SISTOOL: FERRAMENTA WEB DE PROJETO PARA SISTEMAS INSTRUMENTADOS DE SEGURANÇA (SIS)

CAIO C. P. AMALFI, EDUARDO P. GODOY

UNESP – Universidade Estadual Paulista, Sorocaba - SP
E-mails: c_amalfi@hotmail.com, epgodoy@sorocaba.unesp.br

Abstract— Safety Instrumented Systems (SIS) are responsible for operational safety processes by monitoring values and parameters when there are risk conditions. Nowadays, the challenge of using SIS is the complexity of design procedure and the wide number of analysis methods accepted by the safety standards. The motivation for this paper is to demonstrate the simplification of SIS designs by reducing the number of people involved and automation of the procedures involved. The objective is to present an SIS analysis and design tool (SISTool) created, using web-based programming, capable of performing a study of the risks and failures of a process, calculating an adequate value for selecting the Safety Integrity Level (SIL) and selecting a correct Safety Instrumented Function (SIF) to be implemented by the SIS. The SISTool is innovative by combining all the procedures required for analysing and designing SIS in the same environment.

Keywords— SIS, risk, automation, SIL, SIF.

Resumo— Sistemas Instrumentados de Segurança (SIS) são responsáveis pela segurança operacional dos processos através do monitoramento de valores e parâmetros quando existirem condições de risco. Atualmente o desafio no uso do SIS se refere à complexidade do procedimento de projeto e a existência de diversos métodos de análise aceitos pelas normas. A motivação para este artigo é demonstrar a simplificação dos projetos de SIS através da redução do número de pessoas envolvidas e da automação dos procedimentos. O objetivo é apresentar uma ferramenta de análise e projeto de SIS (SISTool), criada usando programação para web, capaz de realizar uma análise de riscos e falhas de um processo, calcular um valor adequado para a seleção de Nível de Integridade de Segurança (SIL) e selecionar uma correta Função Instrumentada de Segurança (SIF) para ser implementada pelo SIS. A ferramenta SISTool é uma inovação pois combina todos os procedimentos de análise e projeto de SIS no mesmo ambiente.

Palavras-chave— SIS, risco, automação, SIL, SIF.

1 Introdução

Atualmente a automação é uma realidade consolidada para ambientes industriais, reduzindo custos de produção, aumentando qualidade e eficiência. Em termos simplificados, sistemas de segurança específicos tornaram-se indispensáveis para assegurar o desempenho e a integridade das plantas de processo e das malhas de controle (CATELANI; CIANI; LUONGO, 2012). Esses sistemas de segurança, designados como Sistemas de Instrumentados de Segurança (SIS), consistem em métodos de engenharia, hardware e software especialmente concebidos para prevenir e mitigar possíveis falhas e riscos que possam afetar a integridade do equipamento, os trabalhadores envolvidos e até mesmo do ambiente (IEC 61511, 2014).

A consciência da indústria sobre o uso do SIS é o resultado de tragédias ocorridas nas últimas décadas. Desde a catástrofe de Bhopal em 1984 na Índia, na planta industrial de pesticidas da Union Carbide, que teve um número de mortes de aproximadamente 15.000 devido a um vazamento de gás tóxico de 40 toneladas, na qual a atenção foi voltada para o SIS, o qual poderia prevenir o acidente (STIX, 1989). Recentemente, estão sendo realizadas discussões sobre a definição de padrões de segurança de processos industriais e sobre a simplificação do projeto desses sistemas de segurança (GOBLE; CHEDDIE, 2005).

O SIS tem como objetivo mitigar os riscos e implementar instrumentação e controle adicionais para segurança operacional em processos, tornando as plantas e suas malhas capazes de falhar com segurança, independentemente do sistema de controle tradicional, desencadeando ações automáticas para manter ou retornar um processo para um estado seguro, na presença de condições anormais (HUANG; CHEN; LI, 2012). Esses sistemas são projetados com diferentes Níveis de Integridade de Segurança (SIL) de acordo com os riscos do processo. Para o projeto, é essencial compreender o processo e analisar os riscos com base nas probabilidades e consequências.

