suporte Web.
SIL CALCULATOR	Permite análise de riscos; Cálculo do SIL; Cálculo do PFD; Banco de dados vasto;	Extremamente caro; Sem suporte Web

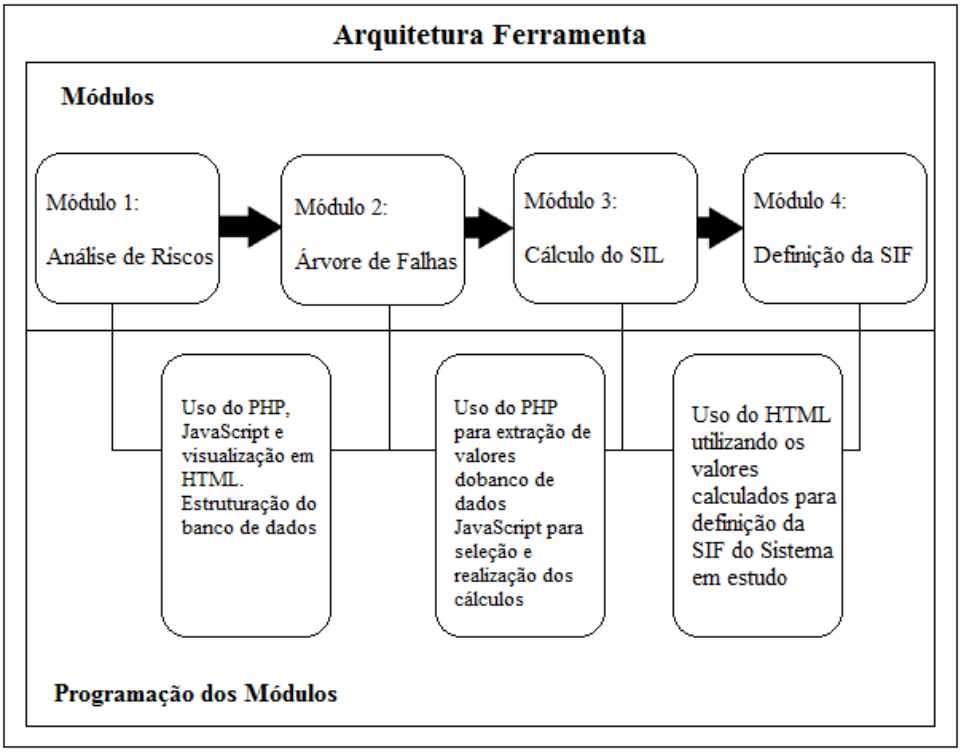
Fonte: Autoria Própria.

4 PROPOSTA DA FERRAMENTA

4.1 ARQUITETURA DA FERRAMENTA

A proposta deste trabalho consistiu no desenvolvimento de uma ferramenta de análise e projeto de um Sistema Instrumentado de Segurança (SIS), utilizando para isso programação em HTML, PHP e JavaScript, principais linguagens para programação web existentes atualmente, além de uma estruturação em banco de dados MySQL, devido ao seu desempenho, segurança e também quanto à aplicabilidade. Tal ferramenta é voltada para Web, permitindo ao usuário o acesso através de qualquer navegador em qualquer lugar do mundo, uma vez que será disponibilizada na Internet inicialmente num servidor de hospedagem gratuito para testes e depois em um domínio próprio. A ferramenta proposta sistematiza e descreve um procedimento adequado, usando técnicas normativas, para realização das etapas necessárias para o projeto de um SIS. A arquitetura da ferramenta é composta de 4 módulos parametrizados para o auxílio da construção de um SIS. A Figura 17 mostra a divisão implementada e o fluxograma de funcionamento da ferramenta.

Figura 17 – Módulos da Ferramenta.



Fonte: Autoria Própria.

- *Módulo 1 – Análise de Riscos*: Este módulo usa as questões fornecidas por Oreda (2009), apresentadas pela Tabela 2. Neste formulário, o usuário deve preencher as entradas para realização de um Estudo de Riscos e Operabilidade (HAZOP). Essas entradas são a identificação do sistema que contém a parte do processo em estudo, o parâmetro que será analisado e seu desvio, a possibilidade ou não de ocorrência de falhas no processo em questão, as causas de uma possível falha, as consequências dessas falhas, as proteções existentes no processo, o risco aceitável e as ações que serão executadas para evitar as falhas. O primeiro módulo da ferramenta é de extrema importância para o funcionamento uma vez que nele estão inseridos todo o levantamento de riscos inerentes aos processos do sistema em que se pretende a utilização de SIS. O Oreda (2009) vem auxiliar explicitando como é construída toda estrutura do HAZOP.

Tabela 8 – Descrição das Entradas e Saídas do Módulo 1 da Ferramenta.

MÓDULO 1	
Entradas	*Identificação*: contendo a parte em estudo, o local onde o estudo está sendo realizado, o elemento em questão e o efeito causado; *Parâmetro e Desvio*: o parâmetro analisado e o desvio relacionado ao parâmetro; *Possibilidade de Ocorrência*: existência ou não da possibilidade de ocorrência do evento; *Causas*: são inseridas as causas que possivelmente ocasionarão o evento; *Consequências*: são inseridas as consequências do evento sobre o sistema; *Proteção*: são inseridas as proteções existentes no projeto ou os métodos de operação; *Risco Aceitável*: são inseridos os riscos toleráveis pelo sistema; *Ações*: são inseridas as a ações necessárias para que o evento seja evitado.
Saídas	Todos os dados coletados, Identificação, Parâmetro e Desvio, Possibilidade de Ocorrência, Causas, Consequências, Proteção, Risco Aceitável e Ações, serão usados como saídas para o relatório final em pdf do HAZOP. As entradas de Identificação como, Parte, Local e Elemento servirão de saída para o Módulo 2, afim de se estabelecer a área do projeto e seus equipamentos para a realização da árvore de falhas.

Fonte: (Oreda, 2009).

- *Módulo 2 – Árvore de Falhas*: Com a Parte, Local e Elemento fornecidos pelas entradas do Módulo 1, é possível estruturar as entradas e saídas da árvore de falhas, utilizando os equipamentos selecionados pelo projetista caso um projeto novo ou os existentes caso esteja ocorrendo a manutenção. A Tabela 9 mostra a descrição das entradas e saídas do Módulo 2. A árvore de falhas (AAF) irá

quantificar os riscos matematicamente partindo de um evento topo e verificando a possibilidade de falhas de equipamentos específicos previamente salvos no banco de dados da ferramenta. A saída do Módulo 2 corresponde à Taxa de Acidentes Fatais (FAR) por ano calculados para cada parte ou malha do processo e que será usado no Módulo 3.

Tabela 9 – Descrição das Entradas e Saídas do Módulo 2 da Ferramenta.

MÓDULO 2	
Entradas	As entradas são os dados de identificação de riscos fornecidos pelo Módulo 1 acompanhados de todos os equipamentos dessa determinada área, fornecidos pelo projeto e pelas tabelas contendo os riscos de falhas de equipamentos previamente inseridas no banco de dados do projeto.
Saídas	A saída deste módulo fornece o valor da Taxa de Fatalidades (FAR) por ano para cada parte do processo em estudo e essencial para o Módulo 3.

Fonte: Autoria Própria.

- *Módulo 3 – Cálculo do SIL*: O Módulo 3 utiliza dos resultados obtidos pela Árvore de Falhas (AAF) para cálculo e obtenção do valor do SIL. A Tabela 10 apresenta as entradas e saídas para este módulo. O cálculo do SIL é importante para a definição de um SIS adequado ao sistema em estudo.

Tabela 10 – Descrição das Entradas e Saídas do Módulo 3 da Ferramenta

MÓDULO 3	
Entradas	A entrada é a taxa de fatalidades por ano usado para o cálculo final do SIL para cada parte do processo em estudo.
Saídas	As saídas são o Fator de Redução de Risco (RRF) e por comparação com a Tabela 5, o valor adequado do SIL para cada parte do processo em estudo.

Fonte: Autoria Própria.

- *Módulo 4 – Definição da SIF*: Com um valor necessário do SIL, é possível escolher a votação de redundância para a definição de uma SIF consistente a ser implementada pelo SIS. Dessa forma, tem-se a Tabela 11.

Tabela 11 – Descrição das Entradas e Saídas do Módulo 4 da Ferramenta.

MÓDULO 4	
Entradas	Como entrada o valor obtido para o SIL da parte em estudo realizado no Módulo 3.
Saídas	A definição de uma SIF a ser executada pelo SIS em caso de falha.

Fonte: Autoria Própria.

4.2 METODOLOGIA DE ANÁLISE E PROJETO

Apesar da evolução das técnicas e a disponibilidade de metodologias existentes, a elaboração do SIS orientada ao desempenho dos sistemas e da ampliação das responsabilidades dos profissionais que atuam nesta área é pouco difundida (BEGA et al, 2011). Não existe apenas uma única receita padrão para um projeto adequado de SIS. Além disso, a maioria dos trabalhos apresentam contribuições específicas em partes ou etapas componentes do projeto de um SIS. Dessa maneira elaborou-se a ferramenta com um procedimento empregando técnicas aceitas pelas normas IEC 61508 e IEC 61511.

4.2.1 MÉTODO DE ANÁLISE DE RISCO: HAZOP

Geralmente, empresas de consultoria que prestam serviços na área de segurança de processos consideram o estudo HAZOP como um item imprescindível em seus portfólios de serviços. Isto ocorre devido ao fato que indústrias dos mais diversificados segmentos de atuação contratam estes estudos como um complemento do projeto de engenharia básica. A implementação de sistemas de proteção, que se mostrem necessários após a análise dos resultados do HAZOP, é definida de acordo com o orçamento, demanda e cultura das empresas. Todavia, ao menos este estudo inicial de riscos é usualmente realizado pelas indústrias, representando um exame dos riscos do projeto.

A análise HAZOP é realizada pela ferramenta após uma revisão criteriosa das literaturas a cerca deste tema. Conforme exposto anteriormente, este estudo é um tipo de análise de riscos, que possui técnicas apuradas de investigação. Os resultados do estudo Riscos e Operabilidade evidencia a necessidade da implementação das funções instrumentadas de segurança, SIFs, a serem executadas pelo SIS.

Inicialmente, o HAZOP identifica no processo a parte, o local, o elemento e o efeito nos quais a análise será realizada, esta etapa é de vital importância para a elaboração do SIS em geral já que é usada posteriormente para a montagem da árvore de falhas e também para o cálculo individual do SIL. Após isso, o projetista deve informar qual é o

parâmetro essencial para esta parte do processo, aquele que, de acordo com um desvio pertinente, pode causar qualquer tipo de falha nos componentes dessa parte. Cabe também ao projetista avaliar se existe ou não possibilidade de ocorrência da falha em estudo, isso deve constar no documento gerado da análise de riscos. Finalmente devem ser levantadas todas as possíveis causas e consequências da ocorrência de tal evento dentro do sistema, o projetista deve evidenciar também as proteções já existentes que evitariam de qualquer forma a ocorrência do evento perigoso, além do risco aceitável para ocorrência de sinistro e as ações necessárias caso tal evento ocorra.

O HAZOP finalizado deve ser então armazenado em pastas que representem a parte que interessa no processo, datado para evitar futuras confusões já que esta análise deve ser feita a cada manutenção preventiva do sistema. A ferramenta então busca automatizar esta análise de forma a simplificar e economizar tempo ao usuário.

4.2.2 MÉTODO DE ANÁLISE DE ÁRVORE DE FALHAS (AAF)

A metodologia da Análise de Árvore de Falhas, ou simplificadamente AAF, consiste basicamente na produção de um sistema lógico dedutivo, que partindo de um evento indesejado, uma hipótese acidental, o chamado “Evento-Topo”, busca suas possíveis causas (SERPA, 2016). O Evento-Topo é identificado pela aplicação de técnicas específicas, para este caso o estudo HAZOP realizado pela ferramenta. O método usa a ramificação e avalia a possibilidade de “E/OU” eventos menores levarem o sistema ao evento-topo, por isso todas as variáveis probabilísticas são usadas para a formação da árvore.

De forma simplificada, primeiramente identifica-se o evento que se deseja obter, como por exemplo a taxa de fatalidades num ano causadas por falhas ou erros humanos num processo. Para se chegar nesse evento, estrutura-se diversos ramos contendo eventos menores como falhas em equipamentos específicos, erros humanos ou a presença de pessoas na área, tudo isso tem que ser analisado e levado em conta. Posteriormente, se estabelecem relações entre os eventos menores. Essas relações podem ser aditivas, se um evento “OU” outro evento acontece, ou multiplicativas, se um evento “E” outro evento acontecem, dependendo de qual for o caso deve-se somar ou multiplicar as probabilidades de cada acontecimento. Por exemplo tem-se a probabilidade x de um episódio A acontecer e uma probabilidade y de outro B acontecer, sabendo-se que o para o evento-topo ocorrer A OU B deve ocorrer, então a probabilidade desse evento-topo existir é x + y. De forma

análoga se um evento-topo necessitar de que A E B aconteçam, então a probabilidade desse evento-topo existir é x × y. Basta se realizar a análise a partir de acontecimentos menores necessários para causar um de maior proporção e se medir baseando-se nas probabilidades conhecidas desses eventos menores a probabilidade do evento-topo.

A AAF usa a identificação da parte do processo levantada pelo HAZOP e avalia qual evento pode ocorrer neste local através do parâmetro e desvio estudados também pela análise de riscos. Com isso monta-se uma estrutura ramificada, por isso o nome árvore de falhas, avaliando e quantificando em cada ramo os fatores responsáveis para ocorrência de tal evento-topo. Esses fatores são fornecidos por manuais escritos como Oreda (2009) e também por bancos de dados já elaborados manualmente com essas informações.

A proposta utilizará um banco de dados programado antecipadamente com os dados de Oreda (2009), contendo as informações de falhas de equipamentos e montar com JavaScript uma árvore ramificada, visualmente fácil de se avaliar o evento topo dando como saída a Taxa de Fatalidades por ano decorrentes dos eventos menores e assim possibilitar o cálculo do SIL da parte do processo em estudo.

4.3 SISTEMATIZAÇÃO DOS CÁLCULOS

Os dados expostos no documento Oreda (2009) indicam a taxa de falha por 10^6 horas de operação, todavia, a fim de auxiliar a manipulação destes dados, foram utilizados neste trabalho valores para taxa de falha por ano como estipulado pela norma IEC 61508 (2010). Sabe-se que 1 ano é igual a 365 dias, cada dia tem 24 horas, dessa forma 1 ano possui 8760 horas. A Equação 1 mostra o cálculo da taxa de falhas por ano.

$$Taxa\ de\ falha\ por\ ano\ = \frac{Taxa\ de\ falha\ por\ 10^6 horas\ \times\ 8760}{10^6}$$

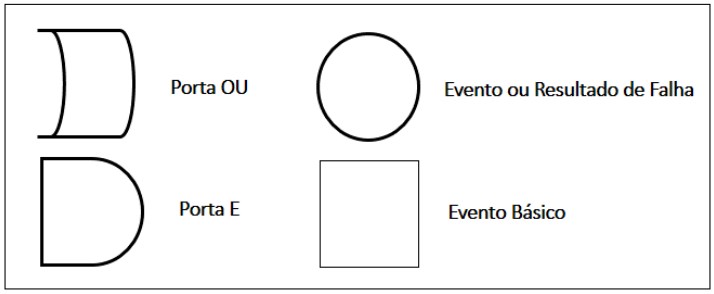
Equação 1 – Conversão da taxa de falhas por 10^6 horas para taxa de falhas por ano.

Os elementos presentes em uma malha de controle atuam em conjunto, sendo que a falha de um instrumento pode acarretar em distúrbios aos demais equipamentos. Sendo assim, a análise da avaliação de riscos deve ser executada utilizando ferramentas completas, que permitam relacionar todos os elementos e fatores que possam contribuir direta ou indiretamente na manifestação do risco. E um dos procedimentos para análise

da avaliação de riscos mais completo é a Árvore de Falhas. O conceito de Árvores de Falhas é uma ajuda valiosa na avaliação dos riscos e no desenvolvimento de sistemas de proteção. Este procedimento é normalmente empregado quando o estudo HAZOP identifica algum evento potencialmente perigoso e a equipe de segurança de processos solicita uma análise da probabilidade e consequências. (MACDONALD, 2004).

Desta maneira, a análise da Árvore de Falhas permite uma relação lógica de probabilidades utilizando alguns símbolos, conforme a Figura 18 ilustra.

Figura 18 – Símbolos utilizados na análise Árvore de Falhas.



Fonte: (GOBLE & CHEDDIE, 2005).

Estas portas utilizadas na análise podem receber informações em suas entradas que são classificadas de diferentes maneiras (MACDONALD, 2004):

P = Probabilidade de o evento ocorrer;

f = Frequência do Evento;

f x t = Duração do Evento.

A variável probabilidade está diretamente relacionada com a frequência, as quais estão inter-relacionadas através da Equação 2 (CROWL & LOUVAS, 2002).

$$Taxa\ de\ falho\ por\ ano = \mu$$

$$Confiabilidade = R$$

$$R = e^{-\mu t}$$

$$P = 1 - R$$

Equação 2 - Relação entre probabilidade e frequência.

As portas “OU” e “E” atuam de maneiras distintas, de acordo com as combinações de variáveis possíveis em suas entradas. A Tabela 12 expõe os comportamentos esperados nas saídas destas portas, de acordo com suas respectivas entradas.

Tabela 12 – Regras de combinações utilizando a análise Árvore de Falhas.

Entrada	Porta	Operação	Saída da Porta
P_1, P_2	E	$P_1 \times P_2$	P
P_1, f_1		$P_1 \times f_1$	f
$(f_1 \times t_1)$, $(f_2 \times t_2)$		$(f_1 \times f_2)$ $(t_1 + t_2)$	f
P_1, P_2	OU	P_1, $+ P_2$	P
f_1 ,f_2		f_1 ,$+ f_2$	f

Fonte: (MACDONALD, 2004).

Resumidamente, a porta “E” é mais completa, visto que permite a combinação nas entradas das variáveis “probabilidade” e “frequência”. A saída desta porta é obtida através da multiplicação dos eventos, sendo que todos os eventos precisam ser verdade para que o resultado da falha se torne verdade.

Por outro lado, a porta “OU” permite apenas relações entre variáveis do mesmo tipo, não sendo possível a relação entre “probabilidade” e “frequência” na mesma porta. Todavia, a saída desta porta é obtida pela simples soma de todos os eventos de entrada.

4.3.1 TAXA DE ACIDENTES FATAIS

A avaliação dos riscos realizada através da ferramenta Árvore de Falhas permite quantificar o evento ou resultado de falha. Todavia, associando às falhas dos componentes e dos operadores de uma malha de processos, com outros fatores externos às estas malhas, é possível alcançar como resultado da falha um acidente fatal.

A taxa de acidentes fatais (*Fatal Accident Rate - FAR*) é dada como o número de fatalidades por 10^8 horas trabalhadas no local onde o perigo está presente. Grosseiramente, uma pessoa que trabalha por 50 anos irá acumular 10^5 horas trabalhadas, assim como se 50 pessoas trabalharem durante 1 ano. Assim, se 1000 pessoas trabalharem por mais de 50 anos irão acumular 10^8 horas de exposição no ambiente de trabalho (MACDONALD, 2004).

Assim, a taxa de fatalidades por ano exposta pela análise Árvore de Falhas se relaciona com o FAR sem proteções através da Equação 3.

$$FAR = \frac{Taxa\ de\ Fatalidades\ por\ ano\ \times 10^8}{Total\ de\ horas\ trabalhadas\ por\ todos\ os\ empregados\ durante\ o\ período\ coberto}$$

Equação 3 - Relação entre taxa de fatalidades ano exposta na análise Árvore de falhas com o índice FAR (CROWL & LOUVAS, 2002).

Sendo que a taxa de horas trabalhadas por todos os empregados durante o período coberto está relacionada com o número de operários que estão diretamente expostos a estes riscos, e que poderão ser uma vítima fatal do mesmo.

Por outro lado, toda empresa que busca implementar um sistema de segurança de processos deve quantificar uma meta, estabelecendo o valor para a taxa de acidentes fatais que deve ser atingida após a inserção destes sistemas de segurança. Esta taxa é conhecida como FAR tolerável, sendo que geralmente possui valores decimais, como:

$$FAR\ tolerável = 0{,}2$$

Desta forma, estas taxas de fatalidade com e sem proteção se relacionam, resultando no índice Fator de Redução de Riscos (RRF), ou também conhecido como *Risk Reduction Factor* (RRF), o qual pode ser obtido através da Equação 4.

$$RRF = \frac{FAR\ sem\ proteção}{FAR\ tolerável}$$

Equação 4 - Cálculo do fator de redução de riscos (MACDONALD, 2004).

O fator de redução de riscos desta fórmula mostra qual a taxa global que se deve aplicar a fim de que ao final se tenha alcançado o risco residual desejado e aceitável (FREIRE, 2013).

O fator de redução de riscos influencia diretamente na obtenção do nível de integridade seguro, ou *Safety* Integrity Level (SIL). A medida da quantidade de redução do risco fornecida por um sistema de segurança é chamada de integridade da segurança (MACDONALD, 2004). Logo, à medida que definimos o RRF para um eminente risco, o SIL pode ser obtido através de uma simples análise dos dados presentes na Tabela 4.

4.3.2 OBTENÇÃO DO NÍVEL DE INTEGRIDADE DE SEGURANÇA (SIL)

O SIL representa o nível discreto para especificação dos requerimentos de integridade de segurança das funções a serem alocadas no SIS. A Tabela 4 apresenta como é possível encontrar o valor do SIL pelo uso do fator de redução de riscos (RRF). De acordo com Macdonald (2004), a medida da quantidade de redução do risco fornecida por um sistema de segurança é chamada integridade de segurança, logo, a medida que se define o RRF para um risco eminente.

5 DESENVOLVIMENTO DA FERRAMENTA

5.1 DESCRIÇÃO DO FUNCIONAMENTO

Para facilitar a compreensão do funcionamento da ferramenta, as telas principais e operação dos módulos são apresentados. Um vídeo tutorial de uso está disponível e é recomendado para facilitar a compreensão e usabilidade da ferramenta (https://youtu.be/jRf5msfsFDI). A ferramenta possui uma tela inicial na qual o usuário devidamente cadastrado insere login e senha. Essa primeira tela dará acesso ao programa principal que possui os procedimentos normativos necessários para análise de riscos e cálculo do SIL. A Figura 19 apresenta os campos de login e senha.

Figura 19 – Tela Inicial.

Fonte: Autoria Própria.

Uma vez tendo acesso ao programa, Figura 20, o usuário deve iniciar um projeto. A ferramenta conta com um painel visual, dinâmico e de fácil entendimento para que todos os usuários possam criar novos projetos. A Figura 20 apresenta essa parte do sistema. Esta etapa é simples, mas importante na estruturação do banco de dados. Cada projeto possui um Nome e se outros projetos possuírem nomes iguais, o programa usa a

Área como separador. Caso a área também tenha nomes idênticos, a Data então é usada como diferencial.

Figura 20 – Tela Principal do Programa.

Fonte: Autoria Própria.

Figura 21 – Primeira Parte do Sistema: Projetos.

Fonte: Autoria Própria.

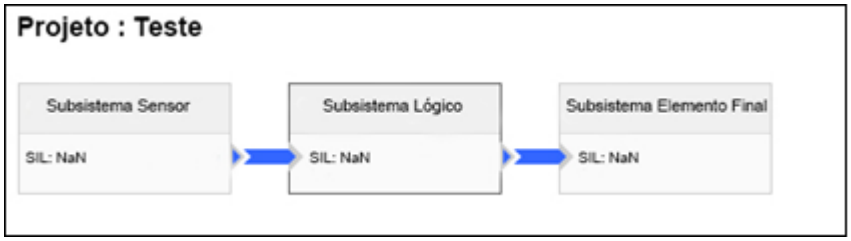
Todos os projetos criados são então disponibilizados na aba “Meus Projetos” e os usuários podem carregá-los e até mesmo deletá-los se necessário. Essa aba é apresentada na Figura 22.

Figura 22 – Projetos Salvos.

Fonte: Autoria Própria.

A partir da criação de um novo projeto, o ambiente de trabalho permite a divisão do projeto em subsistemas como descritos pela norma IEC 61511 (2003). Essa funcionalidade facilita a próxima etapa de análise de risco (HAZOP) e também realiza checklist dos equipamentos que compõe os subsistemas do processo em análise, como mostrado pela Figura 23.

Figura 23 – Divisão de Subsistemas.



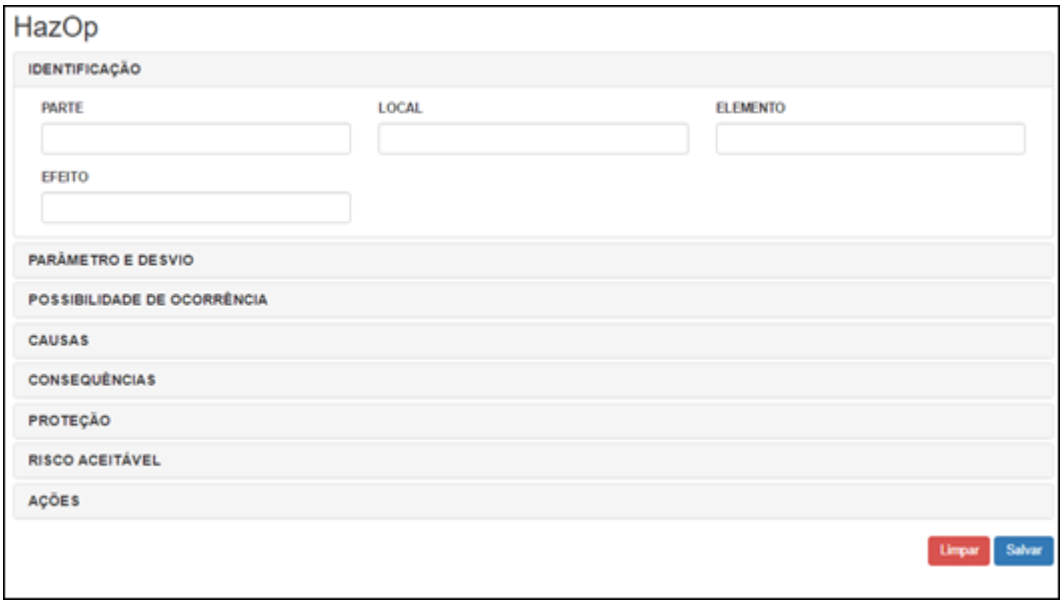
Fonte: Autoria Própria.

Após a divisão dos subsistemas, o usuário pode iniciar preenchimento dos dados para a análise de risco,Figura 24, de cada processo composto por um subsistema sensor-controlador-atuador. Os campos existentes para inserção dos dados foram estudados e retirados de Oreda (2009), um importante documento usado para análise de riscos em processos.

Esse primeiro procedimento implementa o estudo HAZOP, um método sistemático utilizado para quantificação de falhas em determinados processos e geralmente feito manualmente com perguntas e palavras-chave (uso das Tabelas 1 e 2), permitindo ao projetista levantar todas as informações de possíveis erros e falhas inerentes ao processo. O teste HAZOP foi implementado usando programação em JavaScript com maior simplicidade para o preenchimento do usuário e depois inserido em banco de dados com auxílio da linguagem PHP. No banco de dados são inseridas todas

as informações relevantes ao projeto, as quais podem ser editadas pelo projetista a qualquer momento, conforme podem ser visualizadas na Figura 24.

Figura 24 – Segunda Parte do Sistema: HAZOP Visão Geral.



Fonte: Autoria Própria.

Os dados de Identificação, que compõe a Figura 24, são importantes para a estruturação do estudo HAZOP e correspondem à a primeira etapa desenvolvida pelo projetista. De acordo com a Figura 25, os dados de identificação são: a Parte relacionada à parte do processo em análise, o Local relacionado ao local do processo em análise, o Elemento relacionado a qual subsistema sensor/controlador/atuador e Efeito que corresponde ao efeito causado por aquele elemento no processo. O fornecimento desses dados são essências para a construção da Árvore de Falhas (AAF).

Figura 25 – Campos dos dados Identificação do HAZOP na Ferramenta.

Fonte: Autoria Própria.

O Parâmetro e o Desvio são os campos de determinação do parâmetro em estudo, ou seja, a variável do processo que pode ocasionar a falha no sistema bem como seu desvio fornecido por Oreda (2009) e presentes na Tabela 1como mostrado na Figura 26.

Figura 26 – Dados de Parâmetro e de Desvio do HAZOP na ferramenta.

Fonte: Autoria Própria.

A Possibilidade de Ocorrência é o dado que avalia a viabilidade de ocorrência da falha ou sinistro em estudo, como mostrado na Figura 27

Figura 27 - Possibilidade de Ocorrência.

Fonte: Autoria Própria.

O dado de entrada Causas permite o cadastramento dos motivos que possivelmente ocasionarão um evento falha no processo. O cadastramento dos motivos é feito via texto como visto na Figura 28.

Figura 28 – Causas dos Possíveis Eventos-Falha.

Fonte: Autoria Própria.

As possíveis consequências causadas pelo evento falha sobre o sistema devem ser cadastradas na ferramenta a partir do campo Consequências mostrado na Figura 29.

Figura 29 – Consequências dos Possíveis Eventos-Falha.

Fonte: Autoria Própria.

No HAZOP, também devem ser inseridas as proteções existentes contra acidentes e falhas no projeto ou na operação do sistema em análise. A Figura 30 mostra o espaço destinado ao cadastramento dessas informações.

Figura 30 – Proteção existente contra falhas no sistema.

Fonte: Autoria Própria.

Existe também um campo específico para o cadastramento das informações sobre riscos toleráveis para o sistema como apresentado pela Figura 31.

Figura 31 – Risco Aceitável para o Sistema.

Fonte: Autoria Própria.

Finalizando o cadastramento de informações referentes ao módulo 1 da ferramenta, o usuário deve preencher as ações necessárias para que o evento falha ou sinistro elencados pelo HAZOP sejam evitados de modo rápido e eficiente. A Figura 32 apresenta o campo onde o projetista insere as ações necessárias. Estas ações podem estar relacionadas ou podem nortear a definição das funções de segurança (SIFs) que deverão ser implementadas pelo SIS.

Figura 32 – Ações necessárias em caso de falhas.

Fonte: Autoria Própria.

Um banco de dados projetado em MySQL é responsável por receber todos os dados de entrada do módulo 1 da ferramenta e gerar um relatório de análise de riscos para a parte do sistema sob exame. Este relatório da análise de riscos é um requisito para implantação de um SIS. A Figura 33 mostra a estruturação da tabela do banco de dados.

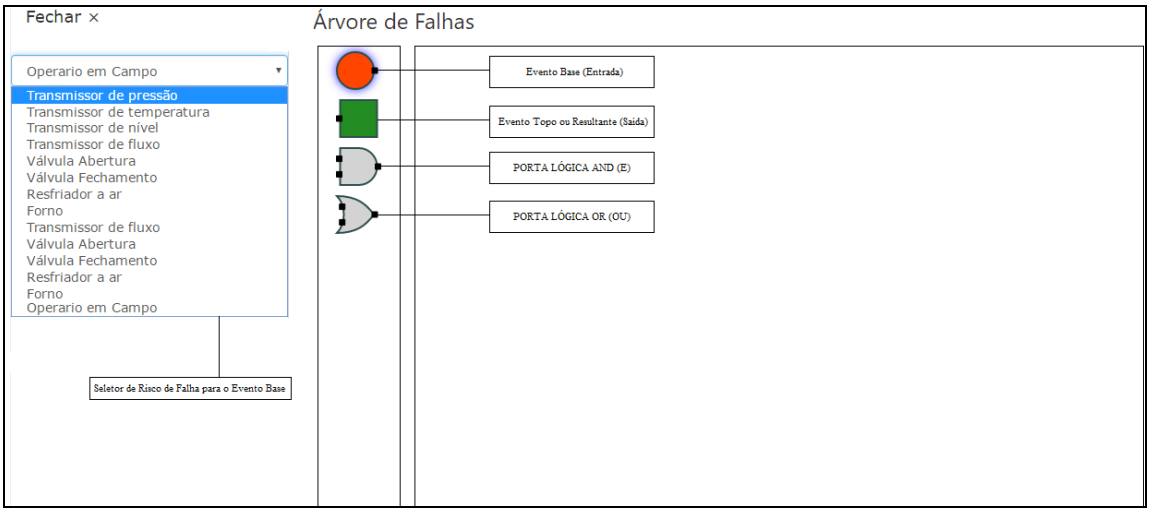
Figura 33 – Tabela do banco de dados do HAZOP.

id	parte	local	elemento	efeito	parametro	desvio	po	causas	consequencias	protecao	ra	acoes

Fonte: Autoria Própria.

A próxima etapa da ferramenta está relacionada à execução do Módulo 2 da Análise de Árvore de Falhas (AAF). A AAF foi implementada em JavaScript e resumidamente estuda todas as possibilidades de um evento ocorrer. Nesta etapa, a ferramenta permite a elaboração de uma árvore de falhas visual através de um diagrama com entradas, saídas e elementos lógicos. Este é o grande diferencial obtido pela ferramenta com a adoção do método AAF para quantificação de riscos. Através de um duplo-clique sobre a entrada (ícone laranja), é possível selecionar o equipamento (subsistema sensor, controlado ou atuador) estudado pelo teste HAZOP. A Figura 34 apresenta a elaboração da árvore de falhas descrita.

Figura 34 – Terceira Parte do Sistema: Árvore de Falhas.



Fonte: Autoria Própria.

A terceira etapa da ferramenta, após a elaboração da árvore de falhas, está relacionada à execução do Módulo 3 de Cálculo do SIL. Esta etapa envolve o cálculo sistemático da taxa de acidentes fatais (FAR), do fator de redução de riscos (RRF) e da descoberta do valor do SIL adequado a parte do projeto em questão. Estes três cálculos são dependentes uns dos outros como demonstrado anteriormente na seção 4.3 e por isso são apresentados juntos.

O cálculo da FAR é obtido através da árvore de falhas e por isso o procedimento anterior é de extrema importância para o funcionamento geral da ferramenta. Com o valor da FAR, é possível calcular o RRF e por comparação, usando a Tabela 4 disponibilizada na ferramenta, é possível obter o valor adequado para o SIL.

A apresentação desses valores de saída do módulo 3 pode ser vista na Figura 35. A realização dos cálculos é feita por código JavaScript de forma instantânea.

Figura 35 – Quarta Parte do Sistema: Obtenção do SIL.

Fonte: Autoria Própria.

5.2 VALIDAÇÃO

Com o objetivo de validar o funcionamento da ferramenta e mostrar a aplicação do procedimento proposto, utilizou-se os dados do trabalho de Freire (2013) como dados de entrada para uso na ferramenta. É importante esclarecer que os dados do trabalho de Freire (2013) são reais, fornecidos por uma empresa multinacional parceira (identidade não revelada por solicitação da empresa).

Freire (2013) descreve os procedimentos manuais para a análise de riscos HAZOP e cálculo do SIL de uma planta desbutanizadora. O foco neste estudo foi para o processo de desbutanização, que por ser uma das últimas etapas do processamento do gás natural, é responsável por gerar dois produtos de alto valor agregado: a gasolina natural (C5+) e o gás liquefeito de petróleo (GLP). Esses dados foram usados na ferramenta de projeto de SIS desenvolvida e os resultados foram comparados para fins de validação.

Os resultados do HAZOP em Freire (2013) evidenciaram a necessidade da implementação de três funções instrumentadas de segurança a serem executadas pelo SIS. Estas funções se referem aos riscos:

- Pressão alta no topo da torre desbutanizadora;
- Nível baixo no fundo da torre desbutanizadora;
- Temperatura alta no fundo da torre desbutanizadora.

Para fins de simplificação, considerando que as análises e procedimentos são os mesmos de forma repetida na ferramenta, o risco Nível baixo no fundo da torre desbutanizadora serve como exemplo considerável para a validação da ferramenta. A Figura 36 apresenta a realização do estudo HAZOP que constata a necessidade de implementação de funções de segurança para o parâmetro (Nível).

Figura 36 – HAZOP Nível Fundo da Torre.

Sistema:				
Planta Desbutanizadora				
Parte	**Elemento**	**Parâmetro**	**Desvio**	**Efeito**
Processamento de LGN	Produtos internos à Torre Desbutanizadora	Nível no Fundo da Torre	Menos	Tanque Esvaziando
É possível ocorrer?	Sim			
Causas	Falha na malha LC-011 / FIC-010. Falha na malha PC-008.			
Consequências	Gases poderão ser liberados nas tubulações de saída do C5+ no fundo da torre			
Proteção	Alarme com Alta prioridade. Ação do SIS.			
Risco Aceitável	Não.			
O que pode ser feito	Liberação de gases no topo da Torre Desbutanizadora. Redução no envio de C5+ para armazenagem.			
Ação	O operador deve fechar a válvula FV-103, e abrir a válvula PV-100. O SIS deve possuir uma malha que realiza a liberação máxima de gases no topo da Torre Desbutanizadora e corte no envio de C5+ para armazenagem.			

Fonte: Adaptado de (Freire, 2013).

De acordo com os procedimentos de uso da ferramenta apresentados na seção 5.1, os dados do processo (Planta Desbutanizadora) necessários para criação do projeto do sistema da planta desbutanizadora contendo a Data e Área onde será realizado o HAZOP são cadastrados como mostrado pela Figura 37

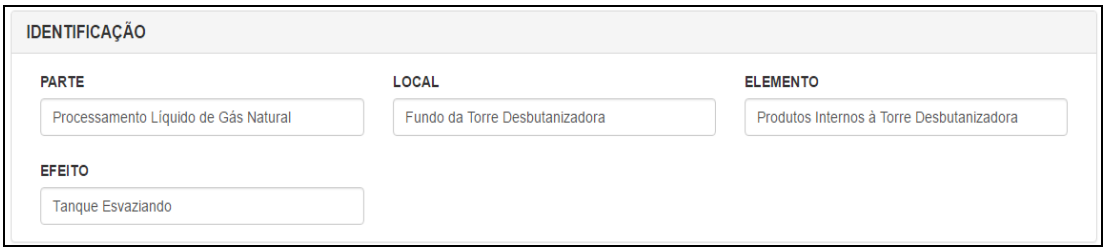
Figura 37 – Dados de Entrada Planta Desbutanizadora.

Fonte: Autoria Própria.

Com a criação da nova área do projeto, é possível cadastrar os dados do HAZOP, de acordo com as entradas do Módulo 1 da ferramenta apresentados pela Tabela 6. Portanto, o preenchimento de cada campo pode ser visto da Figura 38 a Figura 45.

É necessário inicialmente inserir todos os dados da Identificação do HAZOP especificando corretamente a Parte, Local, Elemento e o Efeito. Estes dados serão importantes na criação das tabelas do Módulo 2. A Figura 38 apresenta os dados de entrada de Identificação.

Figura 38 – Identificação HAZOP Torre Planta Desbutanizadora.



Fonte: Autoria Própria.

Posteriormente, na Figura 39 se constata a aquisição do Parâmetro, variável na qual é feito o estudo de riscos, e do Desvio necessário para se saber o que acontece com a variável num evento-falha.

Figura 39 – Parâmetro e Desvio HAZOP Torre Planta Desbutanizadora.

Fonte: Autoria Própria.

A Figura 40 mostra a possibilidade do evento ocorrer ou não atendendo a necessidade do HAZOP.

Figura 40 – Possibilidade de Ocorrência HAZOP Torre Planta Desbutanizadora.

Fonte: Autoria Própria.

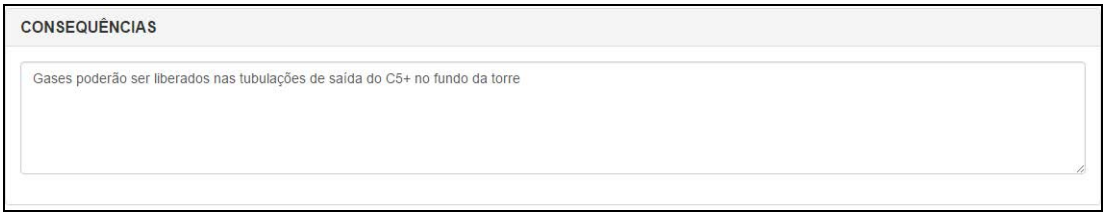
As Causas, como demonstrado pela Figura 41, são inseridas corretamente e separadamente em texto, necessárias para se levantar os motivos das falhas e para gerar o relatório final do Módulo 1.

Figura 41 – Causas HAZOP Torre Planta Desbutanizadora.

Fonte: Autoria Própria.

As Consequências, como visualizado na Figura 42, são inseridas corretamente e separadamente em texto, havendo sua necessidade para se avaliar as consequências das falhas e também gerar o relatório final do Módulo 1.

Figura 42 – Consequências HAZOP Torre Planta Desbutanizadora.



Fonte: Autoria Própria.

Proteção, além de ser usada no relatório do Módulo 1, deve ser cadastrada servindo de alerta, a quem tiver acesso ao HAZOP, daquilo que já existe no sistema e que pode impedir o sistema de falhar ou levá-lo ao estado seguro. A Figura 43 apresenta o cadastramento desse campo.

Figura 43 – Proteção HAZOP Torre Planta Desbutanizadora.

Fonte: Autoria Própria.

O Risco Aceitável deve ser cadastrado para demonstrar até quanto determinado subsistema em análise encontra-se suscetível ao risco e para gerar o relatório do Módulo 1 A Figura 44 apresenta tal campo, para este exemplo é interessante perceber que não existem riscos aceitáveis.

Figura 44 – Risco Aceitável HAZOP Torre Planta Desbutanizadora.

Fonte: Autoria Própria.

As Ações, como demonstrado na Figura 45, são inseridas corretamente em texto, sendo necessárias para se estudar as providências que podem ser tomadas para evitar falhas graves e para gerar o relatório final do Módulo 1.

Figura 45 – Ações HAZOP Torre Planta Desbutanizadora.

Fonte: Autoria Própria.

Os dados de entrada cadastrados para a execução do Módulo 1 da ferramenta também são salvos no banco de dados e permitem que a ferramenta gere relatórios da análise HAZOP conforme requisitado pelo projeto do SIS. O relatório do estudo HAZOP gerado para o caso de estudo da validação é apresentado no Anexo A.

Após a identificação dos subsistemas que necessitam da inserção de funções de segurança pelo HAZOP, Freire (2013) busca quantificar estes riscos analisando os elementos do processo envolvidos. As frequências de falha por ano dos elementos do estudo de caso foram obtidas em Oreda (2009), sendo os principais mostrados na Tabela 13.

Tabela 13 – Frequência de falha por ano dos possíveis elementos causadores dos riscos expostos pelo HAZOP.

Instrumento	**Tipo de Falha**	**Frequência de falha por ano**
Transmissor de pressão	Modo de falha degradado	0,0465
Transmissor de temperatura	Falha crítica em demanda	0,0196

Transmissor de nível	Falha crítica em demanda	0,0041
Transmissor de fluxo	Falha crítica em demanda	0,0233
Válvula	Falha em demanda na abertura	0,0106
Válvula	Falha em demanda no fechamento	0,022
Resfriador a ar	Falha crítica em demanda, podendo emitir faíscas	0,075
Forno	Superaquecimento, podendo gerar labaredas	0,1786

Fonte: (Oreda, 2009).

Estas frequências de falhas, entre outras listadas e descritas por Oreda (2009), foram previamente cadastradas em uma tabela do banco de dados, pois quando forem requisitadas serão fornecidas automaticamente pela ferramenta. A Figura 46 exemplifica essa tabela contendo as frequências de falhas por ano, mostrada no banco de dados como FFA.

Figura 46 – Frequência de falha por ano dos possíveis elementos causadores dos riscos expostos pelo HAZOP salvas em banco de dados.

equipamento	tipo de falha	FFA
Transmissor de pressão	Modo de falha degradado	0.0465
Transmissor de temperatura	Falha crítica em demanda	0.0196
Transmissor de nível	Falha crítica em demanda	0.0041
Transmissor de nível	Falha crítica em demanda	0.0041
Transmissor de fluxo	Falha crítica em demanda	0.0233
Válvula Abertura	Falha em demanda na abertura	0.0106
Válvula Fechamento	Falha em demanda na fechamento	0.022
Resfriador a ar	Falha crítica em demanda, podendo emitir faíscas	0.075
Forno	Superaquecimento, podendo gerar labaredas	0.1786
Transmissor de fluxo	Falha crítica em demanda	0.0233
Válvula Abertura	Falha em demanda na abertura	0.0106
Válvula Fechamento	Falha em demanda na fechamento	0.022
Resfriador a ar	Falha crítica em demanda, podendo emitir faíscas	0.075
Forno	Superaquecimento, podendo gerar labaredas	0.1786
Operario em Campo	Humana	0.8

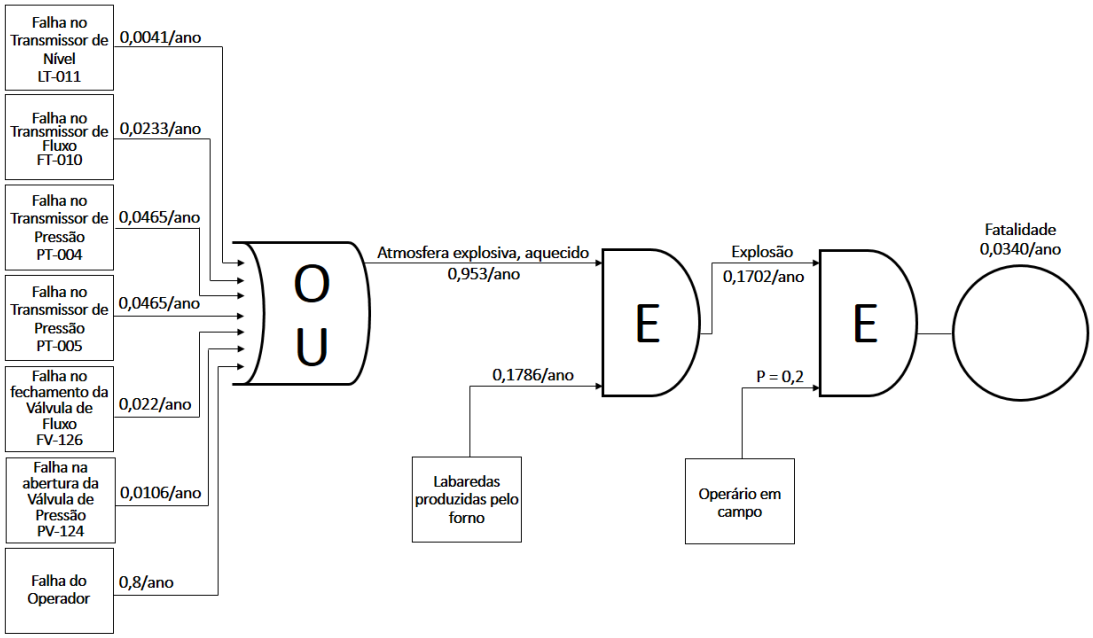
Fonte: Autoria Própria.

Em adição à frequência de falha dos equipamentos, também pode se considerar o risco de falha humana do operador destes equipamentos, no que se refere à uma falha crítica do mesmo, em momento de demanda. O valor dessa frequência de falhas no ano é

de 80% (0,8) e deve ser considerada pela Árvore de Falhas toda vez em que houver no mínimo um operador em campo.

Freire (2013) constrói manualmente uma árvore de falhas quantificando os riscos para se obter o valor da taxa de fatalidades por ano. A Figura 47 mostra a árvore de falhas para esta parte do processo.

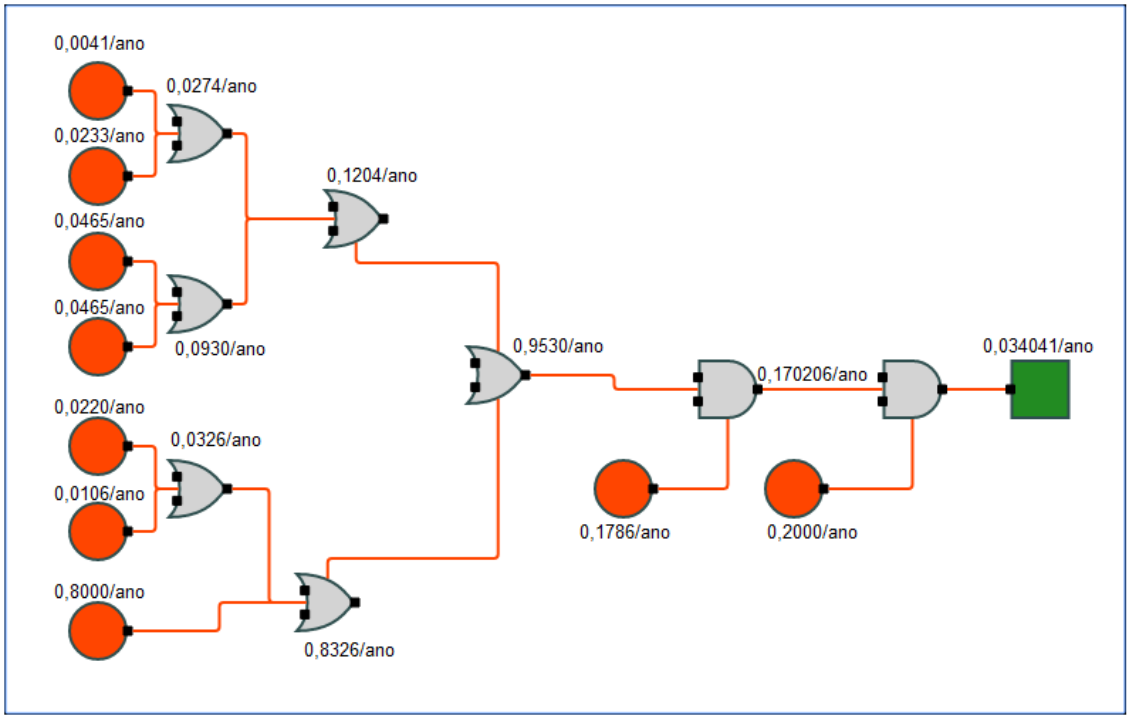
Figura 47 – Árvore de Falhas para o Nível Baixo Fundo da Torre Manual.



Fonte: Adaptado de (Freire, 2013).

Utilizando dos mesmos conceitos, a ferramenta desenvolvida permite a construção da árvore de falhas em ambiente visual e interativo para obtenção da taxa de fatalidades por ano como observado na Figura 48.

Figura 48 – Árvore de Falhas para o Nível Baixo Fundo da Torre Ferramenta.



Fonte: Autoria Própria.

O Fator de Redução de Riscos (RRF), conforme exposto anteriormente pela Equação 4, utiliza como variáveis a Taxa de Acidentes Fatais (FAR), Equação 3, resultante da avaliação dos riscos, dividida pelo valor FAR aceitável para o projeto. Para este projeto de implantação do Sistema Instrumentado de Segurança, utiliza-se o valor de FAR tolerável de 0,2.

Freire (2013) calcula o valor do FAR e do RRF através das Equações 3 e 4 como pode ser observado a seguir.

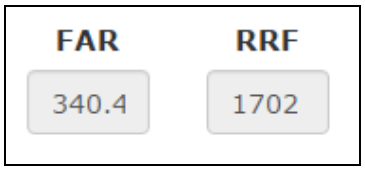
$$FAR\ sem\ proteção = Fatalidades\ \times 10000$$

$$FAR\ sem\ proteção = 0{,}0340\ \times 10000 = \ 340$$

$$RRF = \frac{FAR\ sem\ proteção}{FAR\ tolerável} = \frac{340}{0{,}2} = 1700$$

A ferramenta calcula automaticamente os valores do FAR e do RRF, conforme pode ser visualizado na Figura 49.

Figura 49 – Cálculo dos Valores dos da FAR e RRF pela Ferramenta.



Fonte: Autoria Própria.

Finalmente, utilizando comparação com a Tabela 4, Freire (2013) obtém um valor correto para o SIL dessa parte do sistema. De acordo com a Tabela 4, para um valor de RRF de 1700 o valor adequado para o SIL deve ser o 3.

A ferramenta utiliza também de comparação para calcular um SIL, com dados inseridos na programação também da mesma tabela. Na Figura 50 é possível observar que o valor do SIL calculado pela ferramenta em comparação ao calculado manualmente no trabalho de Freire (2013) é o mesmo.

Figura 50 – Cálculo do SIL pela Ferramenta.

Fonte: Autoria Própria.

Para fins de comparação entre os resultados obtidos pela ferramenta desenvolvida e o trabalho de Freire (2013), repetiu-se o procedimento de uso da ferramenta para a análise dos outros riscos levantados: Pressão alta no topo da torre desbutanizadora e Temperatura alta no fundo da torre desbutanizadora. A Tabela 14 compila e apresenta uma comparação dos resultados para os valores teóricos e os calculados pela ferramenta.

Tabela 14 – Resultados Teóricos x Calculados pela Ferramenta.

Parâmetro/ Desvio/ Local	**FAR Teórico**	**FAR Ferramenta**	**RRF Teórico**	**RRF Ferramenta**	**SIL Teórico**	**SIL Ferramenta**
Pressão/ Mais/ Fundo da Torre	135	135,54	675	677,70	SIL 2	SIL 2
Temperatura / Mais/ Fundo da Torre	332	332,562	1660	1662,78	SIL 3	SIL 3
Nível/ Menos/ Fundo da Torre	340	340,40	1700	1702,00	SIL 3	SIL 3

Fonte: Autoria Própria.

Observando os valores da Tabela 14, a ferramenta foi validada por obter o mesmo resultado que o calculado manualmente no trabalho de referência e realizou o preenchimento do estudo de riscos salvando-os em banco de dados para posterior criação dos relatórios de todos os módulos do projeto. Além de se obter o mesmo valor, nota-se também que o tempo de realização do projeto cai drasticamente, uma vez que essa validação foi realizada em alguns minutos e o trabalho manual foi executado em semanas. Este fato constata a automatização de um procedimento anteriormente extremamente maçante e com alto índice de erros.

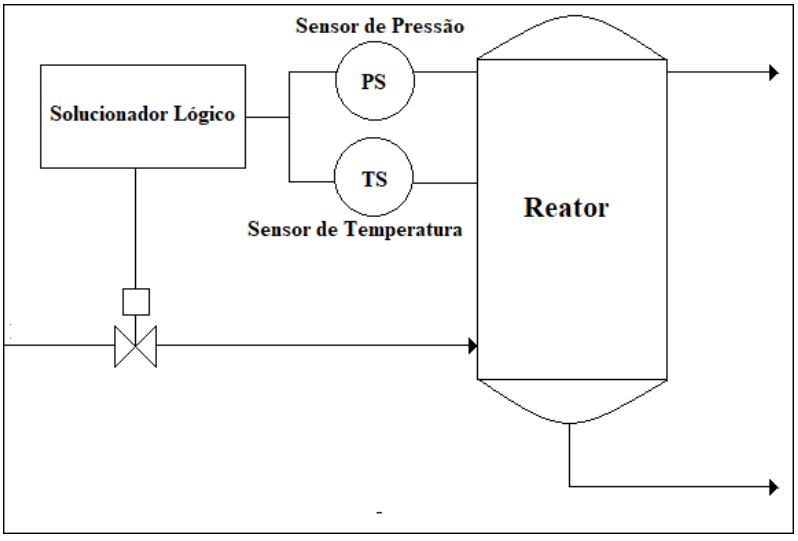
6 CASOS DE ESTUDO

Para testar a ferramenta foram selecionados diversos casos de estudo reais da indústria de processo disponíveis na literatura relacionado ao tema de projeto de SIS. Esses casos de estudo foram divididos por complexidade, podendo-se desta maneira demonstrar a eficiência e flexibilidade de uso da ferramenta desenvolvida para diferentes tipos de processos, tipos de variáveis e quantidade de malhas de controle de processo, configurações de redundância, verificando a exatidão dos resultados obtidos com a sua aplicação em comparação aos dados da literatura.

6.1 CASO DE ESTUDO 1 – PLANTA QUÍMICA

O primeiro caso de estudo tem relação com o reator de uma planta química que pode ser encontrada em Goble e Cheddie (2005). Reatores são usados em plantas químicas para a produção de uma vasta gama de produtos e em sua maioria são exotérmicos. A temperatura e pressão envolvidas nesse processo podem subir rapidamente se uma reação ocorrer. Assim a necessidade do SIS é identificada para o processo em estudo como mostrado pela Figura 50.

Figura 51 – Processo do Reator.



Fonte: (GOBLE & CHEDDIE, 2005).

Goble e Cheddie (2005) realizam a análise de riscos do reator conforme mostrado na Tabela 15.

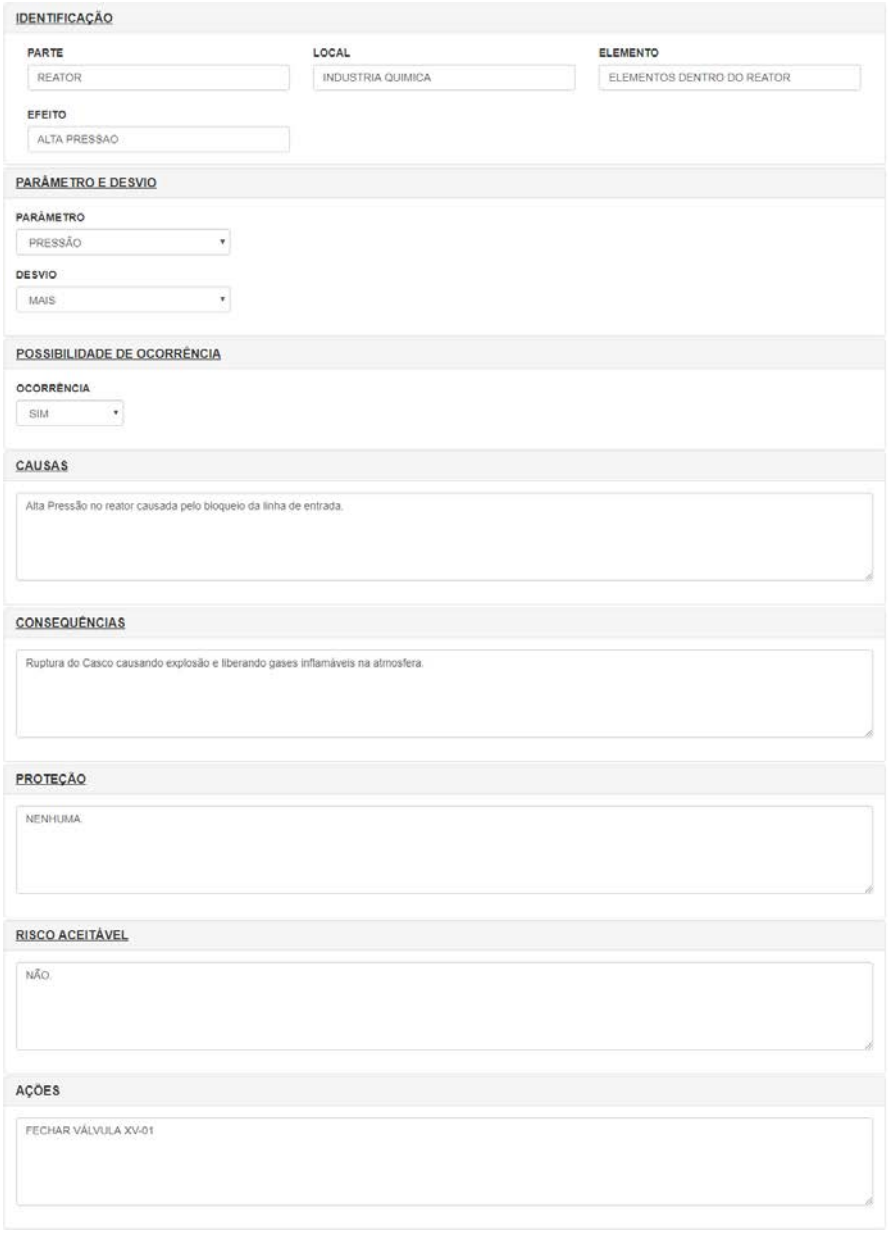
Tabela 15 – Comparação das Ferramentas Desenvolvidas.

Variável/Parâmetro	Evento Perigoso
Alta Temperatura.	Ruptura do casco causando explosão e lançando gás inflamável na atmosfera.
Alta Pressão.	Ruptura do casco causando explosão e lançando gás inflamável na atmosfera.

Fonte: (GOBLE & CHEDDIE, 2005).

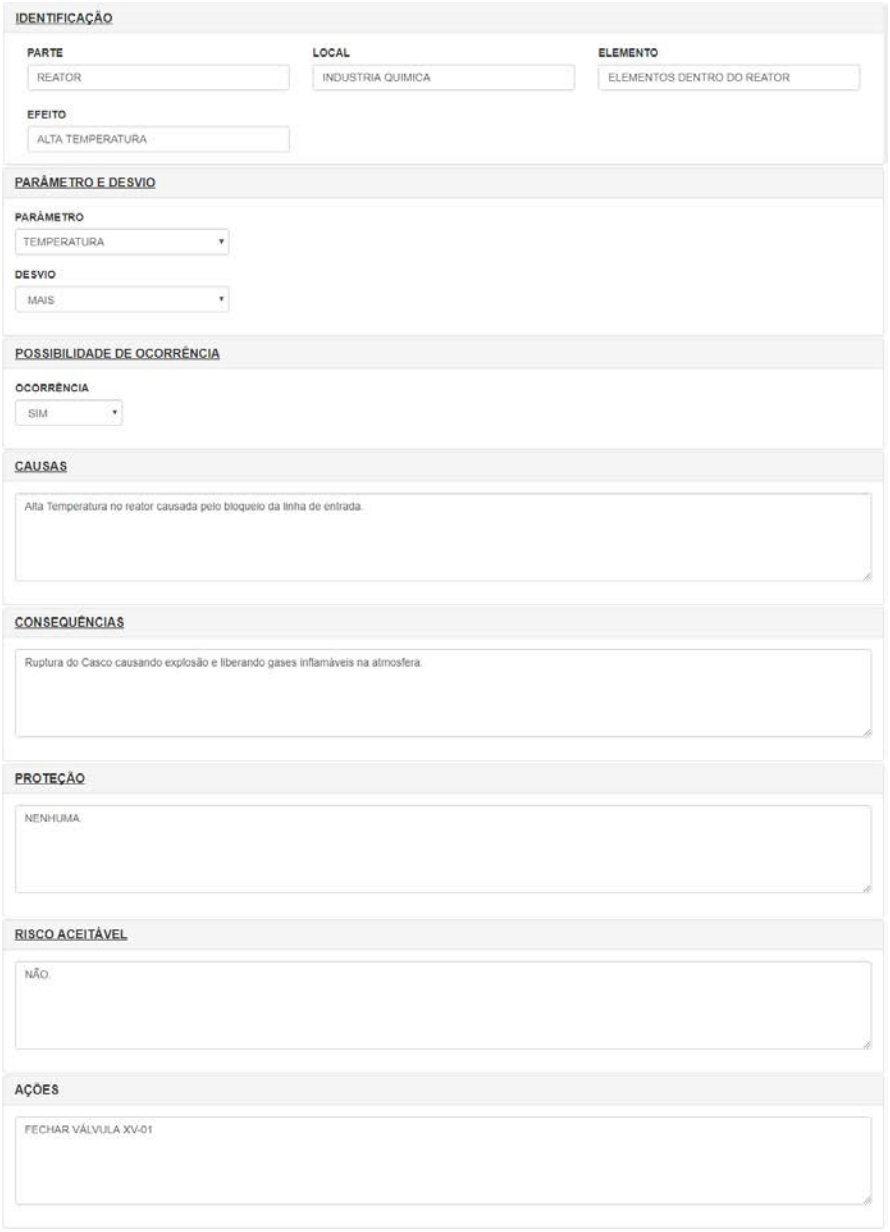
Na ferramenta foi criado um novo projeto e realizados os estudos HAZOP como mostrado pela Figura 52 e pela Figura 53.

Figura 52 – HAZOP Reator - Pressão.



Fonte: Autoria Própria.

Figura 53 – HAZOP Reator - Temperatura.



Fonte: Autoria Própria.

A ferramenta salva os dados adquiridos no banco de dados e apresenta na área de análises, Figura 54.

Figura 54 – HAZOPs área de análises.

ID	PARTE	LOCAL
1	REATOR - PRESSAO	INDUSTRIA QUIMICA
2	REATOR - TEMPERATURA	INDUSTRIA QUIMICA

Fonte: Autoria Própria.

Os autores obtiveram através da análise de PFD, o valor de SIL 2 para os para esse processo. O módulo 2 da ferramenta usa a árvore de falhas para encontrar o valor de taxa de fatalidades por ano para casa sensor. O valor de SFF e HFT desses sensores foram fornecidos também pelo livro utilizado como base para este caso de estudo. A Figura 55 mostra o resultado da análise de árvore de falhas.

Figura 55 – Resultado da Análise de Árvore de Falhas na área de análises.

ID	PARTE	LOCAL	TAXA DE FATALIDADES/ANO
1	REATOR - PRESSAO	INDUSTRIA QUIMICA	0.016298296
2	REATOR - TEMPERATURA	INDUSTRIA QUIMICA	0.010918296000000001

Fonte: Autoria Própria.

Com o resultado apresentado pela Figura 54 é possível avaliar, usando o módulo 3 da ferramenta, o SIL calculado para o processo. A Figura 56 mostra os resultados.

Figura 56 – Resultado do Cálculo do SIL na área de análises.

ID	PARTE	LOCAL	FAR TOLERÁVEL	FAR SEM PROTEÇÃO	FATOR DE REDUÇÃO DE RISCO(RRF)	SIL
1	REATOR - PRESSAO	INDUSTRIA QUIMICA	0.2	148.16632727272727	740.8316363636363	SIL 2
2	REATOR - TEMPERATURA	INDUSTRIA QUIMICA	0.2	99.25723636363637	496.28618181818183	SIL 2

Fonte: Autoria Própria.

Enfim é possível selecionar as votações das arquiteturas para cada subsistema. Goble e Cheddie (2005) selecionaram a votação 1oo2 para o subsistema sensor, a votação 1oo1 para o subsistema lógico e também a 1oo1 para o subsistema elemento final. Apesar de existirem outras votações capazes de satisfazer os requisitos de segurança necessários, foram selecionadas na ferramenta as mesmas arquiteturas apresentadas pela Figura 57.

Figura 57 – Resultado SIF na área de análises.

SIF	SUBSISTEMA SENSOR	SIL	VOTAÇÃO	SUBSISTEMA LÓGICO	SIL	VOTAÇÃO	SUBSISTEMA ELEMENTO FINAL	SIL	VOTAÇÃO
SIF 1	TRANSMISSOR DE PRESSÃO TRANSMISSOR DE TEMPERATURA	SIL 2 SIL 2	1oo2 1oo2	CLP	SIL 3	1oo1	VÁLVULA	SIL 2	1oo1
PFD TOTAL: 0.0552720700152207									

Fonte: Autoria Própria.

Vale ressaltar que o resultado para esse primeiro caso de estudos é o mesmo que os calculados pelo livro. A Tabela 16 apresenta os resultados comparativos dos resultados obtido pela ferramenta e pelos autores. O relatório desta análise completa pode ser visto nos anexos deste documento.

Tabela 16 – Comparação dos Resultados da Ferramenta para o Caso de Estudo do Reator Químico

Módulos	**Literatura**	**Ferramenta**
Análise de Riscos	A análise foi realizada conforme a Tabela 15 como demonstrado pelos autores	A análise inseriu os dados da Tabela 15 no banco de dados da ferramenta
Análise de Árvore de Falhas	O valor de Fatal Accident Rate obtido para temperatura é 0,011 e para pressão é 0,017	O valor de Fatal Accident Rate obtido para temperatura é 0.010918296e para pressão é 0.016298296, como mostrado pelas Figura 54. A diferença é vista no arredondamento decimal
Cálculo do SIL	O valor de SIL obtido pelos autores é o 2	A ferramenta apresenta também o SIL 2 como mostrado pela Figura 55
Definição da SIF	A redundância definida pelos autores é 1oo2 para os transmissores de pressão e temperatura, 1ooo1 para o CLP e 1oo1 para a válvula	A redundância definida pela ferramenta ée 1oo2 para os transmissores de pressão e temperatura, 1ooo1 para o CLP e 1oo1 para a válvula

Fonte: Autoria Própria.

6.2 CASO DE ESTUDO 2 – PLANTA DESESTABILIZAÇÃO DE EMULSÕES DE PETRÓLEO VIA MICRO-ONDAS

De maneira análoga ao caso de estudo anterior agora é escolhida uma planta de desestabilização de emulsões de petróleo via micro-ondas mostrada por Santos e Theobald (2013). Segundo os autores a produção de petróleo é acompanhada pela produção de água, muitas vezes com alta salinidade, gás, sedimentos e outros contaminantes, que devem ser removidos para que o petróleo seja especificado dentro de certos parâmetros para o envio às refinarias. Por esse motivo, o processo deve ser avaliado com uma análise qualitativa de riscos e assim pode ser usado como um caso de estudo para a ferramenta.

As Tabela 17 e Tabela 18 mostram os HAZOPs realizados por Santos e Theobald (2013). Esses HAZOPs são divididos em duas partes, a primeira referente às variáveis do micro-ondas e a segunda às variáveis do tanque de separação.

Tabela 17 - HAZOP referente ás variáveis do Micro-Ondas.

Parâmetro	Palavra-Guia	Desvio	Causas	Detecção	Consequências
Vazão de entrada	Não	Sem vazão	Bomba desliga; Válvula V1 fora de posição; Válvula V2 fora de posição.	Visual	Parada da unidade; Descarte da emulsão; Parada da unidade.
Vazão de entrada	Menos	Menos fluxo	Viscosidade elevada da emulsão; Rotação da bomba baixa.	Não há	Quebra da bomba; Redução na alimentação do reator.
Vazão de entrada	Mais	Mais fluxo	Viscosidade baixa da emulsão; Rotação da bomba elevada.	Não há	Redução na eficiência de separação
Pressão	Menos	Menos pressão	Falha na bomba de alimentação; Obstrução da válvula V2.	Pressostato	Parada da unidade
Pressão	Mais	Mais pressão	Válvula V2 fora de posição; Obstrução da válvula V2.	Pressostato	Explosão.
Nível	Menos	Nível mais baixo	Reservatório de emulsão vazio.	Não há.	Parada da unidade
Nível	Mais	Nível mais alto	Transbordo do reservatório de Emulsão	Não há	Contaminação ambiental
Viscosidade	Menos	Viscosidade mais baixa	Característica do óleo.	Não há	Emulsão escoa rapidamente pelo processo
Viscosidade	Mais	Viscosidade mais alta	Característica do óleo.	Não há	Dificuldade no escoamento para alimentação da unidade

Fonte: (SANTOS & THEOBALD, 2013).

Tabela 18 - HAZOP referente ás variáveis do Tanque de Separação.

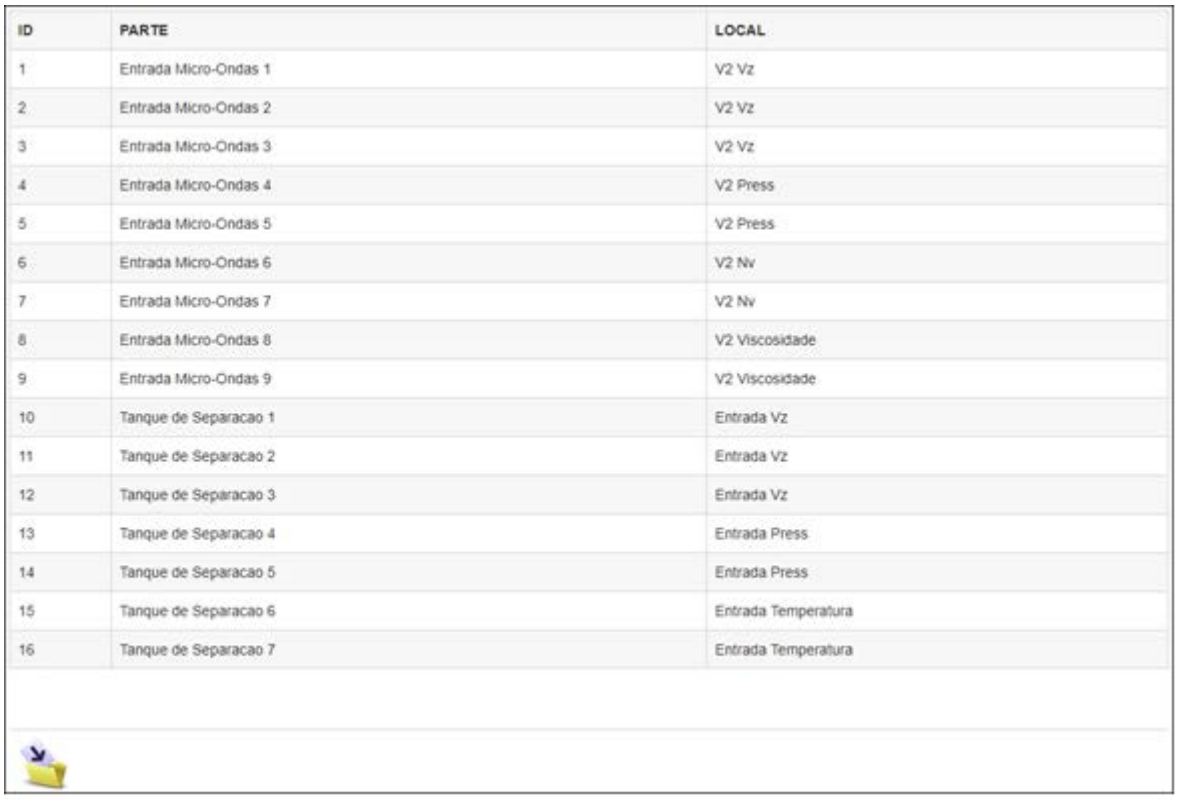
Parâmetro	Palavra-Guia	Desvio	Causas	Detecção	Consequências
Vazão de entrada	Não	Sem vazão	Obstrução na entrada do reator; Obstrução na saída do reator; Obstrução válvula reguladora de pressão.	Visual	Parada da unidade
Vazão de entrada	Menos	Menos fluxo	Vazamento de conexões e tubulações; Vazamento no reator.	Visual	Contaminação ambiental
Vazão de entrada	Mais	Mais fluxo	Válvula de pressão danificada; Válvula reguladora de Pressão aberta.	Visual	Redução na eficiência de separação
Pressão	Menos	Menos pressão	Válvula reguladora de pressão totalmente aberta;	Pressostato	Redução na eficiência de separação

			Vazamento no reator.		
Pressão	Mais	Mais pressão	Válvula reguladora de pressão fechada; Obstrução no reator	Pressostato	Explosão
Temperatura	Menos	Temperatura mais baixa	Falhas nos sensores de temperatura; Falha no sistema de irradiação de micro-ondas.	Termopares	Insuficiência no processo de separação
Temperatura	Mais	Temperatura mais alta	Falhas nos sensores de temperatura; Falha no sistema de irradiação de micro-ondas.	Termopares	Contaminação ambiental

Fonte: (SANTOS & THEOBALD, 2013).

Com isso, procede-se com a inserção desses dados na ferramenta. A Figura 58 apresenta todos os HAZOPs criados pela ferramenta separados por parte e local.

Figura 58 – HAZOPs do Caso de Estudo 2.



ID	PARTE	LOCAL
1	Entrada Micro-Ondas 1	V2 Vz
2	Entrada Micro-Ondas 2	V2 Vz
3	Entrada Micro-Ondas 3	V2 Vz
4	Entrada Micro-Ondas 4	V2 Press
5	Entrada Micro-Ondas 5	V2 Press
6	Entrada Micro-Ondas 6	V2 Nv
7	Entrada Micro-Ondas 7	V2 Nv
8	Entrada Micro-Ondas 8	V2 Viscosidade
9	Entrada Micro-Ondas 9	V2 Viscosidade
10	Tanque de Separacao 1	Entrada Vz
11	Tanque de Separacao 2	Entrada Vz
12	Tanque de Separacao 3	Entrada Vz
13	Tanque de Separacao 4	Entrada Press
14	Tanque de Separacao 5	Entrada Press
15	Tanque de Separacao 6	Entrada Temperatura
16	Tanque de Separacao 7	Entrada Temperatura

Fonte: Autoria Própria.

Os autores, após a execução do estudo de riscos HAZOP, levantaram os valores adequados para o SIL de cada parte. A Tabela 19 e a Tabela 20 mostram para cada parte, o parâmetro/desvio, o grau de severidade, a frequência de ocorrência e o SIL encontrado através

do método de Matriz de Riscos. Assim, também é possível comparar os resultados obtidos pelo método de quantificação de riscos de Santos e Theobald (2013) com o método usado pela ferramenta.

Tabela 19 – Grau de Severidade, Frequência de Ocorrência e o SIL através do método de matriz de riscos para Entrada do Micro-Ondas.

Parte	Parâmetro/Desvio	Grau de Severidade	Frequência de Ocorrência	SIL
Micro-Ondas	Vazão/Não	III	D	4
	Vazão/Menos	III	D	4
	Vazão/Mais	III	D	4
	Pressão/Menos	IV	D	4
	Pressão/Mais	III	D	3
	Nível/Menos	III	D	2
	Nível/Mais	IV	D	4
	Viscosidade/Menos	III	D	3
	Viscosidade/Mais	III	D	4

Fonte: (SANTOS & THEOBALD, 2013).

Tabela 20 – Grau de Severidade, Frequência de Ocorrência e o SIL através do método de matriz de riscos para Tanque de Separação.

Parte	Parâmetro/Desvio	Grau de Severidade	Frequência de Ocorrência	SIL
Tanque de Separação	Vazão/Não	III	D	3
	Vazão/Menos	IV	D	4
	Vazão/Mais	III	D	4
	Pressão/Menos	III	D	3
	Pressão/Mais	IV	D	3
	Temperatura/Menos	III	D	2
	Temperatura/Mais	III	D	3

Fonte: (SANTOS & THEOBALD, 2013).

Usando os valores de SIL apresentados pela Tabela 19 e Tabela 20 obtidos pelos autores, obtém-se os valores para o SIL pela ferramenta mostrados pela Figura 59.

Figura 59 – Cálculo SIL do Caso de Estudo 2.

ID	PARTE	LOCAL	FAR TOLERÁVEL	FAR SEM PROTEÇÃO	FATOR DE REDUÇÃO DE RISCO(RRF)	SIL
1	Entrada Micro-Ondas 1	V2 Vz	0.1	1244.9162679425838	12449.162679425837	SIL 4
2	Entrada Micro-Ondas 2	V2 Vz	0.1	1519.7088068181818	15197.088068181816	SIL 4
3	Entrada Micro-Ondas 3	V2 Vz	0.1	1487.9261363636365	14879.261363636364	SIL 4
4	Entrada Micro-Ondas 4	V2 Press	0.1	1625.384024577573	16253.84024577573	SIL 4
5	Entrada Micro-Ondas 5	V2 Press	0.1	172.99107142857144	1729.9107142857144	SIL 3
6	Entrada Micro-Ondas 6	V2 Nv	0.2	4116.287878787879	20581.439393939392	SIL 4
7	Entrada Micro-Ondas 7	V2 Nv	0.2	84.7107438016529	423.55371900826447	SIL 2
8	Entrada Micro-Ondas 8	V2 Viscosidade	0.125	776.7857142857143	6214.285714285715	SIL 3
9	Entrada Micro-Ondas 9	V2 Viscosidade	0.125	2106.6468253968255	16853.174603174604	SIL 4
10	Tanque de Separacao 1	Entrada Vz	0.25	757.5757575757575	3030.30303030303	SIL 3
11	Tanque de Separacao 2	Entrada Vz	0.25	3672.7627840909095	14691.051136363638	SIL 4
12	Tanque de Separacao 3	Entrada Vz	0.25	2759.555785123967	11038.223140495867	SIL 4
13	Tanque de Separacao 4	Entrada Press	0.08333333333333333	440.3409090909091	5284.09090909091	SIL 3
14	Tanque de Separacao 5	Entrada Press	0.08333333333333333	440.61942959001783	5287.433155080214	SIL 3
15	Tanque de Separacao 6	Entrada Temperatura	0.2	55.68181818181818	278.4090909090909	SIL 2
16	Tanque de Separacao 7	Entrada Temperatura	0.2	308.55263157894734	1542.7631578947367	SIL 3

Fonte: Autoria Própria.

É possível analisar pra este caso de estudo da planta de desestabilização de emulsões de petróleo, através da comparação entre os valores do SIL calculados por Santos e Theobald (2013) na Tabela 19 e Tabela 20 com os valores obtidos pela ferramenta na Figura 59, que os valores encontrados tanto para o SIL calculado usando a matriz de riscos quanto para o uso da árvore de falhas da ferramenta são compatíveis. Este resultado demonstra a flexibilidade de uso da ferramenta e a exatidão dos cálculos realizados par diferentes tipos de variáveis e malhas de processo.

Apesar de os autores não gerarem as arquiteturas para a SIF, foi construído no módulo 4 da ferramenta as arquiteturas SIF de forma que o projeto fosse concluído completamente e mostrar o potencial da ferramenta para solução de processos simples e complexos. As Figura 60 e Figura 61 abaixo fornecem as arquiteturas para a SIF dos dados fornecidos por Santos e Theobald (2013).

Figura 60 – SIFs do Caso de Estudo 2 (Parte 1).

SIF	SUBSISTEMA SENSOR	SIL	VOTAÇÃO	SUBSISTEMA LÓGICO	SIL	VOTAÇÃO	SUBSISTEMA ELEMENTO FINAL	SIL	VOTAÇÃO
SIF 1	TRANSMISSOR DE VAZÃO	SIL 4	1oo3				VÁLVULA FECHAMENTO VÁLVULA ABERTURA	SIL 3 SIL 3	1oo3 1oo3
PFD TOTAL: 8.0326687484987E-5									

SIF	SUBSISTEMA SENSOR	SIL	VOTAÇÃO	SUBSISTEMA LÓGICO	SIL	VOTAÇÃO	SUBSISTEMA ELEMENTO FINAL	SIL	VOTAÇÃO
SIF 2	TRANSMISSOR DE FLUXO	SIL 3	1oo3				VÁLVULA ABERTURA VÁLVULA FECHAMENTO	SIL 3 SIL 3	1oo3 1oo3
PFD TOTAL: 6.5802079682206E-5									

SIF	SUBSISTEMA SENSOR	SIL	VOTAÇÃO	SUBSISTEMA LÓGICO	SIL	VOTAÇÃO	SUBSISTEMA ELEMENTO FINAL	SIL	VOTAÇÃO
SIF 3	TRANSMISSOR DE NÍVEL TRANSMISSOR DE FLUXO	SIL 4 SIL 3	1oo3 1oo3				VÁLVULA ABERTURA	SIL 3	1oo3
PFD TOTAL: 6.7207637231504E-5									

SIF	SUBSISTEMA SENSOR	SIL	VOTAÇÃO	SUBSISTEMA LÓGICO	SIL	VOTAÇÃO	SUBSISTEMA ELEMENTO FINAL	SIL	VOTAÇÃO
SIF 4	TRANSMISSOR DE PRESSÃO	SIL 3	1oo3						
PFD TOTAL: 6.1523922031896E-5									

SIF	SUBSISTEMA SENSOR	SIL	VOTAÇÃO	SUBSISTEMA LÓGICO	SIL	VOTAÇÃO	SUBSISTEMA ELEMENTO FINAL	SIL	VOTAÇÃO
SIF 5	TRANSMISSOR DE PRESSÃO	SIL 3	1oo3						
PFD TOTAL: 0.00057806451612903									

SIF	SUBSISTEMA SENSOR	SIL	VOTAÇÃO	SUBSISTEMA LÓGICO	SIL	VOTAÇÃO	SUBSISTEMA ELEMENTO FINAL	SIL	VOTAÇÃO
SIF 6	TRANSMISSOR DE NÍVEL	SIL 4	1oo3				VÁLVULA ABERTURA VÁLVULA FECHAMENTO	SIL 3 SIL 3	1oo3 1oo3
PFD TOTAL: 4.8587466642128E-5									

SIF	SUBSISTEMA SENSOR	SIL	VOTAÇÃO	SUBSISTEMA LÓGICO	SIL	VOTAÇÃO	SUBSISTEMA ELEMENTO FINAL	SIL	VOTAÇÃO
SIF 7	TRANSMISSOR DE NÍVEL	SIL 2	2oo2D						
PFD TOTAL: 0.0023609756097561									

SIF	SUBSISTEMA SENSOR	SIL	VOTAÇÃO	SUBSISTEMA LÓGICO	SIL	VOTAÇÃO	SUBSISTEMA ELEMENTO FINAL	SIL	VOTAÇÃO
SIF 8	TRANSMISSOR DE VISCOSIDADE	SIL 3	2oo3						
PFD TOTAL: 0.00016091954022989									

Fonte: Autoria Própria.

Figura 61 – SIFs do Caso de Estudo 2 (Parte 2).

SIF	SUBSISTEMA SENSOR	SIL	VOTAÇÃO	SUBSISTEMA LÓGICO	SIL	VOTAÇÃO	SUBSISTEMA ELEMENTO FINAL	SIL	VOTAÇÃO
SIF 9	TRANSMISSOR DE VISCOSIDADE TRANSMISSOR DE FLUXO	SIL 4 SIL 3	1oo3 1oo3						
PFD TOTAL: 5.9336001883683E-5									

SIF	SUBSISTEMA SENSOR	SIL	VOTAÇÃO	SUBSISTEMA LÓGICO	SIL	VOTAÇÃO	SUBSISTEMA ELEMENTO FINAL	SIL	VOTAÇÃO
SIF 10	TRANSMISSOR DE FLUXO TRANSMISSOR DE NÍVEL	SIL 3 SIL 3	1oo3 2oo3				VÁLVULA ABERTURA VÁLVULA FECHAMENTO	SIL 3 SIL 3	1oo3 1oo3
PFD TOTAL: 0.00033									

SIF	SUBSISTEMA SENSOR	SIL	VOTAÇÃO	SUBSISTEMA LÓGICO	SIL	VOTAÇÃO	SUBSISTEMA ELEMENTO FINAL	SIL	VOTAÇÃO
SIF 11	TRANSMISSOR DE NÍVEL TRANSMISSOR DE FLUXO	SIL 4 SIL 3	1oo3 1oo3						
PFD TOTAL: 6.8068648779309E-5									

SIF	SUBSISTEMA SENSOR	SIL	VOTAÇÃO	SUBSISTEMA LÓGICO	SIL	VOTAÇÃO	SUBSISTEMA ELEMENTO FINAL	SIL	VOTAÇÃO
SIF 12	TRANSMISSOR DE NÍVEL TRANSMISSOR DE FLUXO	SIL 4 SIL 3	1oo3 1oo3						
PFD TOTAL: 9.0594291062237E-5									

SIF	SUBSISTEMA SENSOR	SIL	VOTAÇÃO	SUBSISTEMA LÓGICO	SIL	VOTAÇÃO	SUBSISTEMA ELEMENTO FINAL	SIL	VOTAÇÃO
SIF 13	TRANSMISSOR DE PRESSÃO	SIL 3	1oo3						
PFD TOTAL: 0.00018924731182796									

SIF	SUBSISTEMA SENSOR	SIL	VOTAÇÃO	SUBSISTEMA LÓGICO	SIL	VOTAÇÃO	SUBSISTEMA ELEMENTO FINAL	SIL	VOTAÇÃO
SIF 14	TRANSMISSOR DE PRESSÃO	SIL 3	1oo3				VÁLVULA FECHAMENTO VÁLVULA ABERTURA	SIL 3 SIL 3	1oo3 1oo3
PFD TOTAL: 0.00018912768647282									

SIF	SUBSISTEMA SENSOR	SIL	VOTAÇÃO	SUBSISTEMA LÓGICO	SIL	VOTAÇÃO	SUBSISTEMA ELEMENTO FINAL	SIL	VOTAÇÃO
SIF 15	TRANSMISSOR DE TEMPERATURA	SIL 2	2oo2						
PFD TOTAL: 0.0035918367346939									

SIF	SUBSISTEMA SENSOR	SIL	VOTAÇÃO	SUBSISTEMA LÓGICO	SIL	VOTAÇÃO	SUBSISTEMA ELEMENTO FINAL	SIL	VOTAÇÃO
SIF 16	TRANSMISSOR DE TEMPERATURA	SIL 3	2oo3				VÁLVULA FECHAMENTO VÁLVULA ABERTURA	SIL 3 SIL 3	1oo3 1oo3
PFD TOTAL: 0.00064818763326226									

Fonte: Autoria Própria.

As informações de todas as análises realizadas pela ferramenta são arquivadas e finalmente é gerado o relatório final. Este relatório está alocado nos anexos deste documento.

6.3 CASO DE ESTUDO 3 – SUBESTAÇÃO DE ENERGIA – TRANSFORMADOR DE CONRRENTE E TRANSFORMADOR DE POTENCIAL

Buscando testar o uso da ferramenta para uma área de aplicação diferente, uma análise e quantificação de riscos realizadas em uma subestação de energia foi realizada. Este caso de estudo foi fornecido pela empresa Acom Energy e foi realizado em 2013. O autor do relatório, Negri (2013), realizou as análises nos transformadores de corrente (TC) e potencial (TP) da

subestação de energia de uma empresa multinacional (por motivos de sigilo não terá o nome divulgado).

Transformadores de corrente ou TCs são usados para sistemas de medição de corrente elétrica e são capazes de reduzir a corrente em estudo para níveis compatíveis com o valor máximo suportável pelos instrumentos de medição. Analogamente os transformadores de potencial ou TPs servem para a medição da tensão elétrica reduzindo a mesma a valores compatíveis com os equipamentos de medição.

Negri (2013) inicia os procedimentos com o estudo HAZOP em caso de sobrecorrente para o TC e sobretensão o TP. As análises HAZOP's são mostradas abaixo pela Tabela 21 e pela Tabela 22.

Tabela 21 – HAZOP SOBRECORRENTE TC.

Parâmetro	Desvio	Causas	Detecção	Consequências
Corrente	Mais	Falha do Disjuntor de Entrada DJ01.	Visual	Acionamento do Disjuntor do TC DJT01; Parada da subestação.

Fonte: (NEGRI, 2013).

Tabela 22 – HAZOP SOBRETENSÃO TP.

Parâmetro	Desvio	Causas	Detecção	Consequências
Tensão	Mais	Falha do Disjuntor de Entrada DJ01.	Visual	Acionamento do Disjuntor do TP DJT04; Parada da subestação.

Fonte: (NEGRI, 2013).

Utilizando-se os dados do HAZOP de Negri (2013), pode-se inserir os mesmos na ferramenta, conforme mostrado pela Figura 62.

Figura 62 – HAZOPs TC e TP na Ferramenta.

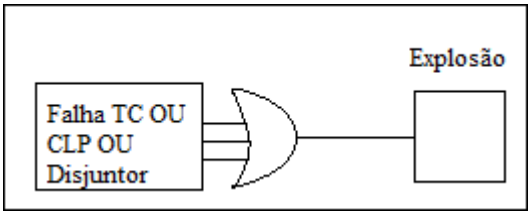
ID	PARTE	LOCAL
1	TC	ENTRADA
2	TP	ENTRADA

Fonte: (Autoria Própria).

Em seguida houve o levantamento da árvore de falhas (AAF) elaborada em Negri (2013). A árvore foi elaborada dando como evento topo uma catástrofe explosiva dos equipamentos e

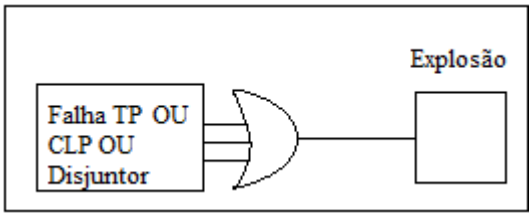
incêndio na subestação. A Figura 63 e a Figura 64 mostram as árvores levantadas para o TC e o TP.

Figura 63 – AAF TC.



Fonte: (NEGRI, 2013).

Figura 64 – AAF TP.



Fonte: (NEGRI, 2013).

Os valores obtidos de taxa de fatalidades em Negri (2013), considerando que não há operador em campo (já que não é comum operadores trabalharem nos equipamentos de subestação), com os mesmos em operação foram 0,25 para o TC e 0,63 para o TP.

A ferramenta encontrou os mesmos valores de taxas de fatalidades por ano, fato esse que pode ser visualizado pela Figura 65.

Figura 65 – Taxa de Fatalidades para TC e TP.

ID	PARTE	LOCAL	TAXA DE FATALIDADES/ANO
1	TC	ENTRADA	0.0244404
2	TP	ENTRADA	0.06266028

Fonte: (Autoria Própria).

Por fim, Negri (2013) definiu o valor do SIL adequado para os equipamentos e elaborou a linha de emergência da subestação usando os dados da SIF. O SIL elencado para ambos os equipamentos é SIL 3 e votação 1oo2D. Esses valores são compatíveis com os encontrados pela ferramenta e mostrados a seguir.

Figura 66 – SIL para TC e TP.

ID	PARTE	LOCAL	FAR TOLERÁVEL	FAR SEM PROTEÇÃO	FATOR DE REDUÇÃO DE RISCO(RRF)	SIL
1	TC	ENTRADA	1	1110.9272727272728	1110.9272727272728	SIL 3
2	TP	ENTRADA	1	2848.1945454545453	2848.1945454545453	SIL 3

Fonte: (Autoria Própria).

Da mesma forma que nos casos de estudo 1 e 2, todos os resultados obtidos pela ferramenta de projeto de SIS desenvolvida são iguais aos resultados da literatura. Esses resultados mostram a eficácia e exatidão da ferramenta desenvolvida.

Figura 67 – Votação para TC e TP.

SIF	SUBSISTEMA SENSOR	SIL	VOTAÇÃO	SUBSISTEMA LÓGICO	SIL	VOTAÇÃO	SUBSISTEMA ELEMENTO FINAL	SIL	VOTAÇÃO
SIF 1	Transformador de Corrente	SIL 3	1oo2D						
PFD TOTAL: 0.00090014893373267									
SIF	SUBSISTEMA SENSOR	SIL	VOTAÇÃO	SUBSISTEMA LÓGICO	SIL	VOTAÇÃO	SUBSISTEMA ELEMENTO FINAL	SIL	VOTAÇÃO
SIF 2	Transformador de Potencial	SIL 3	1oo2D						
PFD TOTAL: 0.00035109961206685									

Fonte: (Autoria Própria).

6.4 CASOS DE ESTUDO COMPLEMENTARES

Buscando a demonstração do funcionamento da ferramenta para projeto de SIS para processos diferentes e com tipos de variáveis e malhas de controle diferentes, casos de estudo adicionais foram realizados. De forma a simplificar a apresentação dos resultados, a comparação entre os resultados da literatura e os obtidos com a ferramenta foram resumidos e compilados nas Tabela 23 e Tabela 24. Os casos de estudo adicionais selecionados foram sobre um processo de Fabricação de Fibra de Poliéster (IELO; SILVA, 2015) e sobre uma Esteira de Transporte de Medicamentos (SANTOS; GUERREIRO, 2010

Tabela 23 –Comparação de Resultados do Caso de Estudo de Fabricação de Fibra de Poliéster

Processo	Referência	Breve Descrição
Fabricação de Fibra de Poliéster	Ielo e Silva (2015)	As autoras utilizam para esse processo real um P&ID como base e estudam detalhadamente todas as possíveis causas de falha para cada processo envolvido na fabricação.
HAZOP Abrandamento de Aguas		

Parâmetro	Desvio	Causas	Consequências	Proteção	Ações	SIL	Resultado igual ao da ferramenta?
Dureza	Mais	Tratamento inadequado acarretando em concentração alta de sais.	Incrustação, reduzindo a produção de vapor e eficiência térmica do processo.	Barreiras existentes: FIC 0741, LIC 0739	Não se aplica.	SIL 2	SIM
Dureza	Menos	Não se aplica	Sem riscos de explosão ou danos à caldeira.	Não se aplica	Não se aplica.	SIL 1	SIM
Nível	Menos	Furos nas tubulações devido a negligência nos procedimentos de manutenção; falha do operador ao realizar a leitura incorreta no controlador de nível	Ruptura das paredes metálicas ou superaquecimento das placas metálicas com risco de explosão.	Barreiras existentes: LT 0739, LSLL 0977	Não se aplica.	SIL 2	SIM
Nível	Mais	Leitura inadequada do controlador de nível.	Diminuição na transferência de calor sensível ocasionando a queda da temperatura na caldeira.	Barreiras existentes: LT 0739, LSLL 0977	Não se aplica	SIL 2	SIM
HAZOP Caldeira Aquatubular							
Parâmetro	Desvio	Causas	Consequências	Proteção	Ações	SIL	Resultado igual ao da ferramenta?
Pressão	Menos	Vazamento proveniente da entrada de ar de combustão e do gás natural; falha no controlador de pressão.	Menor rendimento da produção, gerando gastos com a manutenção e atraso na produção. Risco de explosão ou graves acidentes.	Barreiras existentes: PT 0965, PIC 0965, PR 0965.	Não se aplica.	SIL 3	SIM
Pressão	Mais	Falha no controlador de pressão (manômetro); Excesso de entrada de ar de combustão e gás natural.	Menor rendimento da produção, gerando gastos com a manutenção e atraso na produção. Risco de explosão ou graves acidentes	Barreiras existentes: PT 0965, PIC 0965, PR 0965.	Não se aplica.	SIL 3	SIM
Reação	Também	Proveniente de qualquer impureza/contaminação presente nos componentes da alimentação.	Incrustação. Os componentes podem reagir entre si e provocar uma explosão ou acidente, como também pode haver a formação de vapor contaminado.	Não	Não se aplica.	SIL 3	SIM
HAZOP Ar de Combustão							
Parâmetro	Desvio	Causas	Consequências	Proteção	Ações	SIL	Resultado igual ao da ferramenta?

Vazão	Mais	Maior ingestão de ar, diminuindo a temperatura e o comprimento da chama. Pode provocar o apagamento total da chama.	Menor eficiência de combustão. Risco de acidente/explosão. Parada obrigatória para remoção do excesso de gás.	Barreiras existentes: FT 3905 UV, PSL 3903 UV, FAL 3905, PAL 3903.	Não se aplica	SIL 2	SIM
Vazão	Menos	Menor ingestão de ar resultante de vazamentos ou entupimentos na tubulação.	Combustão incompleta e formação de CO2, fuligem e fumaça. Risco de acidente/explosão devido ao acúmulo de combustível não queimado.	Barreiras existentes: FT 3905 UV, PSL 3903 UV, FAL 3905, PAL 3903.	Não se aplica	SIL 2	SIM

Fonte: (Autoria Própria).

Tabela 24 –Comparação dos Resultados do Caso de Estudo da Esteira de Transporte de Medicamentos

Processo		**Referência**	**Breve Descrição**				
Esteira de Transporte de Medicamentos		Santos e Guerreiro (2010)	Os autores fazem os estudos dos riscos envolvendo o processo de transporte de medicamentos através de uma esteira automatizada.				
HAZOP Abrandamento de Aguas							
Parâmetro	Desvio	Causas	Consequências	Proteção	Ações	SIL	Resultado igual ao da ferramenta?
Corrente	Menos	Rompimento de cabo ligado aos motores da esteira.	Funcionamento incorreto do motor M0B1.	Não se aplica.	Ação imediata do controlador	SIL 2	SIM
Corrente	Mais	Sobrecorrente nos enrolamentos do motor M0B1	Desligamento do Motor ou queima do equipamento.	Relé de proteção RZ2322.	Ação imediata do controlador	SIL 3	SIM

Fonte: (Autoria Própria).

Conforme verificado nos casos de estudo apresentados nesta seção, todos os resultados obtidos pela ferramenta desenvolvida relacionados ao projeto do SIS foram iguais aos resultados disponíveis na literatura. Os casos de estudo utilizados contemplaram áreas de aplicação diferentes, bem como tipos de variáveis e malhas de controle diferentes. Além disso, as malhas de controle possuíam complexidade distintas, com diferentes números de variáveis e configurações de redundância. Dessa forma, é possível afirmar que a ferramenta web desenvolvida fornece grande flexibilidade de uso e facilita o projeto de um SIS. A exatidão dos resultados obtidos, mesmo em casos de estudo onde as técnicas utilizadas para análise de riscos e cálculo do SIL eram diferentes das técnicas implementadas na ferramenta, valida o desenvolvimento realizado e enfatiza o potencial de aplicação da ferramenta.

7 CONCLUSÕES

Neste trabalho foi desenvolvida uma ferramenta de análise e auxílio ao projeto de Sistemas Instrumentados de Segurança (SIS) utilizando linguagem própria para Web: o HTML, o PHP e o JavaScript. Para este desenvolvimento foi definida uma metodologia sistematizada de análise de riscos e de obtenção do Nível de Integridade de Segurança (SIL), satisfazendo as normas e os requisitos de segurança de um processo. O procedimento empregado foi dividido em quatro módulos ou etapas com funcionalidades específicas e compatíveis com a elaboração de um projeto de SIS.

O primeiro módulo está relacionado com a análise dos riscos e possibilidades de falhas presentes no processo, o qual é realizado pela ferramenta usando a técnica do Estudo de Perigos e Operabilidade (HAZOP). O levantamento quantitativo dos riscos e falhas possíveis elencados para o processo é realizado no segundo módulo, usando a técnica da Análise de Árvore de Falhas (AAF). A flexibilidade fornecida pela implementação computacional da AAF representa um diferencial da ferramenta obtido com a adoção dessa técnica para quantificação de riscos. O cálculo do SIL é realizado no terceiro módulo da ferramenta e utiliza uma tabela de fator de redução de risco (Tabela 5) disponível na norma de segurança. O nível de integridade de segurança (SIL) requerido para o processo é calculado com base no fator de redução de risco necessário para mitigar os riscos e falhas possíveis elencados e levar a operação do processo em análise a uma condição segura. O quarto módulo é o responsável pela definição das Funções Instrumentadas de Segurança (SIFs) a serem implementadas no SIS para efetivação das ações de segurança. Este módulo considera o SIL requerido e a configuração de redundância (votação) dos equipamentos de segurança definidas pelo projetista e que serão utilizados no SIS. O quarto módulo apresenta a divisão dos subsistemas, os valores de SIL e também as arquiteturas selecionadas para a SIF.

A ferramenta desenvolvida é inovadora e proporciona uma contribuição importante para esta temática de SIS, pois não foi encontrada na revisão bibliográfica realizada nenhuma ferramenta que englobasse todos os procedimentos requeridos para a análise e projeto de SIS. Isso representa um diferencial da ferramenta proposta em relação a outras soluções disponíveis na literatura, pois a mesma automatiza e auxilia nas etapas de projeto de um SIS, reduzindo principalmente tempo para execução dessas tarefas. Outro fator importante é que a ferramenta foi desenvolvida em ambiente Web, o que facilita seu uso e disseminação (sem a necessidade de instalação de software ou gerenciamento de permissões de acesso em empresas).

Os resultados obtidos através da validação e dos diferentes casos de estudo apresentados possibilitaram verificar o correto desenvolvimento da ferramenta proposta. Tais resultados como a Taxa de Acidentes Fatais (FAR), o Fator de Redução de Risco (RRF) e o Nível de Integridade de Segurança (SIL) foram os mesmos que os calculados manualmente nos trabalhos usados como referência. Dessa forma, constata-se a eficácia da ferramenta de análise e projeto de SIS, bem como a automatização de um procedimento geralmente manual.

Por fim, todos os dados recebidos e calculados das entradas e saídas dos módulos da ferramenta são armazenados em banco de dados específico, podendo ser consultados a qualquer momento pelo usuário e usados para a elaboração de um relatório final da construção do projeto de SIS. Os módulos, no relatório, são inseridos em arquivos separados por página contendo o histórico de cada análise realizada juntamente com os resultados.

8 REFERÊNCIAS BIBLIOGRÁFICAS

AMIGO, C. (2012), “FMEA (Failure Mode and Effect Analysis)”, USP, São Carlos, SP, Disponível em: http://www.portaldeconhecimentos.org.br/index.php/por/Conteudo/FMEA-Failure-Mode-and-Effect-Analysis. Acesso em: 07/05/2017.

ANSI/ISA – 84.00.01 – 2011 Part 1, “Functional Safety Instrumented Systems for the Process Industry Sector – Part 1: Framework, Definitions, System, Hardware and Software Requirements”, 2011.

AYAZ H.; TESTIK M. (2017), "Automation of FMEA for computer servers using log data with grey relational analysis,"*2017 International Conference on Computer Science and Engineering (UBMK),* Antalya, Turkey, 2017, pp. 616-620.

BARTOLOZZI V.; CASTIGLIONE L.; PICIOTTO A; GALLUZZO M. (2000), “Qualitative models of equipment units and their use in automatic HAZOP analysis”, In Reliability Engineering & System Safety, Volume 70, Issue 1, 2000, Pages 49-57.

BOONTHUM N.; MULALEE U; SRINOPHAKUN T. (2014), “A systematic formulation for HAZOP analysis based on structural model”, In Reliability Engineering & System Safety, Volume 121, 2014, Pages 152-163.

CATELANI, M.; CIANI, L.; LUONGO, V. (2012), “A new proposal for the analysis of Safety Instrumented Systems”. 2012 IEEE International Instrumentation and Measurement Technology Conference, Graz, pp. 1612-1616.

CASSIOLATO, C (2010). “Sistemas Instrumentados de Segurança – Uma Visão Prática – Parte 2”, SMAR Artigos Técnicos. Disponível em: http://www.smar.com/newsletter/marketing/index80.html. Aceso em: 03/2016.

CASSIOLATO, C (2012). “Sistemas Instrumentados de Segurança – Uma Visão Prática – Parte 5”, SMAR Artigos Técnicos. Disponível em: http://www.smar.com/noticias/conteudo/index92.html. Aceso em: 05/2016.

CROWL, D. A.; LOUVAS, J. F.(2002), “Chemical Process Safety”, 2th Edition. Prentice Hall, Upper Saddle River, New Jersey.

CRUZ-CAMPA, H. J.;CRUZ-GOMES, M. J.(2009), “Determine SIS and SIL using HAZOPs”, Process Safety Progress, Vol 29, pp. 22-31.

CUI L.; SHU Y.; WANG Z.; ZHAO J.; SUN T.; WEI Z. (2012), “HASILT: An intelligent software platform for HAZOP”, LOPA, SRS and SIL verification, In Reliability Engineering & System Safety, Volume 108, 2012, Pages 56-64.

DING L.; WANG H.; KANG K.; WANG K. (2014), “A novel method for SIL verification based on system degradation using reliability block diagram”, In Reliability Engineering & System Safety, Volume 132, 2014, Pages 36-45

EMERSON. “Emerson Automation SIS”., 2015 Disponível em: < http://www.emerson.com/en-us/automation/control-and-safety-systems/safety-instrumented-systems-sis >. Acesso em: 13/04/2017.

EXIDA. “Exida Engineering Tools”., 2017. Disponível em: < http://www.exida.com/exSILentia >. Acesso em: 08/05/2017.

FREIRE, V. H. (2013), “Análise Hazop e Projeto de Arquitetura de Automação de um Sistema Instrumentado de Segurança”, Trabalho de Graduação, UNESP, Sorocaba.

FINKEL, V.; NININ, N.; ZEE, D. (2006), Controle e Instrumentação – Análise de Riscos e o SIL, Edição nº 98 de Novembro de 2006.

GANDY, S. (2013), “Entries Tagged with: Risk Reduction Factor”, Dísponível em: http://www.exida.com/Blog/tag/Risk%20Reduction%20Factor. Acesso em: 28/08/2017

GIGIOSOFT. “SILmple”., 2017. Disponível em: < https://lh3.googleusercontent.com/uu>. Acesso em: 08/05/2017.

GOBLE, W.;M. CHEDDIE, H. L. (2005). Safety Instrumented Systems Verification – Pratical Probabilistic Calculations. 1st ed. Durham: ISA.

GOMES, B. S.(2014), “Automação, Investimento que dá retorno!”, SENAI – RJ, Diretoria de Tecnologia, SENAI.

GREENPEACE, Bhopal Documentos, Disponível em: <www.greenpeace.org.br/bhopal/ Bhopal_desastre_continua> Acesso em:18/05/2015.

GRUHN, P.; CHEDDIE, H. L. (2006). Safety Instrumented Systems: Design, Analysis and Justification. 2nd ed. Durham: ISA.

HILDEBRANDT A. (2007), "Calculating the "Probability of Failure on Demand" (PFD) of complex structures by means of Markov Models," *2007 4th European Conference on Electrical and Instrumentation Applications in the Petroleum & Chemical Industry*, Paris, 2007, pp. 1-5.

IEC61508 (2010). Functional Safety of electrical / electronic / programmable electronic safety-related systems – Part 2: Requirements for electrical / electronic / programmable electronic safety-related systems. IEC – International Electrotechnical Commission, Geneva.

IEC61511 (2003). Functional Safety – Safety Instrumented Systems for the Process Industry Sector – Part 3: Guidance for the Determination of Required Safety Integrity Levels. IEC – International Electrotechnical Commission, Geneva.

IEC61511-Mod (2014). Functional Safety – Safety Instrumented Systems for the Process Industry Sector – Part 3: Guidance for the Determination of Required Safety Integrity Levels. IEC – International Electrotechnical Commission, Geneva.

IELO, R. F., SILVA, S. Y., "ESTUDO DE CASO: APLICAÇÃO DA FERRAMENTA HAZOP EM SEGURANÇA DE PROCESSOS – EMPRESA M&G - POÇOS DE CALDAS/MG", 2015, UNIFAL – Universidade Federal de Alfenas Campus Poços de Caldas, Disponível em: http://www.unifal-mg.edu.br/engenhariaquimica/system/files/imce/TCC_2015_2/TCC_SUELLEN%20e%20RAFAELA%20Ferfoglia.pdf. Acesso em: 03/11/2017.

LASSEN, C. A. (2008), "Layer of protection analysis (LOPA) for determination of safety integrity level (SIL)", NTNU, Norwegian University of Science.

MACDONALD, D. (2004)," Pratical Hazops, Trips and Alarms", Elsevier, Burlington.

MANSOORI M.; WLECH I.; CHOO K. MAXION R. (2016), "Application of HAZOP to the Design of Cyber Security Experiments," *2016 IEEE 30th International Conference on Advanced Information Networking and Applications (AINA)*, Crans-Montana, 2016, pp. 790-799.

MCLENDON, B.(2013), "Por que o SIL é importante e como a conformidade com o SIL lhe traz benefícios", Scott Safety.

MESSIAS, G. (2015), “Análise Preliminar de Perigo”, Faculdade de Tecnologia e Ciências, Vitória, ES.

MIDT - SILToolbox, 2015. Disponível em:<sil.midt.no> Acesso em: 05/05/2017.

MINORU, M. (2015), “Segurança em Primeiro Lugar.” . Disponível em:< http://www.nei.com.br/artigo/seguranca-em-primeiro-lugar> Acesso em: 04/05/2017.

NAIMAN, V. (2014), “An Essay about SIL” Kyrkjeveien, Norway.

NAIMAN, V. (2015), “Let’s talk about SIL” Kyrkjeveien, Norway.

NEGRI, C. (2013), “Relatório de Análise de Risco Subestação 01”, Acom Energy Ltda., Disponível em: https://acomenergy.com.br/servicos/2/comissionamento-eletrico-de-subestacoes. Acesso em: 04/11/2017

OLIVEIRA, J. C. (2003), “Segurança e saúde no Trabalho: uma questão mal compreendida”, FUNDACENTRO, MG.

OLIVEIRA, E. N. (2012),”Cálculo do SIL Atingido – Estudo de Caso”, BRASKEM, RJ.

OREDA (2009). Offshore Reliability Data Handbook – 5th Edition. SINTEF Industrial Management, Trondheim, Norway.

PEPPERL+FUCHS (2017), “SIL SELECTION TOOL – Find the SIL Assessed Device are Looking For”, Disponível em: https://www.pepperl-fuchs.com/global/en/25702.htm. Acesso em 12/04/2017.

PILZ (2017), “PAScal safety Calculator”, Disponível em: https://www.pilz.com/pt-PT/eshop/00105002187038/PAScal-Safety-Calculator. Aceeso em: 12/04/2017.

PROSIS (2017), “SIL CALCULATOR”, Disponível em: http://www.prosisfse.com/sil-calculator/. Acesso: 12/04/2017.

SANTOS, L. W.; THEOBALD, R. (2013). “Estudo de Perigos e Operabilidade (HAZOP) em uma Planta Piloto de Desetabilização de Emulsões de Petróleo via Micro-Ondas”, XXXIII Encontro Nacional de Engenharia de Produação , Salvador – Bahia.

SANTOS, K. R.; GUERREIRO, E. D. R. (2010), “Study of Storage and Handling System Medicines”, Tékhne ε Lógos, Botucatu, SP, v.1, n.2, fev. 2010.

SAINI, N; PANDEY N.; SINGH A., "Analysis of reliability based algorithm for cognitive networks," *2017 International Conference on Computer Communication and Informatics (ICCCI)*, Coimbatore, India, 2017, pp. 1-4

SERPA, R. R. (2016). Estudo de Análise de Risco em Instalações com Produtos Químicos. Disponível: <http://www.bvsde.paho.org/cursode/p/modulos/modulo_2.2.pdf>. Acesso em: 03/2016.

SILVA, D. C. (2006), “Um Sistema de Gestão de Segurança do Trabalho alinhado à produtividade e à integridade dos colaboradores”, UFOP, Juiz de Fora, MG, Dísponível em: http://www.ufjf.br/ep/files/2014/07/2006_3_Diogo-Cortes.pdf. Acesso em: 25/04/2017

SILVA, J. D. (2012), “Estudo sobre Sistemas Instrumentados de Segurança: Conceitos, Regulamentação e Aplicações na Indústria”, Trabalho de Graduação, UFPR, Curitiba, Disponível em: http://repositorio.roca.utfpr.edu.br/jspui/bitstream/1/1903/1/CT_CEAUT_III_2012_13.pdf. Acesso em: 25/04/2017.

SQUILLANTE Jr., R. (2011), “Diagnóstico e tratamento de falhas críticas em Sistemas Instrumentados de Segurança”, Escola Politécnica, USP.

SOKOLOV, A. (2015), “Radiation Protection for SIS 100”, Scientific Report, Helmholtzzentrum für Schwerionenforschung.

SOUZA, C. L. F. (2012), “Análise Preliminar de Riscos, Perigos e Impactos Ambientais”, A Vez do Mestre, Rio de Janeiro, RJ, Disponível em: http://www.avm.edu.br/docpdf/monografias_publicadas/g201032.pdf. Acesso em: 24/05/2017.

SOUZA, J.A.L.; FO, D.J.S.; MIYAGI, P.E.; JUNQUEIRA, F.;SQUILANTE Jr, R.; LEGASPE, E.P. (2013). Mitigation Control of Faults in Critical Production Systems. In International Congress of Mechanical Engineering. Ribeirão Preto, 2013. pp.3889-99.

STONNER, R.(2014), “What-If – Ferramenta para identificação de riscos”. Disponível: < http://blogtek.com.br/what-if-ferramenta-identificacao-riscos/pdf>. Acesso em: 12/04/2017.

STONNER, R.(2015), “What-If – Ferramenta para identificação de riscos”. Disponível: < http://blogtek.com.br/what-if-ferramenta-questoes >. Acesso em: 27/04/2017.

SUMERS, A. E. (2013), “SIS IMPLEMENTATION”, SIS-TECH Solutions, LLC.

TAHARA, S. (2008), “FMEA (Failure Mode and Effect Analysis)”, USP, São Carlos, SP, Disponível em: http://www.portaldeconhecimentos.org.br/index.php/por/Conteudo/FMEA-Failure-Mode-and-Effect-Analysis. Acesso em: 07/05/2017.

WANG, F., N.; TAI, K. (2010), “Target matching problems and an adaptive constraint strategy for multiobjective design optimization using genetic algorithms”, Computers & Structures, vol. 88, pp. 1064-1076.

ZORZAN, F.; DORNELES, L.; SERVAT, M.E.; PEREIRA, E.O.; POLANCISKI, E. (2015),”FMEA: Orientações Conceituais para Aplicação de uma Ferramenta de Antecipação de Falhas”, 3ª Semana Internaciona das Engenharias da Fahor, Horizontina, RS.

9 ANEXOS/APÊNDICES

Relatório de Análise e Quantificação de Riscos

RELATÓRIO DE ANÁLISE E QUANTIFICAÇÃO DE RISCOS

PROJETISTA: CAIO AMALFI

SISTEMA: PLANTA QUIMICA REATOR-UNESP-2017-08-15

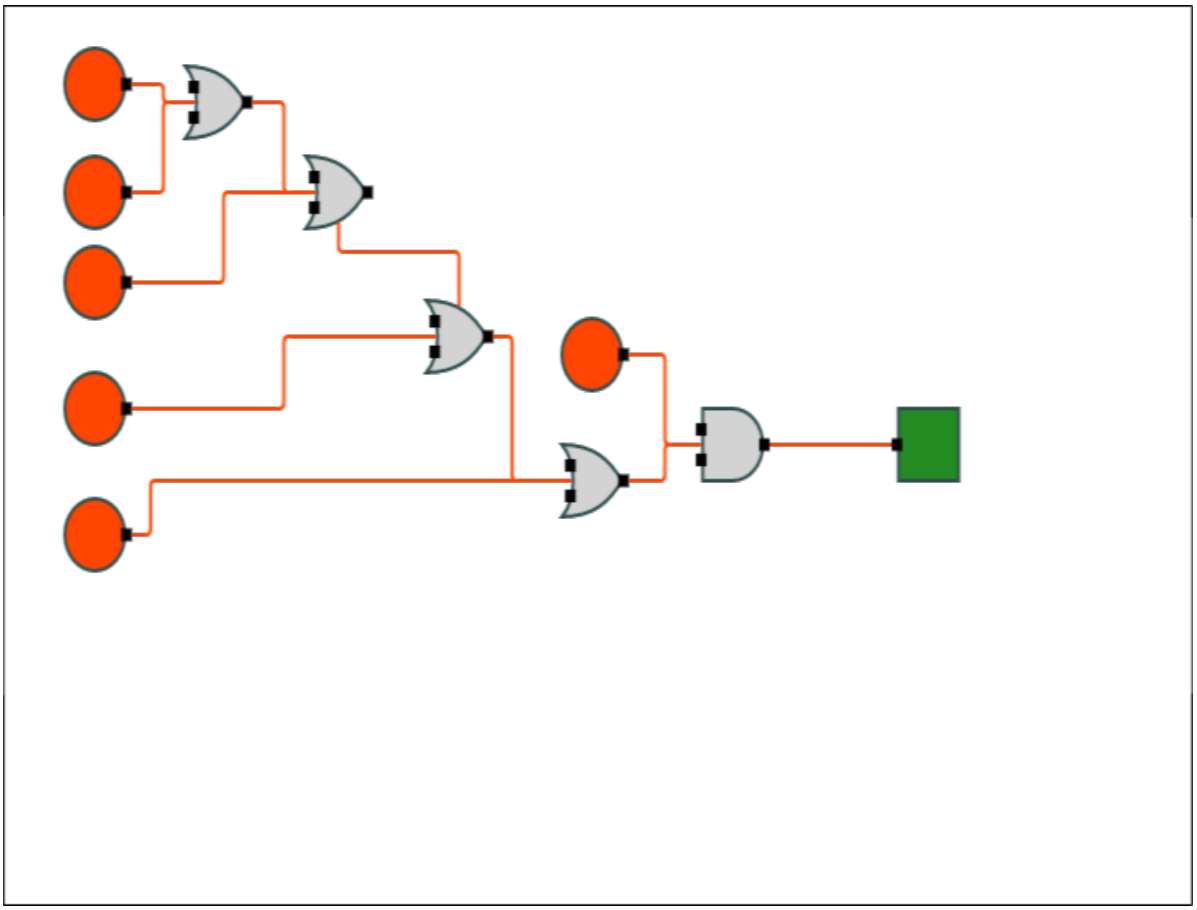
MÓDULO 1 - ANÁLISE DE RISCOS (HAZOP)

PARTE: REATOR
LOCAL: Val Press
ELEMENTO: PRODUTOS QUIMICOS NO INTERIOR DO REATOR
PARÂMETRO: PRESSÃO
DESVIO: MAIS
EFEITO: Aumento de Pressão

POSSIBILIDADE DE OCORRÊNCIA	SIM
CAUSAS	ALTA PRESSÃO CAUSADA PELO BLOQUEIO DA LINHA DO REATOR.
CONSEQUÊNCIAS	RUPTURA DO CASCO DO REATOR; LIBERAÇÃO DOS GASES NA ATMOSFERA.
PROTEÇÃO	NÃO CONSTA.
RISCO ACEITÁVEL	NÃO.
AÇÕES	AÇÃO DO SIS;

MÓDULO 2 - ANÁLISE DE ÁRVORE DE FALHAS (AAF)

LÓGICA	TRANSMISSOR DE PRESSÃO OU CLP OU VÁLVULA ABERTURA OU VÁLVULA FECHAMENTO OU FALHA OPERADOR E PROBABILIDADE DE OPERADOR EM CAMPO
TAXA DE ACIDENTES FATAIS (POR ANO)	0.08814914800000001



MÓDULO 3 - CÁLCULO DO NÍVEL DE INTEGRIDADE DE SEGURANÇA (SIL)

NÚMERO DE OPERÁRIOS EXPOSTOS AO RISCO:	10
QUANTIDADE DE SEMANAS TRABALHADAS POR ANO:	40
QUANTIDADE DE HORAS TRABALHADAS POR SEMANA:	44
FAR TOLERÁVEL:	0.1
FAR SEM PROTEÇÃO:	500.8474318181819
FATOR DE REDUÇÃO DE RISCOS:	5008.4743181818185
NÍVEL DE INTEGRIDADE DE SEGURANÇA (SIL):	SIL 3

MÓDULO 4 - DEFINIÇÃO DA FUNÇÃO INSTRUMENTADA DE SEGURANÇA (SIF)

SUBSISTEMA SENSOR

INSTRUMENTOS	SIL	VOTAÇÃO
TRANSMISSOR DE PRESSÃO	SIL 3	1oo3

SUBSISTEMA LÓGICO

INSTRUMENTOS	SIL	VOTAÇÃO
CLP	SIL 3	2oo2

SUBSISTEMA ELEMENTO FINAL

INSTRUMENTOS	SIL	VOTAÇÃO
VÁLVULA ABERTURA	SIL 3	1oo3
VÁLVULA FECHAMENTO	SIL 3	1oo3

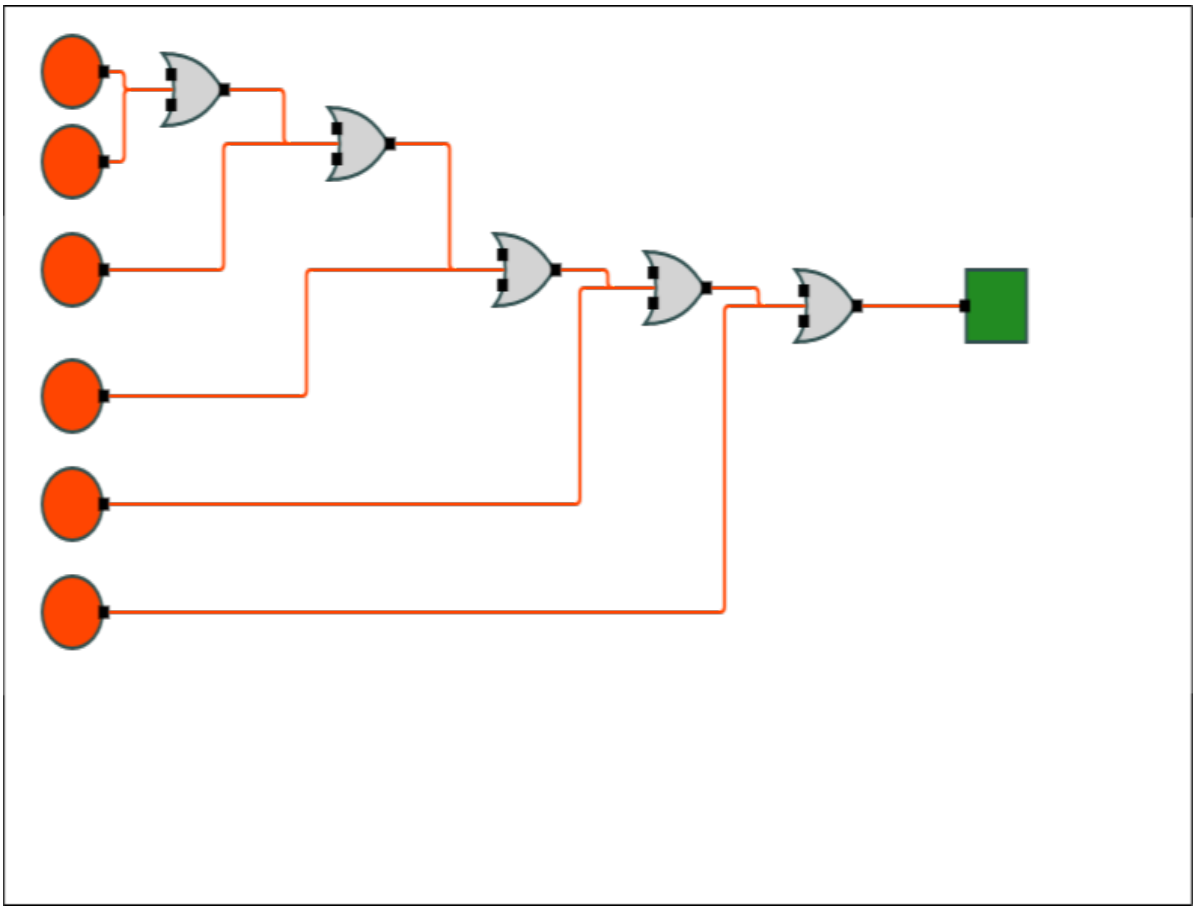
MÓDULO 1 - ANÁLISE DE RISCOS (HAZOP)

PARTE: REATOR
LOCAL: Val Temp
ELEMENTO: PRODUTOS QUIMICOS NO INTERIOR DO REATOR
PARÂMETRO: TEMPERATURA
DESVIO: MAIS
EFEITO: Temperatura acima da Especificada

POSSIBILIDADE DE OCORRÊNCIA	SIM
CAUSAS	ALTA TEMPERATURA CAUSADA PELO BLOQUEIO DA LINHA DO REATOR.
CONSEQUÊNCIAS	EXPLOSÃO DO CASCO DO REATOR.
PROTEÇÃO	ALARME DE TEMPERATURA.
RISCO ACEITÁVEL	NÃO.
AÇÕES	AÇÃO DO SIS.

MÓDULO 2 - ANÁLISE DE ÁRVORE DE FALHAS (AAF)

LÓGICA	VÁLVULA ABERTURA OU VÁLVULA FECHAMENTO OU TRANSMISSOR DE TEMPERATURA OU TRANSMISSOR DE PRESSÃO OU CLP OU RESFRIADOR A AR
TAXA DE ACIDENTES FATAIS (POR ANO)	0.17609148



MÓDULO 3 - CÁLCULO DO NÍVEL DE INTEGRIDADE DE SEGURANÇA (SIL)

NÚMERO DE OPERÁRIOS EXPOSTOS AO RISCO:	10
QUANTIDADE DE SEMANAS TRABALHADAS POR ANO:	44
QUANTIDADE DE HORAS TRABALHADAS POR SEMANA:	44
FAR TOLERÁVEL:	0.1
FAR SEM PROTEÇÃO:	909.5634297520661
FATOR DE REDUÇÃO DE RISCOS:	9095.63429752066
NÍVEL DE INTEGRIDADE DE SEGURANÇA (SIL):	SIL 3

MÓDULO 4 - DEFINIÇÃO DA FUNÇÃO INSTRUMENTADA DE SEGURANÇA (SIF)

SUBSISTEMA SENSOR

INSTRUMENTOS	SIL	VOTAÇÃO
TRANSMISSOR DE TEMPERATURA	SIL 3	2oo3
TRANSMISSOR DE PRESSÃO	SIL 3	1oo3

SUBSISTEMA LÓGICO

INSTRUMENTOS	SIL	VOTAÇÃO
CLP	SIL 3	2oo2D

SUBSISTEMA ELEMENTO FINAL

INSTRUMENTOS	SIL	VOTAÇÃO
VÁLVULA FECHAMENTO	SIL 3	1oo3
VÁLVULA ABERTURA	SIL 3	1oo3

RELATÓRIO DE ANÁLISE E QUANTIFICAÇÃO DE RISCOS

PROJETISTA: CAIO AMALFI

SISTEMA: DESESTABILIZACAO EMULSOES PETROLEO-UNESP-2017-08-14

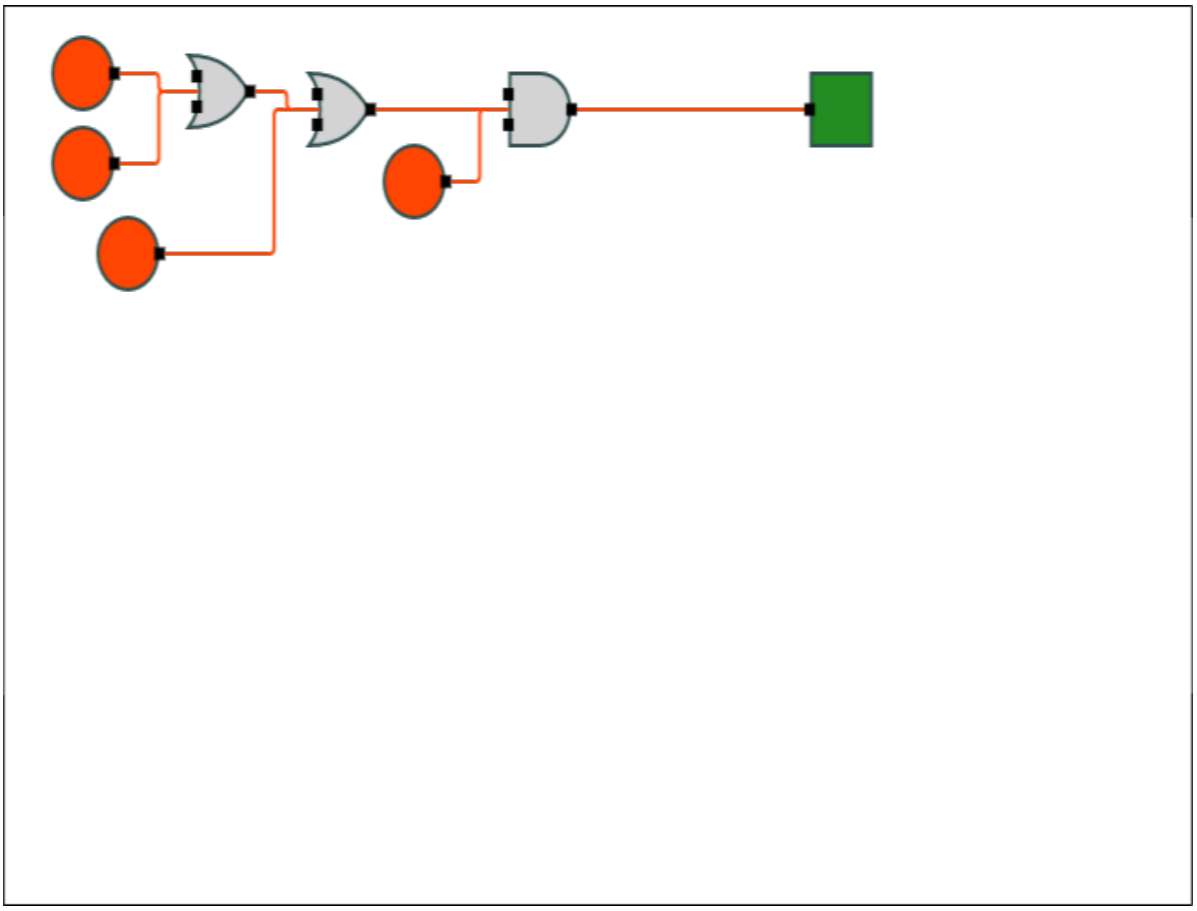
MÓDULO 1 - ANÁLISE DE RISCOS (HAZOP)

PARTE: Entrada Micro-Ondas 1
LOCAL: V2 Vz
ELEMENTO: Petroleo
PARÂMETRO: VAZÃO
DESVIO: NÃO
EFEITO: Variado na Vazão

POSSIBILIDADE DE OCORRÊNCIA	SIM
CAUSAS	BOMBA DESLIGADA OU QUEBRADA.
CONSEQUÊNCIAS	PARADA DA UNIDADE.
PROTEÇÃO	NÃO CONSTA.
RISCO ACEITÁVEL	NÃO
AÇÕES	AÇÃO DOS OPERADORES; AÇÃO DO SIS.

MÓDULO 2 - ANÁLISE DE ÁRVORE DE FALHAS (AAF)

LÓGICA	VÁLVULA ABERTURA OU VÁLVULA FECHAMENTO OU FALHA OPERADOR E PROBABILIDADE DE OPERADOR EM CAMPO
TAXA DE ACIDENTES FATAIS (POR ANO)	0.20815



MÓDULO 3 - CÁLCULO DO NÍVEL DE INTEGRIDADE DE SEGURANÇA (SIL)

NÚMERO DE OPERÁRIOS EXPOSTOS AO RISCO:	10
QUANTIDADE DE SEMANAS TRABALHADAS POR ANO:	44
QUANTIDADE DE HORAS TRABALHADAS POR SEMANA:	38
FAR TOLERÁVEL:	0.1
FAR SEM PROTEÇÃO:	1244.9162679425838
FATOR DE REDUÇÃO DE RISCOS:	12449.162679425837
NÍVEL DE INTEGRIDADE DE SEGURANÇA (SIL):	SIL 4

MÓDULO 4 - DEFINIÇÃO DA FUNÇÃO INSTRUMENTADA DE SEGURANÇA (SIF)

SUBSISTEMA SENSOR

INSTRUMENTOS SIL VOTAÇÃO

SUBSISTEMA LÓGICO

INSTRUMENTOS SIL VOTAÇÃO

SUBSISTEMA ELEMENTO FINAL

INSTRUMENTOS	**SIL**	**VOTAÇÃO**
VÁLVULA FECHAMENTO	SIL 3	1oo3
VÁLVULA ABERTURA	SIL 3	1oo3

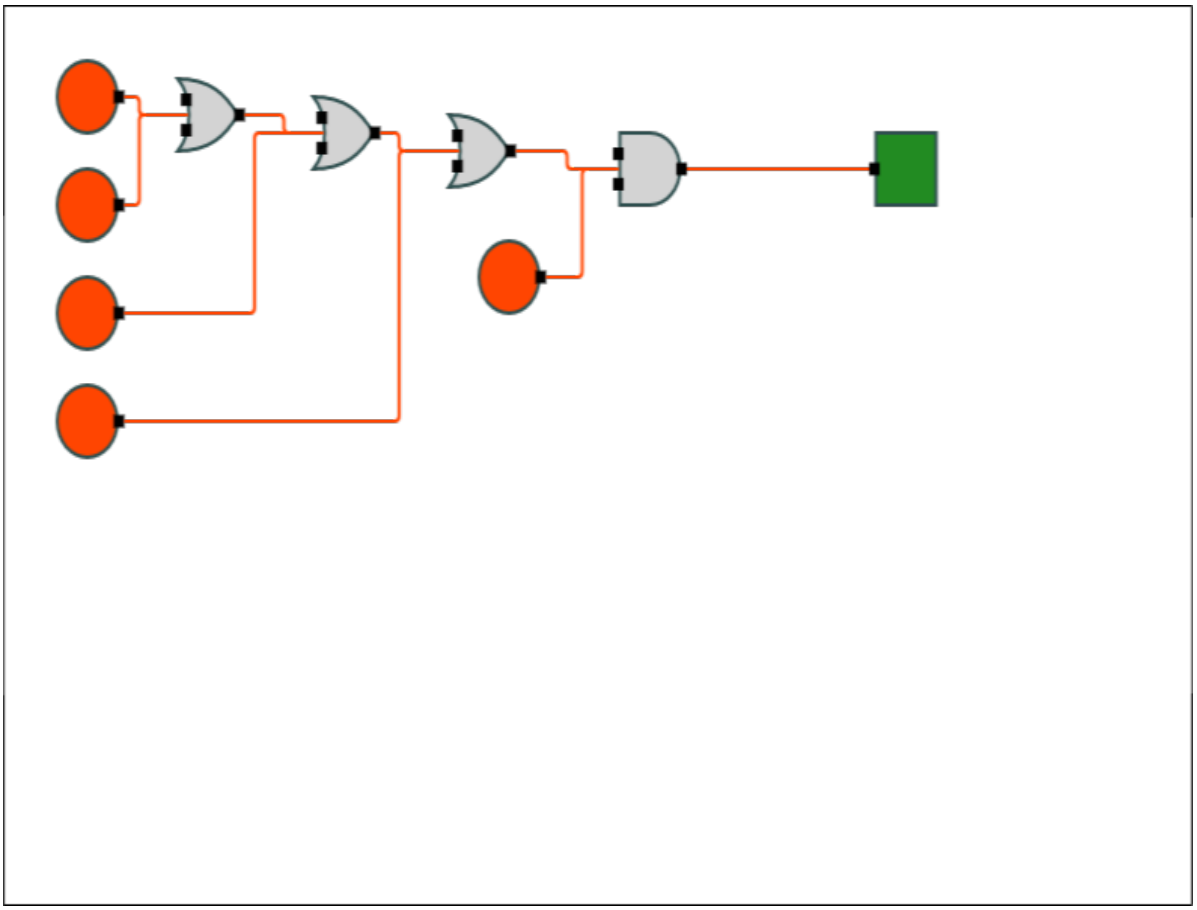
MÓDULO 1 - ANÁLISE DE RISCOS (HAZOP)

PARTE: Entrada Micro-Ondas 2
LOCAL: V2 Vz
ELEMENTO: Petroleo
PARÂMETRO: FLUXO
DESVIO: MENOS
EFEITO: Variado na Vazão

POSSIBILIDADE DE OCORRÊNCIA	SIM
CAUSAS	VISCOSIDADE ELEVADA DA EMULSÃO; BAIXA ROTAÇÃO.
CONSEQUÊNCIAS	QUEBRA DA BOMBA; REDUÇÃO NA ALIMENTAÇÃO DO REATOR.
PROTEÇÃO	NÃO CONSTA.
RISCO ACEITÁVEL	NÃO.
AÇÕES	AÇÃO DOS OPERADORES; AÇÃO DO SIS.

MÓDULO 2 - ANÁLISE DE ÁRVORE DE FALHAS (AAF)

LÓGICA	TRANSMISSOR DE FLUXO OU VÁLVULA ABERTURA OU VÁLVULA FECHAMENTO OU FALHA OPERADOR E PROBABILIDADE DE OPERADOR EM CAMPO
TAXA DE ACIDENTES FATAIS (POR ANO)	0.213975



MÓDULO 3 - CÁLCULO DO NÍVEL DE INTEGRIDADE DE SEGURANÇA (SIL)

NÚMERO DE OPERÁRIOS EXPOSTOS AO RISCO:	10
QUANTIDADE DE SEMANAS TRABALHADAS POR ANO:	44
QUANTIDADE DE HORAS TRABALHADAS POR SEMANA:	32
FAR TOLERÁVEL:	0.1
FAR SEM PROTEÇÃO:	1519.7088068181818
FATOR DE REDUÇÃO DE RISCOS:	15197.088068181816
NÍVEL DE INTEGRIDADE DE SEGURANÇA (SIL):	SIL 4

MÓDULO 4 - DEFINIÇÃO DA FUNÇÃO INSTRUMENTADA DE SEGURANÇA (SIF)

SUBSISTEMA SENSOR

INSTRUMENTOS	SIL	VOTAÇÃO
TRANSMISSOR DE FLUXO	SIL 3	1oo3

SUBSISTEMA LÓGICO

INSTRUMENTOS	SIL	VOTAÇÃO

SUBSISTEMA ELEMENTO FINAL

INSTRUMENTOS	SIL	VOTAÇÃO
VÁLVULA ABERTURA	SIL 3	1oo3
VÁLVULA FECHAMENTO	SIL 3	1oo3

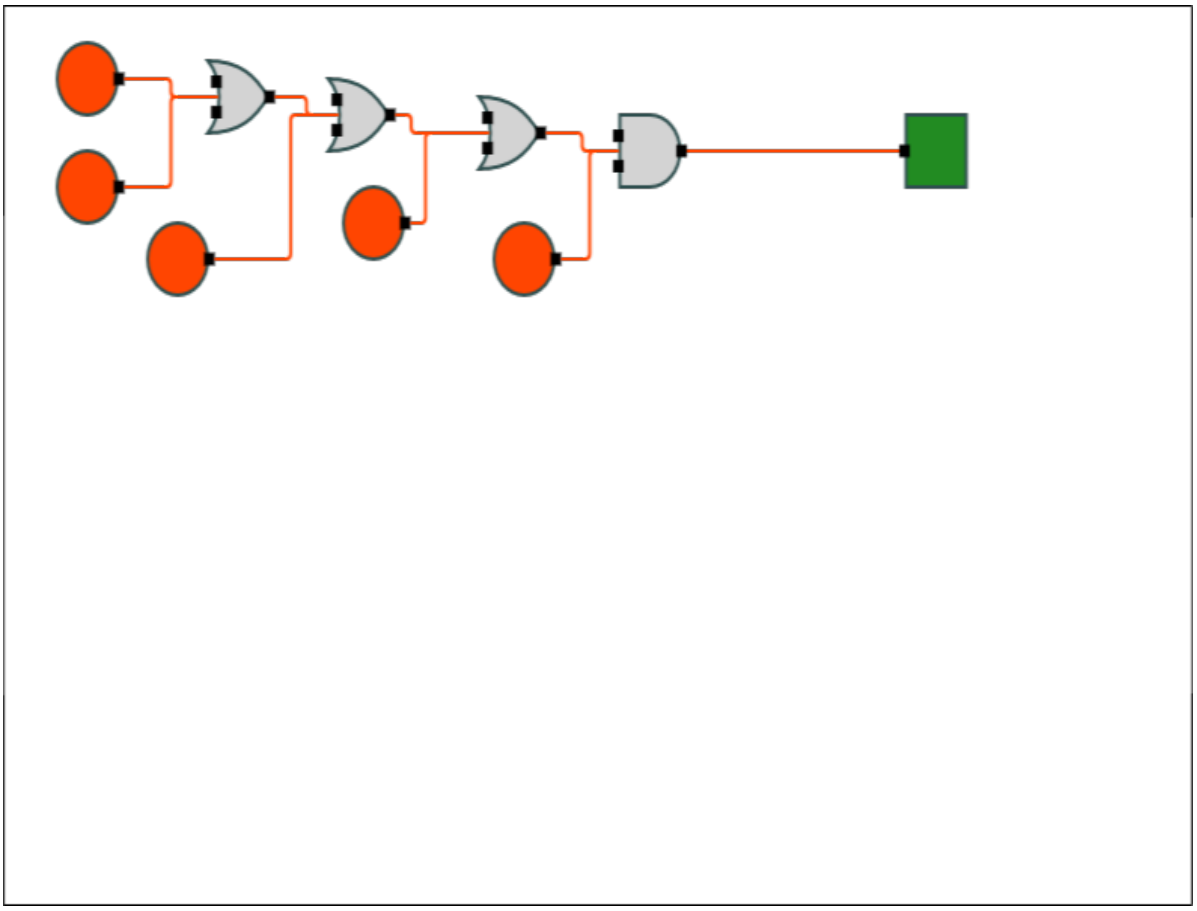
MÓDULO 1 - ANÁLISE DE RISCOS (HAZOP)

PARTE: Entrada Micro-Ondas 3
LOCAL: V2 Vz
ELEMENTO: Petroleo
PARÂMETRO: FLUXO
DESVIO: MAIS
EFEITO: Variado na Vazão

POSSIBILIDADE DE OCORRÊNCIA	SIM
CAUSAS	VISCOSIDADE BAIXA DA EMULSÃO; ELEVADA ROTAÇÃO DA BOMBA.
CONSEQUÊNCIAS	REDUÇÃO NA EFICIÊNCIA DE SEPARAÇÃO.
PROTEÇÃO	NÃO CONSTA.
RISCO ACEITÁVEL	NÃO.
AÇÕES	AÇÃO DOS OPERADORES; AÇÃO DO SIS.

MÓDULO 2 - ANÁLISE DE ÁRVORE DE FALHAS (AAF)

LÓGICA	TRANSMISSOR DE FLUXO OU TRANSMISSOR DE NÍVEL OU VÁLVULA ABERTURA OU FALHA OPERADOR E PROBABILIDADE DE OPERADOR EM CAMPO
TAXA DE ACIDENTES FATAIS (POR ANO)	0.20950000000000002



MÓDULO 3 - CÁLCULO DO NÍVEL DE INTEGRIDADE DE SEGURANÇA (SIL)

NÚMERO DE OPERÁRIOS EXPOSTOS AO RISCO:	10
QUANTIDADE DE SEMANAS TRABALHADAS POR ANO:	44
QUANTIDADE DE HORAS TRABALHADAS POR SEMANA:	32
FAR TOLERÁVEL:	0.1
FAR SEM PROTEÇÃO:	1487.9261363636365
FATOR DE REDUÇÃO DE RISCOS:	14879.261363636364
NÍVEL DE INTEGRIDADE DE SEGURANÇA (SIL):	SIL 4

MÓDULO 4 - DEFINIÇÃO DA FUNÇÃO INSTRUMENTADA DE SEGURANÇA (SIF)

SUBSISTEMA SENSOR

INSTRUMENTOS	SIL	VOTAÇÃO
TRANSMISSOR DE NÍVEL	SIL 4	1oo3
TRANSMISSOR DE FLUXO	SIL 3	1oo3

SUBSISTEMA LÓGICO

INSTRUMENTOS	SIL	VOTAÇÃO

SUBSISTEMA ELEMENTO FINAL

INSTRUMENTOS	SIL	VOTAÇÃO
VÁLVULA ABERTURA	SIL 3	1oo3

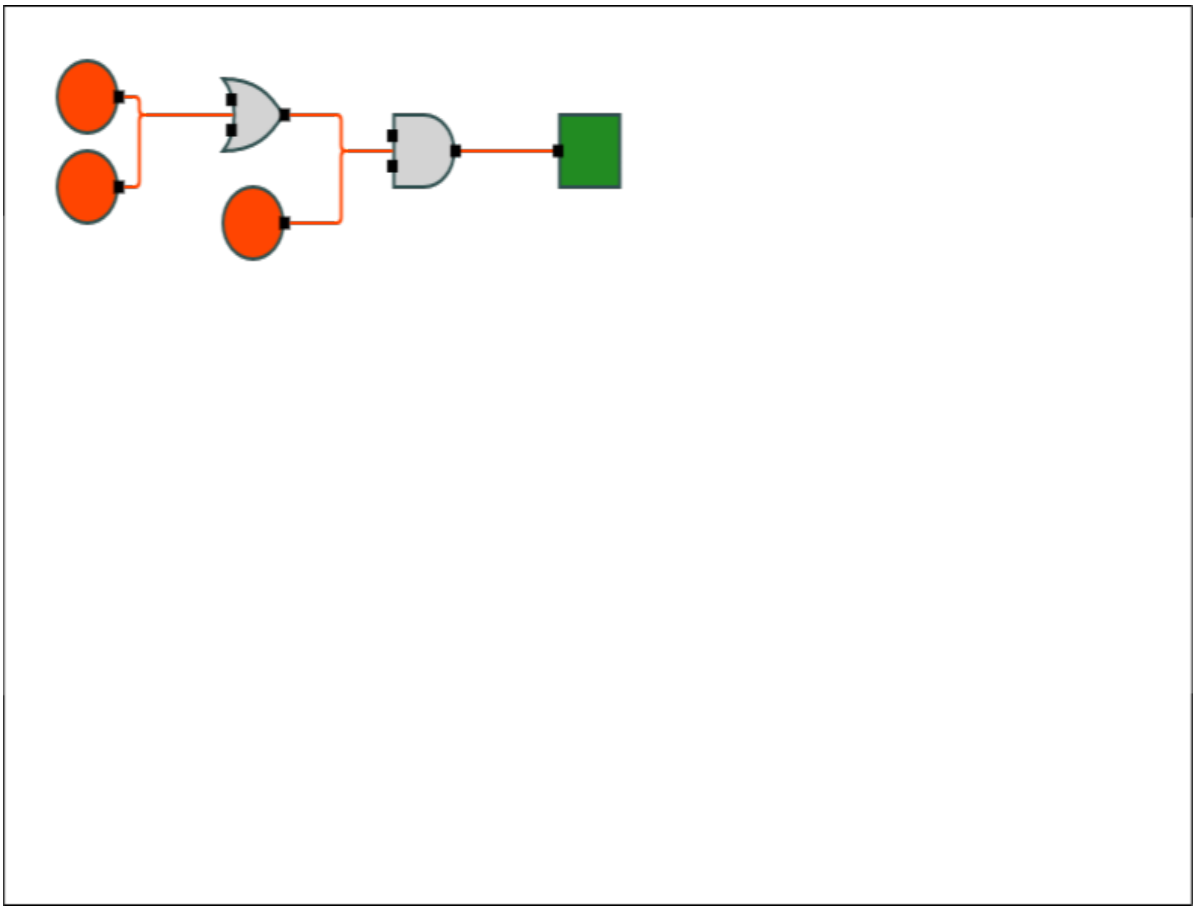
MÓDULO 1 - ANÁLISE DE RISCOS (HAZOP)

PARTE: Entrada Micro-Ondas 4
LOCAL: V2 Press
ELEMENTO: Petroleo
PARÂMETRO: PRESSÃO
DESVIO: MENOS
EFEITO: Variado na Pressão

POSSIBILIDADE DE OCORRÊNCIA	SIM
CAUSAS	FALHA NA BOMBA DE ALIMENTAÇÃO; OBSTRUÇÃO DA VÁLVULA V2.
CONSEQUÊNCIAS	PARADA DA UNIDADE; EXPLOSÃO.
PROTEÇÃO	NÃO CONSTA.
RISCO ACEITÁVEL	NÃO.
AÇÕES	AÇÃO DOS OPERADORES; AÇÃO DO SIS.

MÓDULO 2 - ANÁLISE DE ÁRVORE DE FALHAS (AAF)

LÓGICA	TRANSMISSOR DE PRESSÃO OU FALHA OPERADOR E PROBABILIDADE DE OPERADOR EM CAMPO
TAXA DE ACIDENTES FATAIS (POR ANO)	0.211625



MÓDULO 3 - CÁLCULO DO NÍVEL DE INTEGRIDADE DE SEGURANÇA (SIL)

NÚMERO DE OPERÁRIOS EXPOSTOS AO RISCO:	10
QUANTIDADE DE SEMANAS TRABALHADAS POR ANO:	42
QUANTIDADE DE HORAS TRABALHADAS POR SEMANA:	31
FAR TOLERÁVEL:	0.1
FAR SEM PROTEÇÃO:	1625.384024577573
FATOR DE REDUÇÃO DE RISCOS:	16253.84024577573
NÍVEL DE INTEGRIDADE DE SEGURANÇA (SIL):	SIL 4

MÓDULO 4 - DEFINIÇÃO DA FUNÇÃO INSTRUMENTADA DE SEGURANÇA (SIF)

SUBSISTEMA SENSOR

INSTRUMENTOS	SIL	VOTAÇÃO
TRANSMISSOR DE PRESSÃO	SIL 3	1oo3

SUBSISTEMA LÓGICO

INSTRUMENTOS	SIL	VOTAÇÃO

SUBSISTEMA ELEMENTO FINAL

INSTRUMENTOS	SIL	VOTAÇÃO

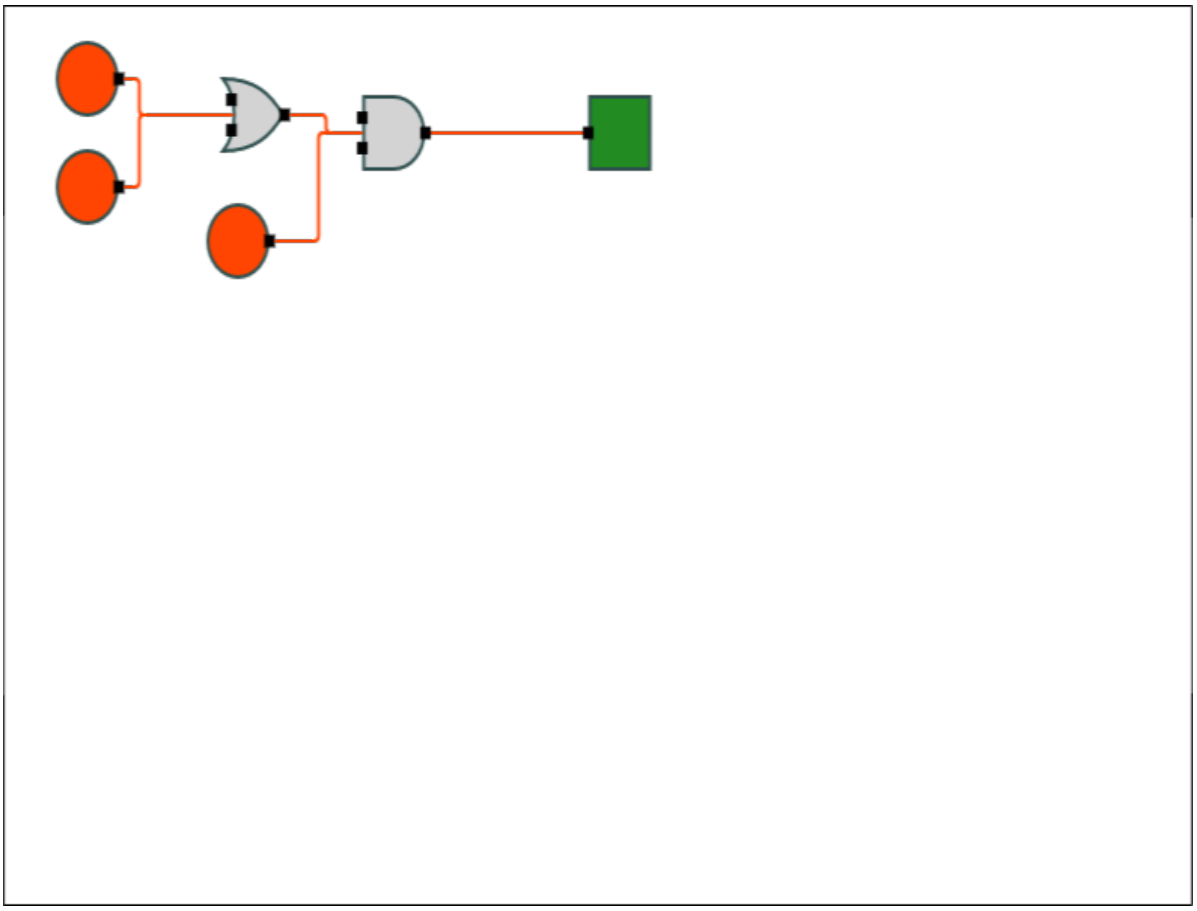
MÓDULO 1 - ANÁLISE DE RISCOS (HAZOP)

PARTE: Entrada Micro-Ondas 5
LOCAL: V2 Press
ELEMENTO: Petroleo
PARÂMETRO: PRESSÃO
DESVIO: MAIS
EFEITO: Variado na Pressão

POSSIBILIDADE DE OCORRÊNCIA	SIM
CAUSAS	VÁLVULA V2 FORA DE POSIÇÃO; OBSTRUÇÃO DA VÁLVULA V2.
CONSEQUÊNCIAS	EXPLOSÃO.
PROTEÇÃO	NÃO CONSTA.
RISCO ACEITÁVEL	NÃO.
AÇÕES	AÇÃO DOS OPERADORES; AÇÃO DO SIS.

MÓDULO 2 - ANÁLISE DE ÁRVORE DE FALHAS (AAF)

LÓGICA	TRANSMISSOR DE PRESSÃO OU TRANSMISSOR DE PRESSÃO E PROBABILIDADE DE OPERADOR EM CAMPO
TAXA DE ACIDENTES FATAIS (POR ANO)	0.02325



MÓDULO 3 - CÁLCULO DO NÍVEL DE INTEGRIDADE DE SEGURANÇA (SIL)

NÚMERO DE OPERÁRIOS EXPOSTOS AO RISCO:	10
QUANTIDADE DE SEMANAS TRABALHADAS POR ANO:	42
QUANTIDADE DE HORAS TRABALHADAS POR SEMANA:	32
FAR TOLERÁVEL:	0.1
FAR SEM PROTEÇÃO:	172.99107142857144
FATOR DE REDUÇÃO DE RISCOS:	1729.9107142857144
NÍVEL DE INTEGRIDADE DE SEGURANÇA (SIL):	SIL 3

MÓDULO 4 - DEFINIÇÃO DA FUNÇÃO INSTRUMENTADA DE SEGURANÇA (SIF)

SUBSISTEMA SENSOR

INSTRUMENTOS	SIL	VOTAÇÃO
TRANSMISSOR DE PRESSÃO	SIL 3	1oo3

SUBSISTEMA LÓGICO

INSTRUMENTOS	SIL	VOTAÇÃO

SUBSISTEMA ELEMENTO FINAL

INSTRUMENTOS	SIL	VOTAÇÃO

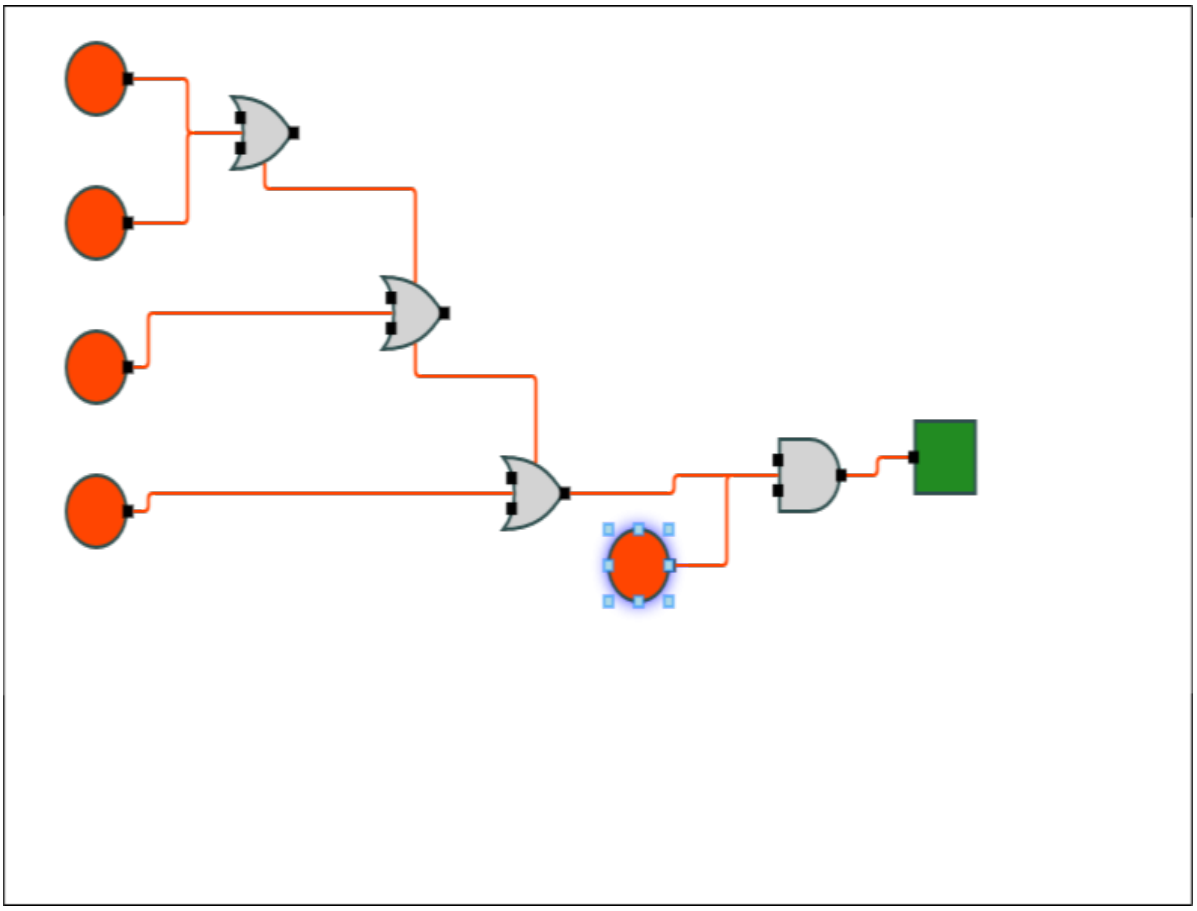
MÓDULO 1 - ANÁLISE DE RISCOS (HAZOP)

PARTE: Entrada Micro-Ondas 6
LOCAL: V2 Nv
ELEMENTO: Petroleo
PARÂMETRO: NÍVEL
DESVIO: MENOS
EFEITO: Variado no Nível

POSSIBILIDADE DE OCORRÊNCIA	SIM
CAUSAS	RESERVATÓRIO DE EMULSÃO VAZIO.
CONSEQUÊNCIAS	PARADA DA UNIDADE.
PROTEÇÃO	NÃO CONSTA.
RISCO ACEITÁVEL	NÃO.
AÇÕES	AÇÃO DOS OPERADORES; AÇÃO DO SIS.

MÓDULO 2 - ANÁLISE DE ÁRVORE DE FALHAS (AAF)

LÓGICA	VÁLVULA FECHAMENTO OU VÁLVULA ABERTURA OU TRANSMISSOR DE NÍVEL OU FALHA OPERADOR PROBABILIDADE DE OPERADOR EM CAMPO E PROBABILIDADE DE OPERADOR EM CAMPO
TAXA DE ACIDENTES FATAIS (POR ANO)	0.271675



MÓDULO 3 - CÁLCULO DO NÍVEL DE INTEGRIDADE DE SEGURANÇA (SIL)

NÚMERO DE OPERÁRIOS EXPOSTOS AO RISCO:	5
QUANTIDADE DE SEMANAS TRABALHADAS POR ANO:	44
QUANTIDADE DE HORAS TRABALHADAS POR SEMANA:	30
FAR TOLERÁVEL:	0.2
FAR SEM PROTEÇÃO:	4116.287878787879
FATOR DE REDUÇÃO DE RISCOS:	20581.439393939392
NÍVEL DE INTEGRIDADE DE SEGURANÇA (SIL):	SIL 4

MÓDULO 4 - DEFINIÇÃO DA FUNÇÃO INSTRUMENTADA DE SEGURANÇA (SIF)

SUBSISTEMA SENSOR

INSTRUMENTOS	SIL	VOTAÇÃO
TRANSMISSOR DE NÍVEL	SIL 4	1oo3

SUBSISTEMA LÓGICO

INSTRUMENTOS	SIL	VOTAÇÃO

SUBSISTEMA ELEMENTO FINAL

INSTRUMENTOS	SIL	VOTAÇÃO
VÁLVULA ABERTURA	SIL 3	1oo3
VÁLVULA FECHAMENTO	SIL 3	1oo3

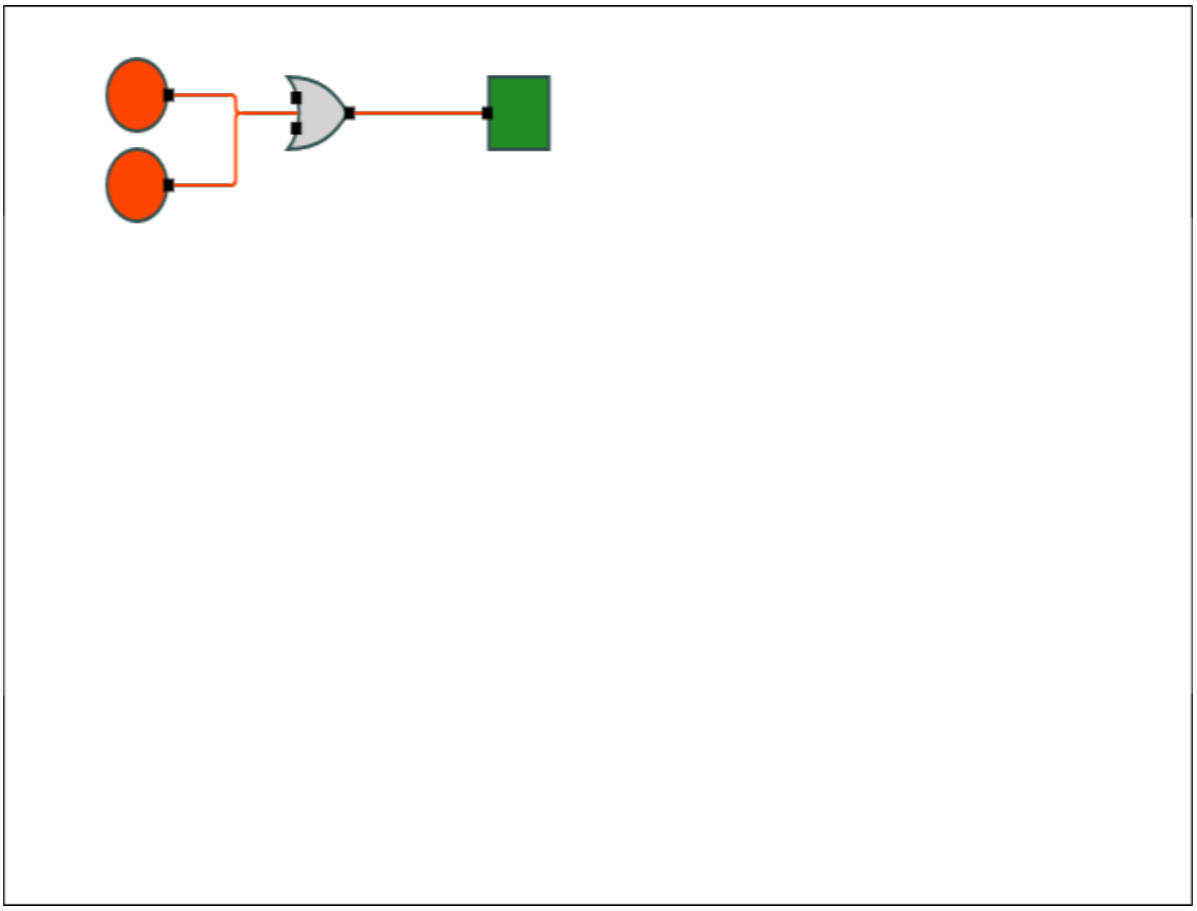
MÓDULO 1 - ANÁLISE DE RISCOS (HAZOP)

PARTE: Entrada Micro-Ondas 7
LOCAL: V2 Nv
ELEMENTO: Petroleo
PARÂMETRO: NÍVEL
DESVIO: MAIS
EFEITO: Variado no Nível

POSSIBILIDADE DE OCORRÊNCIA	SIM
CAUSAS	TRANSBORDO DO RESERVATÓRIO DE EMULSÃO.
CONSEQUÊNCIAS	CONTAMINAÇÃO AMBIENTAL.
PROTEÇÃO	NÃO CONSTA.
RISCO ACEITÁVEL	NÃO.
AÇÕES	AÇÃO DOS OPERADORES; AÇÃO DO SIS.

MÓDULO 2 - ANÁLISE DE ÁRVORE DE FALHAS (AAF)

LÓGICA	TRANSMISSOR DE NÍVEL OU TRANSMISSOR DE NÍVEL
TAXA DE ACIDENTES FATAIS (POR ANO)	0.0082



MÓDULO 3 - CÁLCULO DO NÍVEL DE INTEGRIDADE DE SEGURANÇA (SIL)

NÚMERO DE OPERÁRIOS EXPOSTOS AO RISCO:	5
QUANTIDADE DE SEMANAS TRABALHADAS POR ANO:	44
QUANTIDADE DE HORAS TRABALHADAS POR SEMANA:	44
FAR TOLERÁVEL:	0.2
FAR SEM PROTEÇÃO:	84.7107438016529
FATOR DE REDUÇÃO DE RISCOS:	423.55371900826447
NÍVEL DE INTEGRIDADE DE SEGURANÇA (SIL):	SIL 2

MÓDULO 4 - DEFINIÇÃO DA FUNÇÃO INSTRUMENTADA DE SEGURANÇA (SIF)

SUBSISTEMA SENSOR

INSTRUMENTOS	SIL	VOTAÇÃO
TRANSMISSOR DE NÍVEL	SIL 2	2oo2D

SUBSISTEMA LÓGICO

INSTRUMENTOS	SIL	VOTAÇÃO

SUBSISTEMA ELEMENTO FINAL

INSTRUMENTOS	SIL	VOTAÇÃO

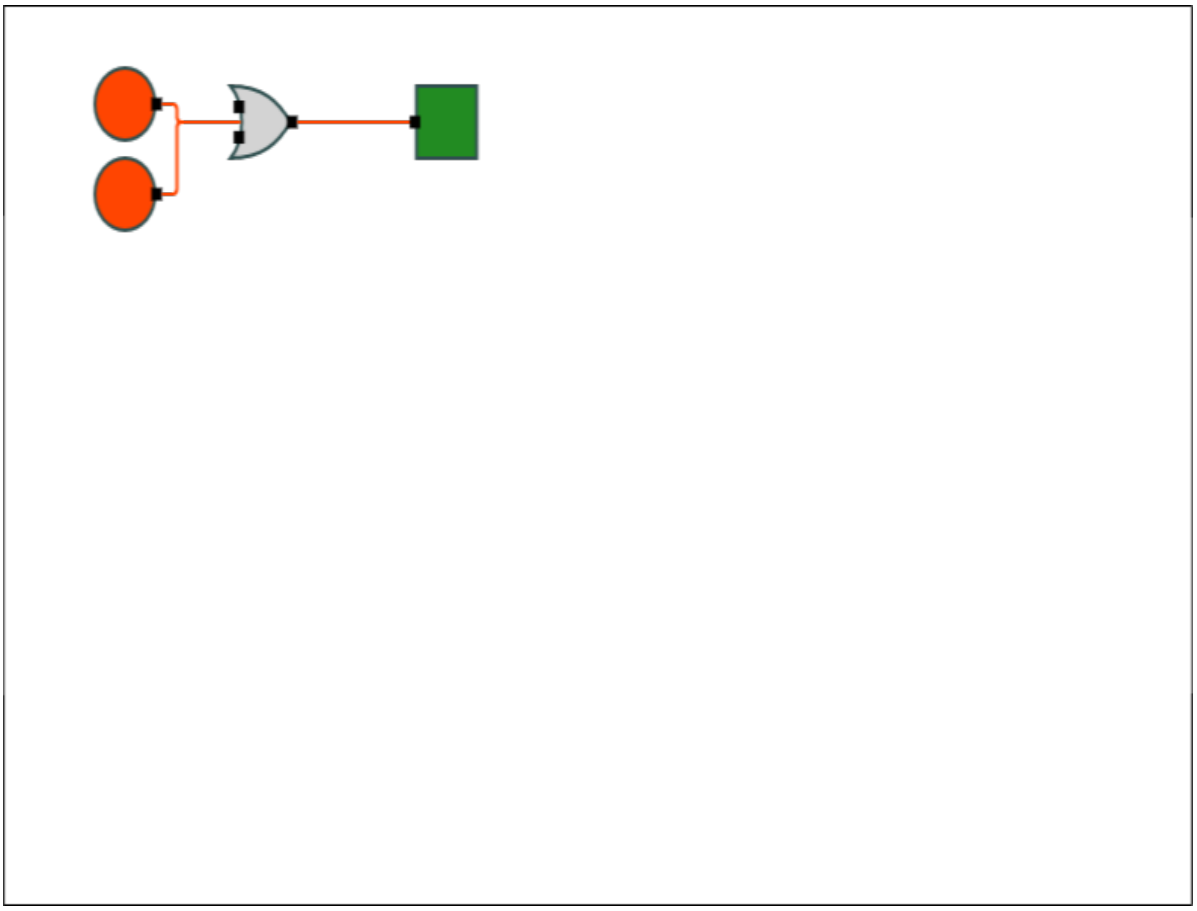
MÓDULO 1 - ANÁLISE DE RISCOS (HAZOP)

PARTE: Entrada Micro-Ondas 8
LOCAL: V2 Viscosidade
ELEMENTO: Petroleo
PARÂMETRO: VISCOSIDADE
DESVIO: MENOS
EFEITO: Variado para Viscosidade

POSSIBILIDADE DE OCORRÊNCIA	SIM
CAUSAS	CARACTERÍSTICA DO ÓLEO.
CONSEQUÊNCIAS	EMULSÃO ESCOA RAPIDAMENTE PELO PROCESSO.
PROTEÇÃO	NÃO CONSTA.
RISCO ACEITÁVEL	NÃO.
AÇÕES	AÇÃO DOS OPERADORES; AÇÃO DO SIS.

MÓDULO 2 - ANÁLISE DE ÁRVORE DE FALHAS (AAF)

LÓGICA	TRANSMISSOR DE VISCOSIDADE OU TRANSMISSOR DE VISCOSIDADE
TAXA DE ACIDENTES FATAIS (POR ANO)	0.0522



MÓDULO 3 - CÁLCULO DO NÍVEL DE INTEGRIDADE DE SEGURANÇA (SIL)

NÚMERO DE OPERÁRIOS EXPOSTOS AO RISCO:	8
QUANTIDADE DE SEMANAS TRABALHADAS POR ANO:	30
QUANTIDADE DE HORAS TRABALHADAS POR SEMANA:	28
FAR TOLERÁVEL:	0.125
FAR SEM PROTEÇÃO:	776.7857142857143
FATOR DE REDUÇÃO DE RISCOS:	6214.285714285715
NÍVEL DE INTEGRIDADE DE SEGURANÇA (SIL):	SIL 3

MÓDULO 4 - DEFINIÇÃO DA FUNÇÃO INSTRUMENTADA DE SEGURANÇA (SIF)

SUBSISTEMA SENSOR

INSTRUMENTOS	SIL	VOTAÇÃO
TRANSMISSOR DE VISCOSIDADE	SIL 3	2oo3

SUBSISTEMA LÓGICO

INSTRUMENTOS	SIL	VOTAÇÃO

SUBSISTEMA ELEMENTO FINAL

INSTRUMENTOS	SIL	VOTAÇÃO

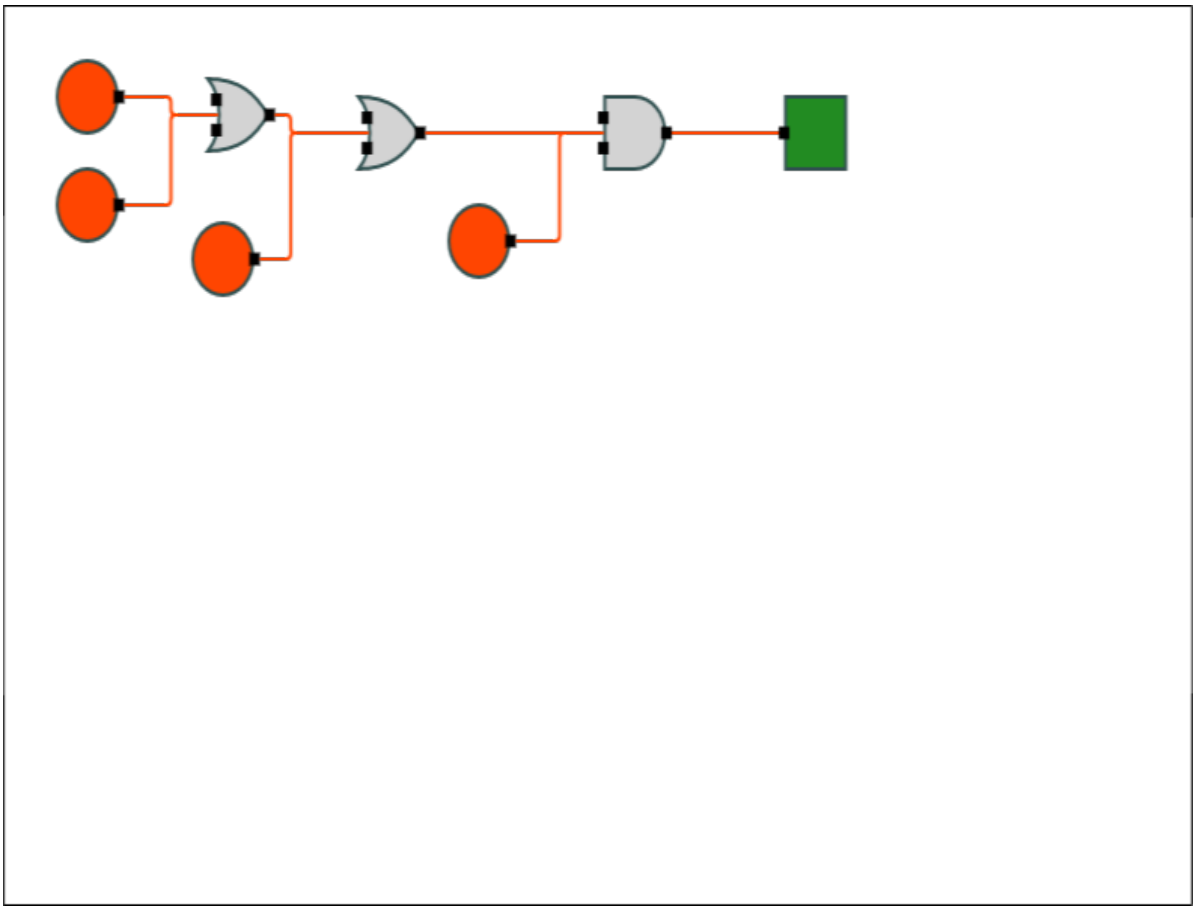
MÓDULO 1 - ANÁLISE DE RISCOS (HAZOP)

PARTE: Entrada Micro-Ondas 9
LOCAL: V2 Viscosidade
ELEMENTO: Petroleo
PARÂMETRO: VISCOSIDADE
DESVIO: MAIS
EFEITO: Variado para Viscosidade

POSSIBILIDADE DE OCORRÊNCIA	SIM
CAUSAS	CARACTERÍSTICA DO ÓLEO.
CONSEQUÊNCIAS	DIFICULDADE NO ESCOAMENTO PARA ALIMENTAÇÃO DA UNIDADE.
PROTEÇÃO	NÃO CONSTA.
RISCO ACEITÁVEL	NÃO.
AÇÕES	AÇÃO DOS OPERADORES; AÇÃO DO SIS.

MÓDULO 2 - ANÁLISE DE ÁRVORE DE FALHAS (AAF)

LÓGICA	TRANSMISSOR DE VISCOSIDADE OU TRANSMISSOR DE FLUXO OU FALHA OPERADOR E PROBABILIDADE DE OPERADOR EM CAMPO
TAXA DE ACIDENTES FATAIS (POR ANO)	0.21235



MÓDULO 3 - CÁLCULO DO NÍVEL DE INTEGRIDADE DE SEGURANÇA (SIL)

NÚMERO DE OPERÁRIOS EXPOSTOS AO RISCO:	8
QUANTIDADE DE SEMANAS TRABALHADAS POR ANO:	42
QUANTIDADE DE HORAS TRABALHADAS POR SEMANA:	30
FAR TOLERÁVEL:	0.125
FAR SEM PROTEÇÃO:	2106.6468253968255
FATOR DE REDUÇÃO DE RISCOS:	16853.174603174604
NÍVEL DE INTEGRIDADE DE SEGURANÇA (SIL):	SIL 4

MÓDULO 4 - DEFINIÇÃO DA FUNÇÃO INSTRUMENTADA DE SEGURANÇA (SIF)

SUBSISTEMA SENSOR

INSTRUMENTOS	SIL	VOTAÇÃO
TRANSMISSOR DE VISCOSIDADE	SIL 4	1oo3
TRANSMISSOR DE FLUXO	SIL 3	1oo3

SUBSISTEMA LÓGICO

INSTRUMENTOS	SIL	VOTAÇÃO

SUBSISTEMA ELEMENTO FINAL

INSTRUMENTOS	SIL	VOTAÇÃO

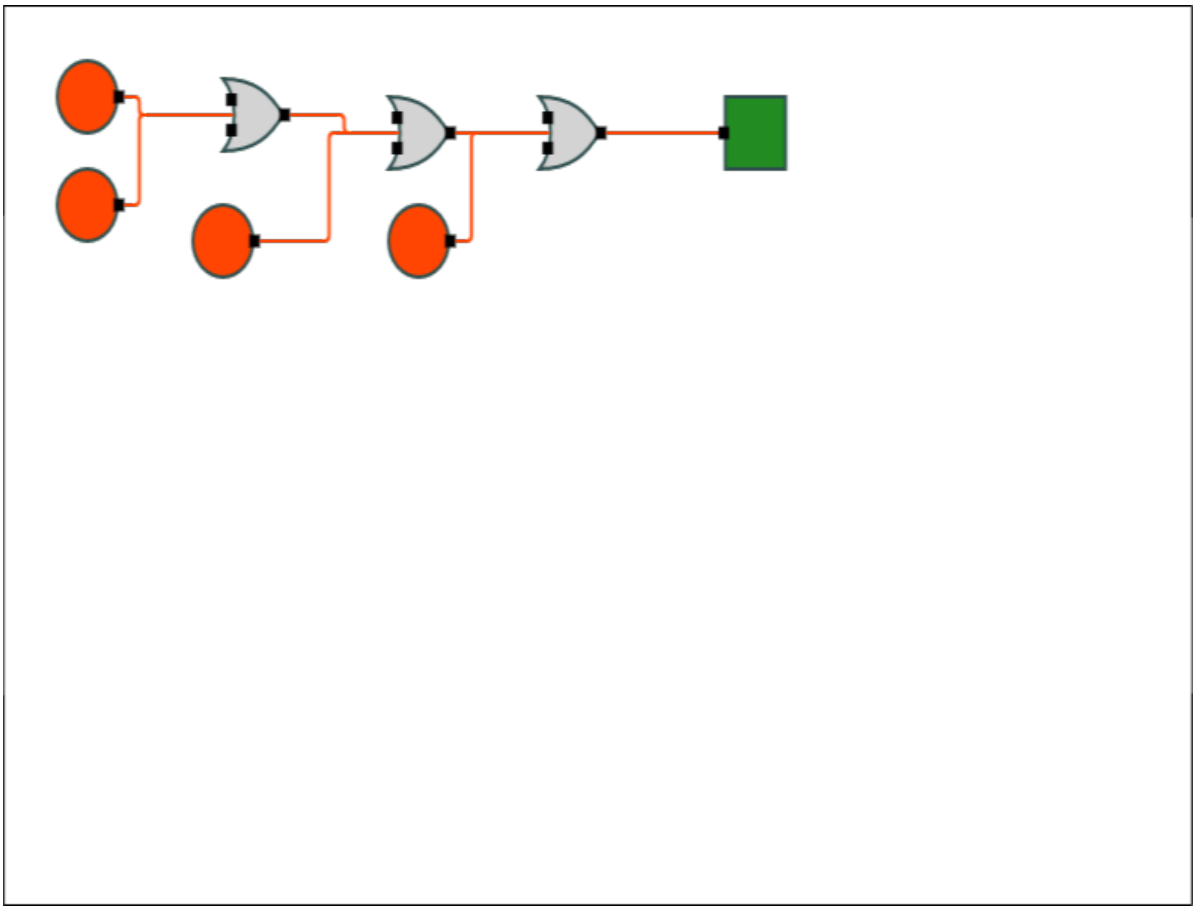
MÓDULO 1 - ANÁLISE DE RISCOS (HAZOP)

PARTE: Tanque de Separacao 1
LOCAL: Entrada Vz
ELEMENTO: Petroleo
PARÂMETRO: VAZÃO
DESVIO: NÃO
EFEITO: Variado para Vazão

POSSIBILIDADE DE OCORRÊNCIA	SIM
CAUSAS	OBSTRUÇÃO ENTRADA DO REATOR; OBSTRUÇÃO NA SAÍDA DO REATOR; OBSTRUÇÃO NA VÁLVULA REGULADORA DE PRESSÃO
CONSEQUÊNCIAS	PARADA NA UNIDADE.
PROTEÇÃO	NÃO CONSTA.
RISCO ACEITÁVEL	NÃO.
AÇÕES	AÇÃO DOS OPERADORES; AÇÃO DO SIS.

MÓDULO 2 - ANÁLISE DE ÁRVORE DE FALHAS (AAF)

LÓGICA	TRANSMISSOR DE NÍVEL OU TRANSMISSOR DE FLUXO OU VÁLVULA ABERTURA OU VÁLVULA FECHAMENTO
TAXA DE ACIDENTES FATAIS (POR ANO)	0.06



MÓDULO 3 - CÁLCULO DO NÍVEL DE INTEGRIDADE DE SEGURANÇA (SIL)

NÚMERO DE OPERÁRIOS EXPOSTOS AO RISCO:	4
QUANTIDADE DE SEMANAS TRABALHADAS POR ANO:	45
QUANTIDADE DE HORAS TRABALHADAS POR SEMANA:	44
FAR TOLERÁVEL:	0.25
FAR SEM PROTEÇÃO:	757.5757575757575
FATOR DE REDUÇÃO DE RISCOS:	3030.30303030303
NÍVEL DE INTEGRIDADE DE SEGURANÇA (SIL):	SIL 3

MÓDULO 4 - DEFINIÇÃO DA FUNÇÃO INSTRUMENTADA DE SEGURANÇA (SIF)

SUBSISTEMA SENSOR

INSTRUMENTOS	SIL	VOTAÇÃO
TRANSMISSOR DE FLUXO	SIL 3	1oo3
TRANSMISSOR DE NÍVEL	SIL 3	2oo3

SUBSISTEMA LÓGICO

INSTRUMENTOS	SIL	VOTAÇÃO

SUBSISTEMA ELEMENTO FINAL

INSTRUMENTOS	SIL	VOTAÇÃO
VÁLVULA ABERTURA	SIL 3	1oo3
VÁLVULA FECHAMENTO	SIL 3	1oo3

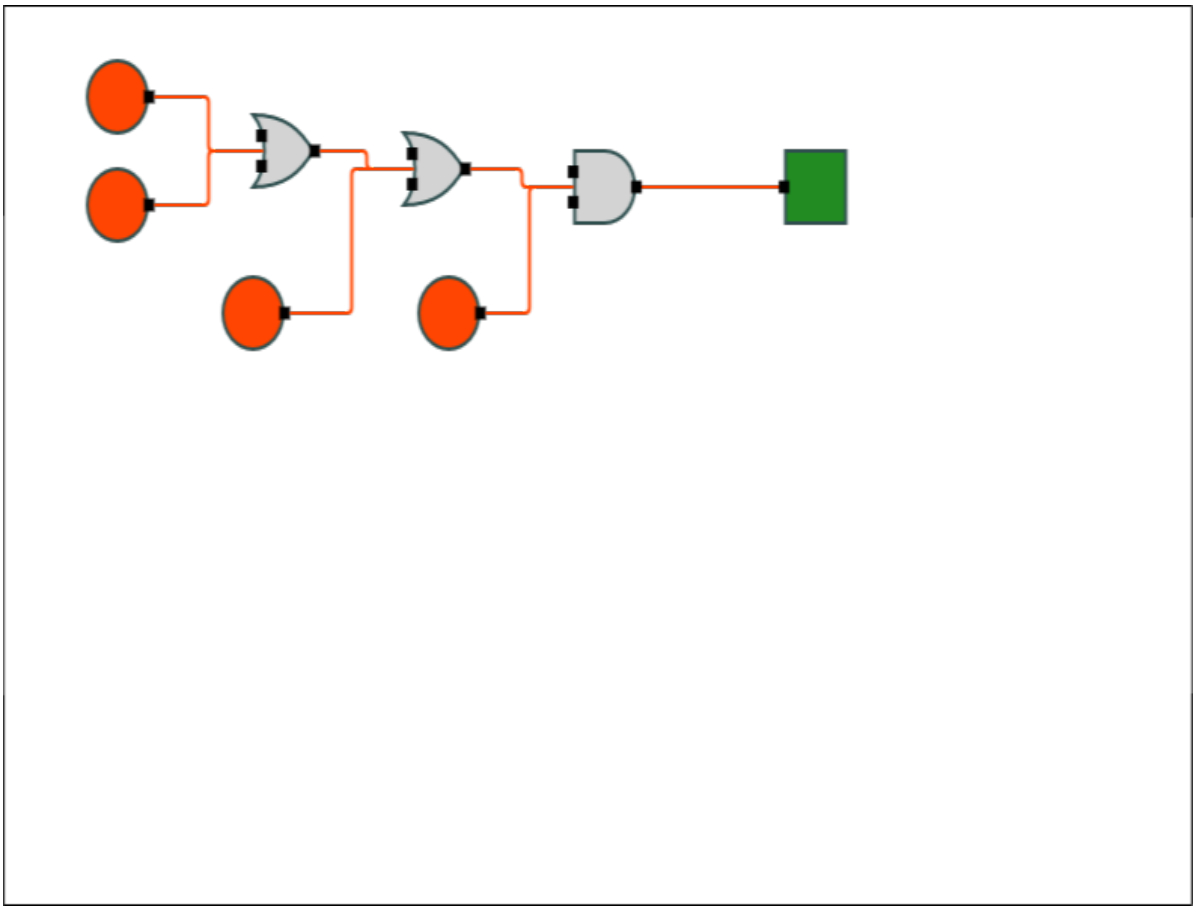
MÓDULO 1 - ANÁLISE DE RISCOS (HAZOP)

PARTE: Tanque de Separacao 2
LOCAL: Entrada Vz
ELEMENTO: Petroleo
PARÂMETRO: FLUXO
DESVIO: MENOS
EFEITO: Variado para Vazão

POSSIBILIDADE DE OCORRÊNCIA	SIM
CAUSAS	VAZAMENTO DE CONEXÕES E TUBULAÇÕES; VAZAMENTO NO REATOR.
CONSEQUÊNCIAS	CONTAMINAÇÃO AMBIENTAL.
PROTEÇÃO	ALARME DE PROTEÇÃO.
RISCO ACEITÁVEL	NÃO.
AÇÕES	AÇÃO DAS VÁLVULAS; AÇÃO DOS OPERADORES; AÇÃO DO SDCD; AÇÃO DO SIS.

MÓDULO 2 - ANÁLISE DE ÁRVORE DE FALHAS (AAF)

LÓGICA	TRANSMISSOR DE NÍVEL OU TRANSMISSOR DE FLUXO OU FALHA OPERADOR E PROBABILIDADE DE OPERADOR EM CAMPO
TAXA DE ACIDENTES FATAIS (POR ANO)	0.20685



MÓDULO 3 - CÁLCULO DO NÍVEL DE INTEGRIDADE DE SEGURANÇA (SIL)

NÚMERO DE OPERÁRIOS EXPOSTOS AO RISCO:	4
QUANTIDADE DE SEMANAS TRABALHADAS POR ANO:	32
QUANTIDADE DE HORAS TRABALHADAS POR SEMANA:	44
FAR TOLERÁVEL:	0.25
FAR SEM PROTEÇÃO:	3672.7627840909095
FATOR DE REDUÇÃO DE RISCOS:	14691.051136363638
NÍVEL DE INTEGRIDADE DE SEGURANÇA (SIL):	SIL 4

MÓDULO 4 - DEFINIÇÃO DA FUNÇÃO INSTRUMENTADA DE SEGURANÇA (SIF)

SUBSISTEMA SENSOR

INSTRUMENTOS	SIL	VOTAÇÃO
TRANSMISSOR DE NÍVEL	SIL 4	1oo3
TRANSMISSOR DE FLUXO	SIL 3	1oo3

SUBSISTEMA LÓGICO

INSTRUMENTOS	SIL	VOTAÇÃO

SUBSISTEMA ELEMENTO FINAL

INSTRUMENTOS	SIL	VOTAÇÃO

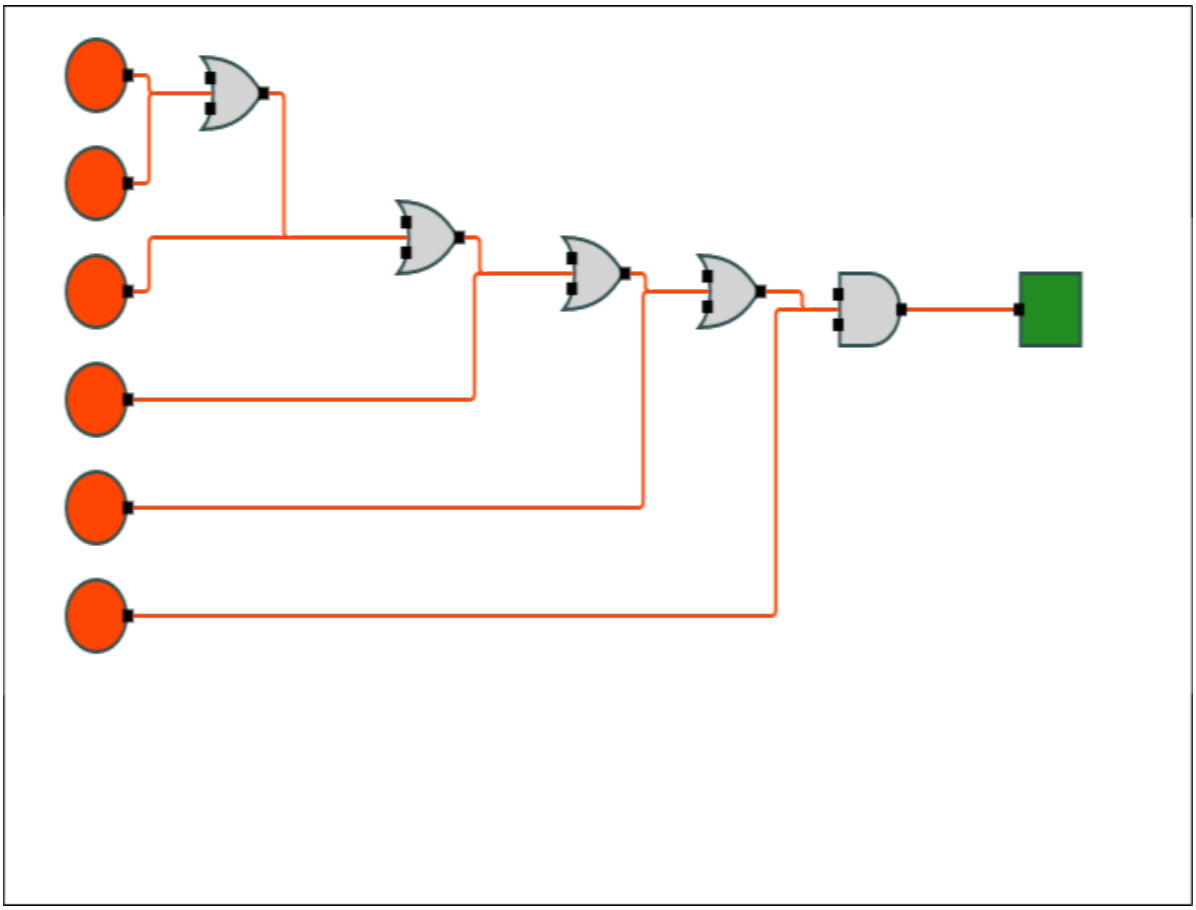
MÓDULO 1 - ANÁLISE DE RISCOS (HAZOP)

PARTE: Tanque de Separacao 3
LOCAL: Entrada Vz
ELEMENTO: Petroleo
PARÂMETRO: FLUXO
DESVIO: MAIS
EFEITO: Variado para Vazão

POSSIBILIDADE DE OCORRÊNCIA	SIM
CAUSAS	VÁLVULA REGULADORA DE PRESSÃO DANIFICADA. VÁLVULA REGULADORA TOTALMENTE ABERTA.
CONSEQUÊNCIAS	REDUÇÃO NA EFICIÊNCIA DE SEPARAÇÃO.
PROTEÇÃO	ALARME DE PROTEÇÃO.
RISCO ACEITÁVEL	NÃO.
AÇÕES	AÇÃO DO SDCD; AÇÃO MANUAL DOS OPERADORES; AÇÃO DO SIS.

MÓDULO 2 - ANÁLISE DE ÁRVORE DE FALHAS (AAF)

LÓGICA	TRANSMISSOR DE NÍVEL OU TRANSMISSOR DE NÍVEL OU TRANSMISSOR DE FLUXO OU TRANSMISSOR DE FLUXO OU FALHA OPERADOR E PROBABILIDADE DE OPERADOR EM CAMPO
TAXA DE ACIDENTES FATAIS (POR ANO)	0.2137



MÓDULO 3 - CÁLCULO DO NÍVEL DE INTEGRIDADE DE SEGURANÇA (SIL)

NÚMERO DE OPERÁRIOS EXPOSTOS AO RISCO:	4
QUANTIDADE DE SEMANAS TRABALHADAS POR ANO:	44
QUANTIDADE DE HORAS TRABALHADAS POR SEMANA:	44
FAR TOLERÁVEL:	0.25
FAR SEM PROTEÇÃO:	2759.555785123967
FATOR DE REDUÇÃO DE RISCOS:	11038.223140495867
NÍVEL DE INTEGRIDADE DE SEGURANÇA (SIL):	SIL 4

MÓDULO 4 - DEFINIÇÃO DA FUNÇÃO INSTRUMENTADA DE SEGURANÇA (SIF)

SUBSISTEMA SENSOR

INSTRUMENTOS	SIL	VOTAÇÃO
TRANSMISSOR DE NÍVEL	SIL 4	1oo3
TRANSMISSOR DE FLUXO	SIL 3	1oo3

SUBSISTEMA LÓGICO

INSTRUMENTOS	SIL	VOTAÇÃO

SUBSISTEMA ELEMENTO FINAL

INSTRUMENTOS	SIL	VOTAÇÃO

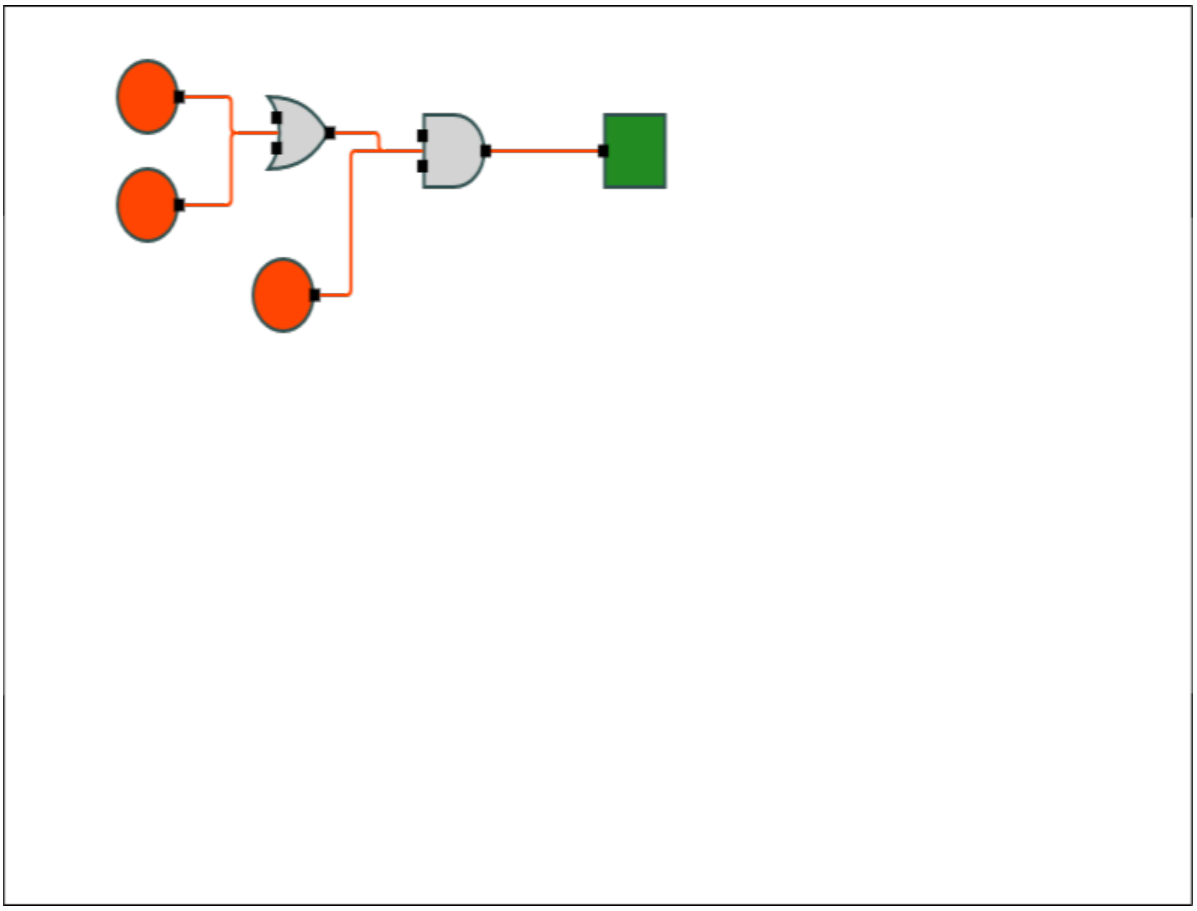
MÓDULO 1 - ANÁLISE DE RISCOS (HAZOP)

PARTE: Tanque de Separacao 4
LOCAL: Entrada Press
ELEMENTO: Petroleo
PARÂMETRO: PRESSÃO
DESVIO: MENOS
EFEITO: Variado para Pressão

POSSIBILIDADE DE OCORRÊNCIA	SIM
CAUSAS	VÁLVULA REGULADORA DE PRESSÃO TOTALMENTE ABERTA; VAZAMENTO NO REATOR.
CONSEQUÊNCIAS	REDUÇÃO NA EFICIÊNCIA DE SEPARAÇÃO.
PROTEÇÃO	NÃO CONSTA.
RISCO ACEITÁVEL	NÃO
AÇÕES	AÇÃO MANUAL DOS OPERADORES; AÇÃO DO SIS.

MÓDULO 2 - ANÁLISE DE ÁRVORE DE FALHAS (AAF)

LÓGICA	TRANSMISSOR DE PRESSÃO OU TRANSMISSOR DE PRESSÃO E FALHA OPERADOR
TAXA DE ACIDENTES FATAIS (POR ANO)	0.07440000000000001



MÓDULO 3 - CÁLCULO DO NÍVEL DE INTEGRIDADE DE SEGURANÇA (SIL)

NÚMERO DE OPERÁRIOS EXPOSTOS AO RISCO:	12
QUANTIDADE DE SEMANAS TRABALHADAS POR ANO:	44
QUANTIDADE DE HORAS TRABALHADAS POR SEMANA:	32
FAR TOLERÁVEL:	0.08333333333333333
FAR SEM PROTEÇÃO:	440.3409090909091
FATOR DE REDUÇÃO DE RISCOS:	5284.09090909091
NÍVEL DE INTEGRIDADE DE SEGURANÇA (SIL):	SIL 3

MÓDULO 4 - DEFINIÇÃO DA FUNÇÃO INSTRUMENTADA DE SEGURANÇA (SIF)

SUBSISTEMA SENSOR

INSTRUMENTOS	SIL	VOTAÇÃO
TRANSMISSOR DE PRESSÃO	SIL 3	1oo3

SUBSISTEMA LÓGICO

INSTRUMENTOS	SIL	VOTAÇÃO

SUBSISTEMA ELEMENTO FINAL

INSTRUMENTOS	SIL	VOTAÇÃO

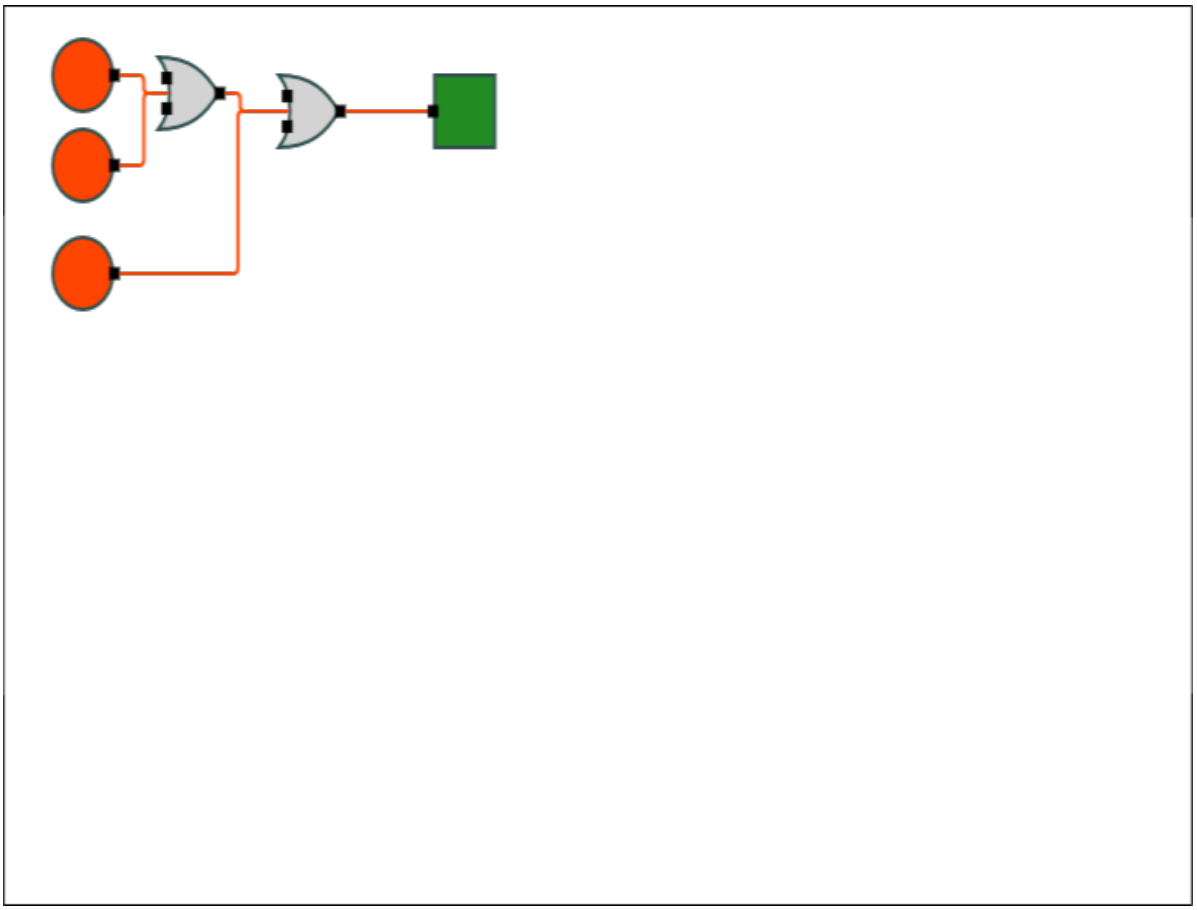
MÓDULO 1 - ANÁLISE DE RISCOS (HAZOP)

PARTE: Tanque de Separacao 5
LOCAL: Entrada Press
ELEMENTO: Petroleo
PARÂMETRO: PRESSÃO
DESVIO: MAIS
EFEITO: Variado na Pressão

POSSIBILIDADE DE OCORRÊNCIA	SIM
CAUSAS	VÁLVULA DE PRESSÃO FECHADA; OBSTRUÇÃO DO REATOR.
CONSEQUÊNCIAS	EXPLOSÃO.
PROTEÇÃO	SISTEMA DE PROTEÇÃO INDIVIDUAL; ALARME DE PROTEÇÃO.
RISCO ACEITÁVEL	NÃO.
AÇÕES	AÇÃO DO SCDCD; AÇÃO DO SISTEMA DE PROTEÇÃO INDIVIDUAL; AÇÃO DO SIS.

MÓDULO 2 - ANÁLISE DE ÁRVORE DE FALHAS (AAF)

LÓGICA	VÁLVULA ABERTURA OU VÁLVULA FECHAMENTO OU TRANSMISSOR DE PRESSÃO
TAXA DE ACIDENTES FATAIS (POR ANO)	0.0791



MÓDULO 3 - CÁLCULO DO NÍVEL DE INTEGRIDADE DE SEGURANÇA (SIL)

NÚMERO DE OPERÁRIOS EXPOSTOS AO RISCO:	12
QUANTIDADE DE SEMANAS TRABALHADAS POR ANO:	44
QUANTIDADE DE HORAS TRABALHADAS POR SEMANA:	34
FAR TOLERÁVEL:	0.08333333333333333
FAR SEM PROTEÇÃO:	440.61942959001783
FATOR DE REDUÇÃO DE RISCOS:	5287.433155080214
NÍVEL DE INTEGRIDADE DE SEGURANÇA (SIL):	SIL 3

MÓDULO 4 - DEFINIÇÃO DA FUNÇÃO INSTRUMENTADA DE SEGURANÇA (SIF)

SUBSISTEMA SENSOR

INSTRUMENTOS	SIL	VOTAÇÃO
TRANSMISSOR DE PRESSÃO	SIL 3	1oo3

SUBSISTEMA LÓGICO

INSTRUMENTOS	SIL	VOTAÇÃO

SUBSISTEMA ELEMENTO FINAL

INSTRUMENTOS	SIL	VOTAÇÃO
VÁLVULA FECHAMENTO	SIL 3	1oo3
VÁLVULA ABERTURA	SIL 3	1oo3

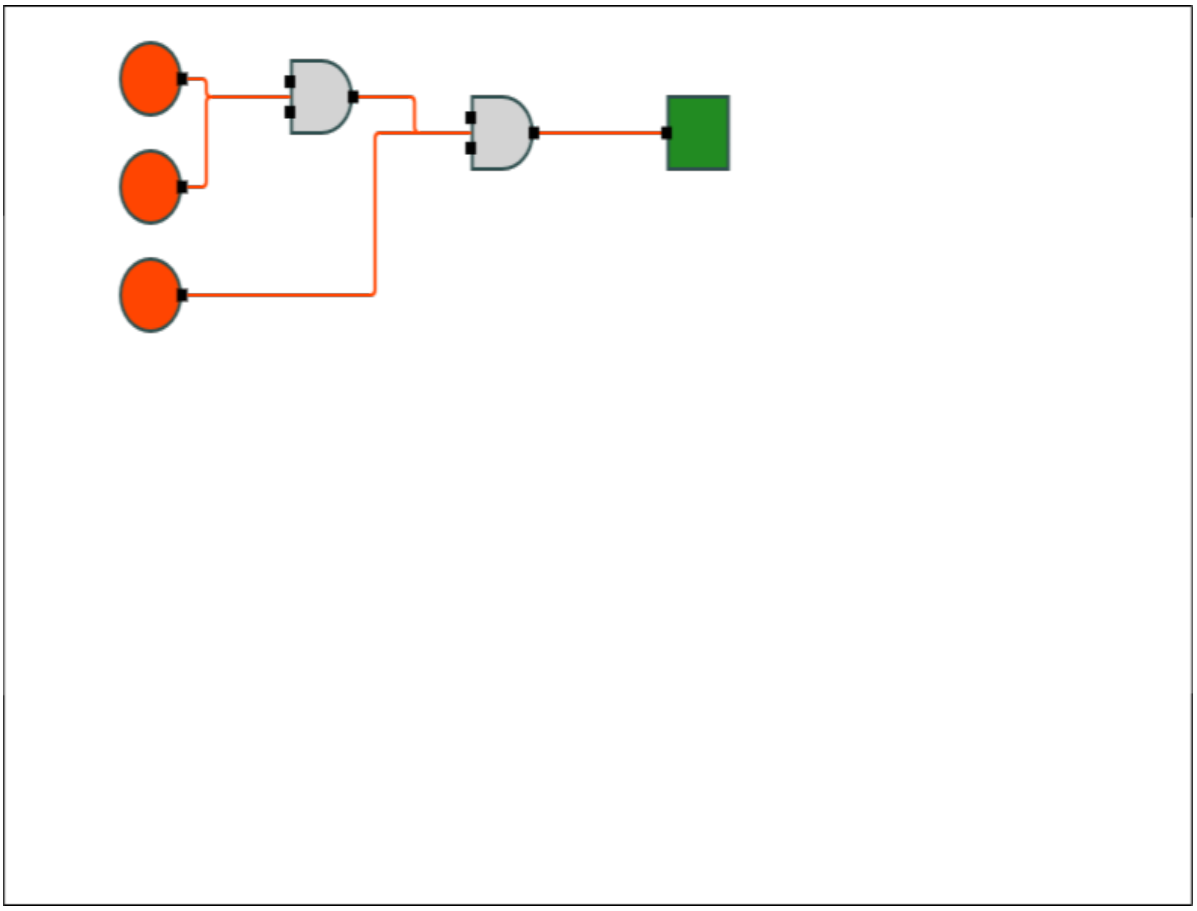
MÓDULO 1 - ANÁLISE DE RISCOS (HAZOP)

PARTE: Tanque de Separacao 6
LOCAL: Entrada Temperatura
ELEMENTO: Petroleo
PARÂMETRO: TEMPERATURA
DESVIO: MENOS
EFEITO: Variado para Temperatura

POSSIBILIDADE DE OCORRÊNCIA	SIM
CAUSAS	FALHA NOS SENSORES DE TEMPERATURA; FALHA NO SISTEMA DE IRRADIAÇÃO.
CONSEQUÊNCIAS	INEFICIÊNCIA NO PROCESSO DE SEPARAÇÃO.
PROTEÇÃO	ALARME.
RISCO ACEITÁVEL	NÃO.
AÇÕES	AÇÃO DO SIS.

MÓDULO 2 - ANÁLISE DE ÁRVORE DE FALHAS (AAF)

LÓGICA	TRANSMISSOR DE TEMPERATURA E FALHA OPERADOR E PROBABILIDADE DE OPERADOR EM CAMPO
TAXA DE ACIDENTES FATAIS (POR ANO)	0.00392



MÓDULO 3 - CÁLCULO DO NÍVEL DE INTEGRIDADE DE SEGURANÇA (SIL)

NÚMERO DE OPERÁRIOS EXPOSTOS AO RISCO:	5
QUANTIDADE DE SEMANAS TRABALHADAS POR ANO:	44
QUANTIDADE DE HORAS TRABALHADAS POR SEMANA:	32
FAR TOLERÁVEL:	0.2
FAR SEM PROTEÇÃO:	55.68181818181818
FATOR DE REDUÇÃO DE RISCOS:	278.4090909090909
NÍVEL DE INTEGRIDADE DE SEGURANÇA (SIL):	SIL 2

MÓDULO 4 - DEFINIÇÃO DA FUNÇÃO INSTRUMENTADA DE SEGURANÇA (SIF)

SUBSISTEMA SENSOR

INSTRUMENTOS	SIL	VOTAÇÃO
TRANSMISSOR DE TEMPERATURA	SIL 2	2oo2

SUBSISTEMA LÓGICO

INSTRUMENTOS	SIL	VOTAÇÃO

SUBSISTEMA ELEMENTO FINAL

INSTRUMENTOS	SIL	VOTAÇÃO

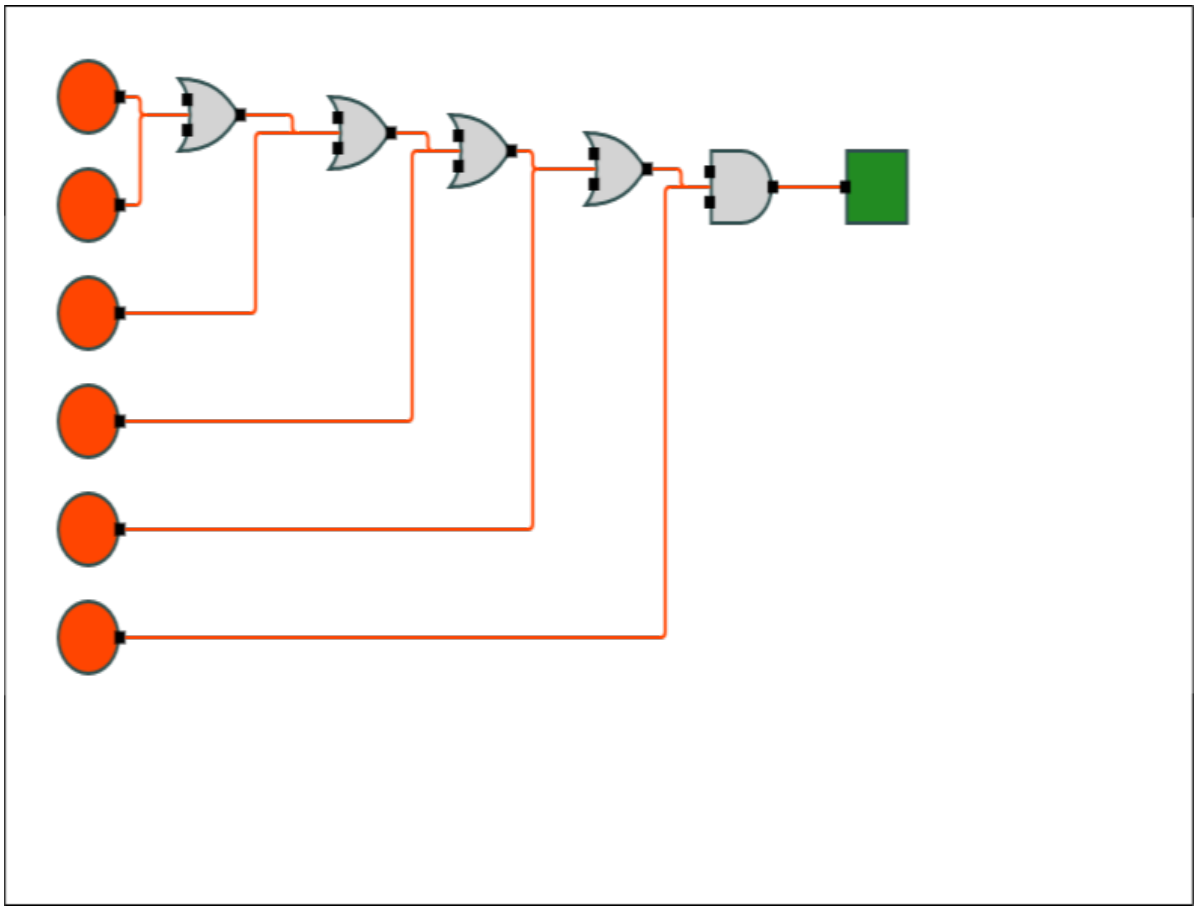
MÓDULO 1 - ANÁLISE DE RISCOS (HAZOP)

PARTE: Tanque de Separacao 7
LOCAL: Entrada Temperatura
ELEMENTO: Petroleo
PARÂMETRO: TEMPERATURA
DESVIO: MAIS
EFEITO: Variado para Temperatura

POSSIBILIDADE DE OCORRÊNCIA	SIM
CAUSAS	FALHA NOS SENSORES DE TEMPERATURA;
CONSEQUÊNCIAS	INEFICIÊNCIA NO PROCESSO DE SEPARAÇÃO; DESCONTROLE DO PROCESSO.
PROTEÇÃO	ALARME DE PROTEÇÃO; SISTEMA REDUNDANTE.
RISCO ACEITÁVEL	NÃO.
AÇÕES	AÇÃO DA REDUNDÂNCIA; AÇÃO DO SIS.

MÓDULO 2 - ANÁLISE DE ÁRVORE DE FALHAS (AAF)

LÓGICA	TRANSMISSOR DE TEMPERATURA OU TRANSMISSOR DE TEMPERATURA OU VÁLVULA FECHAMENTO OU VÁLVULA ABERTURA OU VÁLVULA FECHAMENTO E PROBABILIDADE DE OPERADOR EM CAMPO
TAXA DE ACIDENTES FATAIS (POR ANO)	0.02345



MÓDULO 3 - CÁLCULO DO NÍVEL DE INTEGRIDADE DE SEGURANÇA (SIL)

NÚMERO DE OPERÁRIOS EXPOSTOS AO RISCO:	5
QUANTIDADE DE SEMANAS TRABALHADAS POR ANO:	38
QUANTIDADE DE HORAS TRABALHADAS POR SEMANA:	40
FAR TOLERÁVEL:	0.2
FAR SEM PROTEÇÃO:	308.55263157894734
FATOR DE REDUÇÃO DE RISCOS:	1542.7631578947367
NÍVEL DE INTEGRIDADE DE SEGURANÇA (SIL):	SIL 3

MÓDULO 4 - DEFINIÇÃO DA FUNÇÃO INSTRUMENTADA DE SEGURANÇA (SIF)

SUBSISTEMA SENSOR

INSTRUMENTOS	SIL	VOTAÇÃO
TRANSMISSOR DE TEMPERATURA	SIL 3	2oo3

SUBSISTEMA LÓGICO

INSTRUMENTOS	SIL	VOTAÇÃO

SUBSISTEMA ELEMENTO FINAL

INSTRUMENTOS	SIL	VOTAÇÃO
VÁLVULA FECHAMENTO	SIL 3	1oo3
VÁLVULA ABERTURA	SIL 3	1oo3

RELATÓRIO DE ANÁLISE E QUANTIFICAÇÃO DE RISCOS

PROJETISTA: CAIO AMALFI
SISTEMA: SUBESTACAO-ACOM ENERGY-2013-07-23

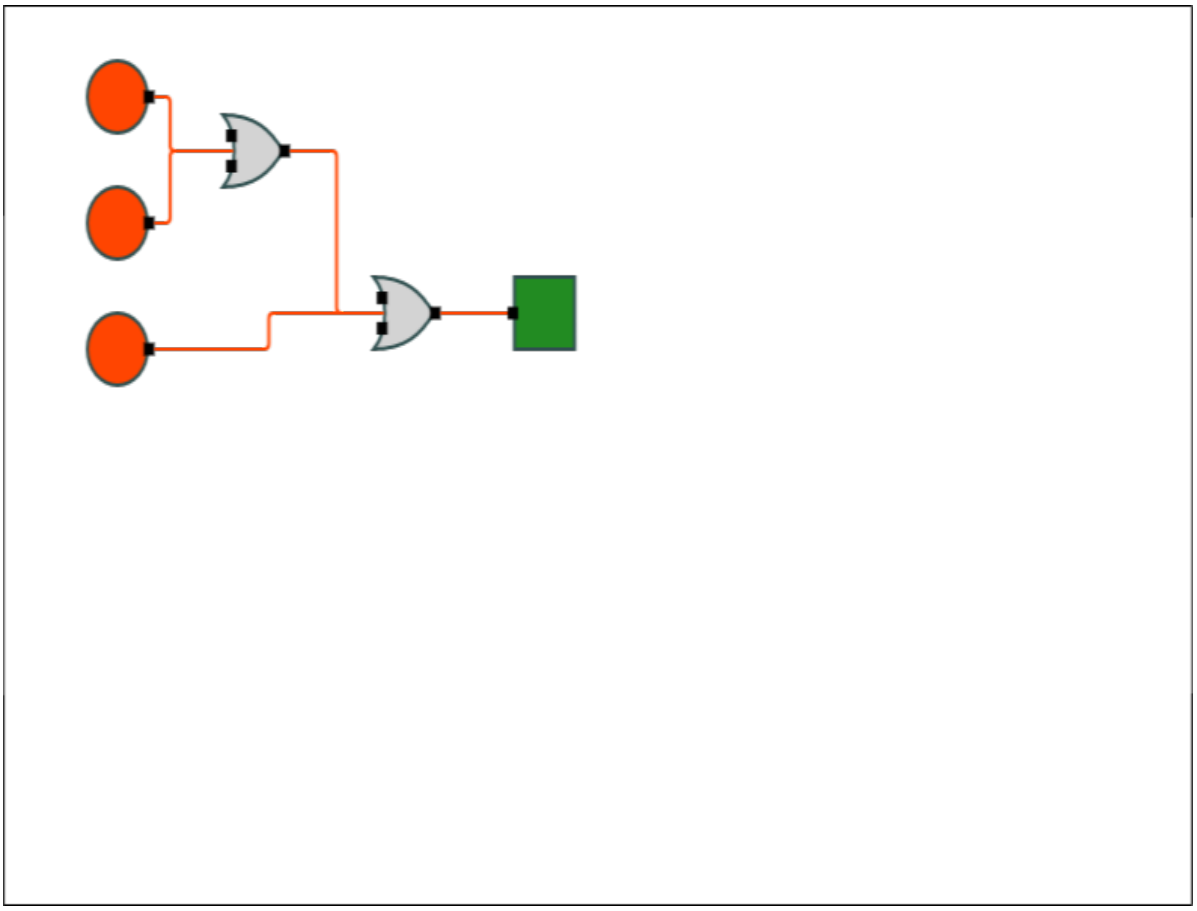
MÓDULO 1 - ANÁLISE DE RISCOS (HAZOP)

PARTE: TP
LOCAL: ENTRADA
ELEMENTO: TP
PARÂMETRO: TENSÃO
DESVIO: MAIS
EFEITO: Elevada Tensão no equipamento.

POSSIBILIDADE DE OCORRÊNCIA	SIM
CAUSAS	Falha do Disjuntor de Entrada DJ01.
CONSEQUÊNCIAS	Acionamento do Disjuntor do TP DJT04; Parada da subestação.
PROTEÇÃO	TRIP DE PROTEÇÃO SOBRETENSÃO.
RISCO ACEITÁVEL	NÃO.
AÇÕES	ALARME DE TRIP; AÇÃO DO CONTROLADOR; SIS.

MÓDULO 2 - ANÁLISE DE ÁRVORE DE FALHAS (AAF)

LÓGICA	TRANSFORMADOR TENSÃO (0.03028332) OU CLP (0.00239148) OU DISJUNTOR (0.02998548)
TAXA DE ACIDENTES FATAIS (POR ANO)	0.06266028



MÓDULO 3 - CÁLCULO DO NÍVEL DE INTEGRIDADE DE SEGURANÇA (SIL)

NÚMERO DE OPERÁRIOS EXPOSTOS AO RISCO:	1
QUANTIDADE DE SEMANAS TRABALHADAS POR ANO:	44
QUANTIDADE DE HORAS TRABALHADAS POR SEMANA:	50
FAR TOLERÁVEL:	1
FAR SEM PROTEÇÃO:	2848.1945454545453
FATOR DE REDUÇÃO DE RISCOS:	2848.1945454545453
NÍVEL DE INTEGRIDADE DE SEGURANÇA (SIL):	SIL 3

MÓDULO 4 - DEFINIÇÃO DA FUNÇÃO INSTRUMENTADA DE SEGURANÇA (SIF)

SUBSISTEMA SENSOR

INSTRUMENTOS	SIL	VOTAÇÃO
Transformador de Potencial	SIL 3	1oo2D

SUBSISTEMA LÓGICO

INSTRUMENTOS	SIL	VOTAÇÃO

SUBSISTEMA ELEMENTO FINAL

INSTRUMENTOS	SIL	VOTAÇÃO

RELATÓRIO DE ANÁLISE E QUANTIFICAÇÃO DE RISCOS

PROJETISTA: CAIO AMALFI
SISTEMA: SUBESTACAO-ACOM ENERGY-2013-07-23

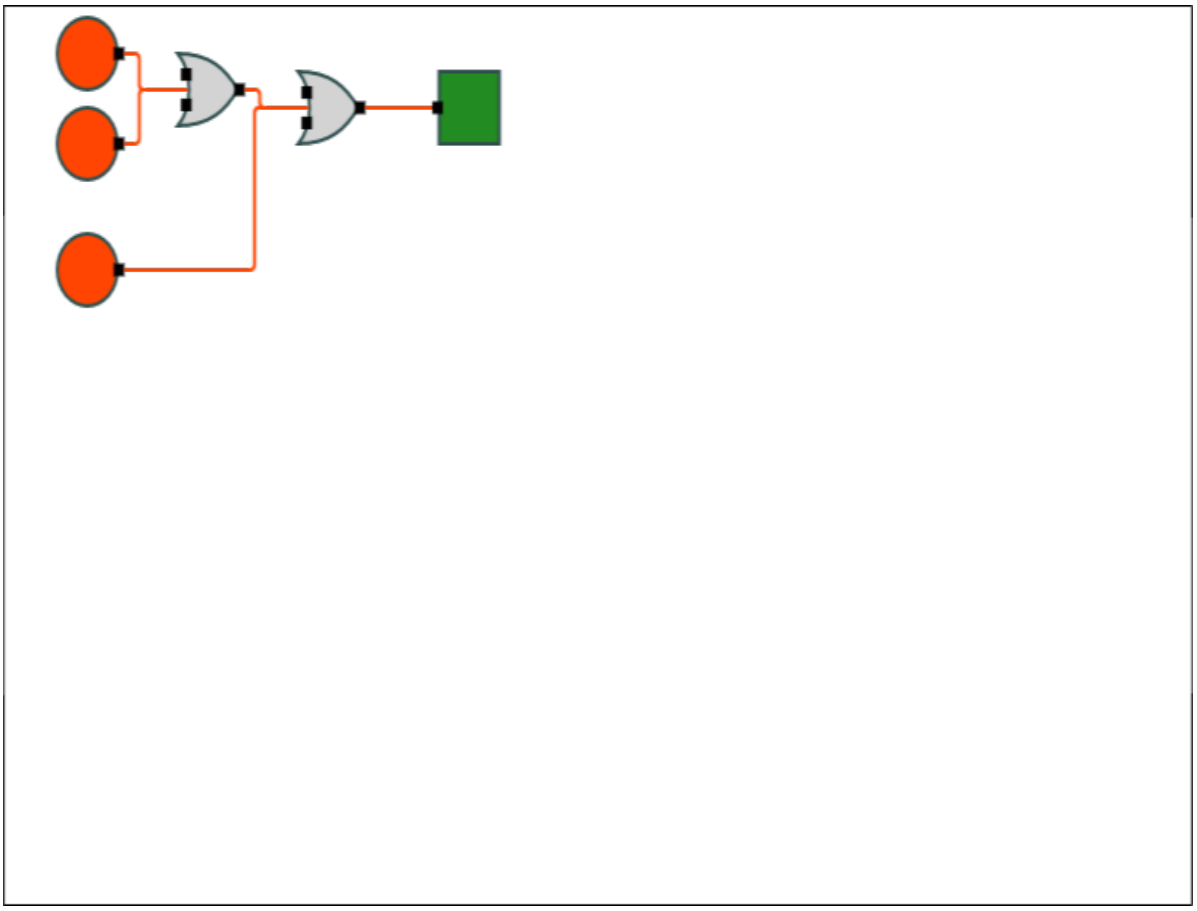
MÓDULO 1 - ANÁLISE DE RISCOS (HAZOP)

PARTE: TC
LOCAL: ENTRADA
ELEMENTO: TC
PARÂMETRO: CORRENTE
DESVIO: MAIS
EFEITO: Corrente elevada equipamento

POSSIBILIDADE DE OCORRÊNCIA	SIM
CAUSAS	Falha do Disjuntor de Entrada DJ01.
CONSEQUÊNCIAS	Acionamento do Disjuntor do TC DJT01; Parada da subestação.
PROTEÇÃO	DISJUNTOR DO TC DJTC01.
RISCO ACEITÁVEL	NÃO.
AÇÕES	AÇÃO DO CONTROLADOR PARA PARADA DA SUBESTAÇÃO; ALARME; SIS.

MÓDULO 2 - ANÁLISE DE ÁRVORE DE FALHAS (AAF)

LÓGICA	TRANSFORMADOR DE CORREN (0.02204892) OU CLP (0.00239148) OU DISJUNTOR (0.02998548)
TAXA DE ACIDENTES FATAIS (POR ANO)	0.0244404



MÓDULO 3 - CÁLCULO DO NÍVEL DE INTEGRIDADE DE SEGURANÇA (SIL)

NÚMERO DE OPERÁRIOS EXPOSTOS AO RISCO:	1
QUANTIDADE DE SEMANAS TRABALHADAS POR ANO:	44
QUANTIDADE DE HORAS TRABALHADAS POR SEMANA:	50
FAR TOLERÁVEL:	1
FAR SEM PROTEÇÃO:	1110.9272727272728
FATOR DE REDUÇÃO DE RISCOS:	1110.9272727272728
NÍVEL DE INTEGRIDADE DE SEGURANÇA (SIL):	SIL 3

MÓDULO 4 - DEFINIÇÃO DA FUNÇÃO INSTRUMENTADA DE SEGURANÇA (SIF)

SUBSISTEMA SENSOR

INSTRUMENTOS	SIL	VOTAÇÃO
Transformador de Corrente	SIL 3	1oo2D

SUBSISTEMA LÓGICO

INSTRUMENTOS	SIL	VOTAÇÃO

SUBSISTEMA ELEMENTO FINAL

INSTRUMENTOS	SIL	VOTAÇÃO