É válido ressaltar ainda que existem vários métodos para análise de risco e cálculo do nível de segurança aceitos pelas normas de segurança (Omeiri et al., 2017). Como resultado desse vasto número, algumas dificuldades e desafios ao projetar e implementar um SIS passam a existir, como os apresentados abaixo por Goble e Cheddie (2005):

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

• Os cálculos manuais dos níveis de segurança podem causar erros que afetam diretamente o projeto SIS;

• As especificações e implantação do sistema de segurança necessário para atingir o nível de segurança exigido;

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

Além disso, é importante enfatizar que, mesmo com a tecnologia existente, o projeto de SIS ainda é realizado, em sua maioria, separadamente sem o auxílio de ferramentas automáticas (GRUHN; CHEDDIE, 2006). As poucas ferramentas computacionais existentes para auxiliar a análise de risco e construção do SIS são softwares proprietários de alto custo econômico. Tal fato cria uma requisição para uma nova abordagem para o a concepção do SIS, já que são procedimentos complexos envolvendo muitas pessoas e usando cálculos matemáticos que, se não forem seguidos corretamente, podem levar a uma implementação incorreta.

Este artigo apresenta o desenvolvimento de uma ferramenta computacional para web e dessa forma, automatizar e simplificar a análise e o projeto de SIS. O SISTool sistematiza e combina os procedimentos e cálculos necessários para analisar e projetar SIS no mesmo ambiente computacional, reduzindo o número de pessoas envolvidas, ocorrências de erros, tempo de design e custos. As principais tarefas executadas por esta ferramenta são (Gabriel, 2017):

• Análise de falhas e riscos usando o método HAZOP (*HAZARD AND OPERABILITY STUDY*);

• Quantificação de riscos e criação de árvores de falhas com suas respectivas funções lógicas;

• Cálculo de SIL através da análise de árvore de falhas (AAF);

• Definição de uma Função Instrumentada de Segurança (SIF) apropriada para o SIL calculado.

2 Conceitos Fundamentais para o Desenvolvimento da Ferramenta

2.1 Normas de Segurança Funcional

O conceito de segurança é imprescindível para projetar sistemas automáticos, uma vez que expressa a ausência de riscos inadmissíveis causados por danos físicos ao equipamento, a saúde das pessoas e até mesmo o meio ambiente (SQUILLANTE et al., 2011). A segurança funcional refere-se à segurança geral que um sistema ou equipamento depende para funcionar corretamente em resposta às suas entradas (DUROCHER; KAY, 2017). As duas principais normas utilizadas para a segurança funcional na regulação dos processos industriais são os IEC 61508 (2010) e IEC 61511 (2014). Essas normas estabelecem critérios para o desenvolvimento do SIS.

A norma internacional IEC 61508 (2010) é aplicada à segurança funcional de equipamentos elétricos, eletrônicos e eletrônicos programáveis (E / E / EP). Pode ser chamada de documento padrão de regulamentação de segurança para segmentos industriais e aplicações derivadas deste (CATELNANI; CIANI; LUONGO, 2013). A norma IEC 61511 (2014) é de grande importância na busca de produtos e certificados. É aplicável à integridade do SIS na indústria de processos (CRUZ-CAMPA; CRUZ-GOMES, 2009).

2.2 Metodologia de Análise de Riscos

Um método de análise de risco é exigido pelas normas para a construção de segurança em automação industrial, além de ser um teste sistemático realizado na fase inicial de projeto (IEC 61511, 2014). Este tipo de estudo é responsável por analisar os possíveis riscos a que o processo ou o sistema como um todo está exposto. Alguns dos métodos utilizados atualmente pelas indústrias são apresentados na Tabela 1.

Tabela 1. Métodos de Análise de Riscos mais utilizados pela indústria atual.

MÉTODO
Análise Preliminar de Risco (APR) (GUENAB; BOULANGER; SCHON, 2008).
Failure Mode and Effect Analysis (FMEA) (LONG et al., 2017).
WHAT-IF (KE et al., 2017).
Hazard and Operability Study (HAZOP) (MACDONALD, 2004).

O método de análise selecionado para o desenvolvimento da ferramenta foi o Estudo de Perigos e Operabilidade (HAZOP), pelo fato de sua grande utilização dentro da construção de segurança de processos no Brasil.

2.2.1 Hazard and Operability Study (HAZOP)

Segundo Macdonald (2004) uma das abordagens mais conhecidas do tipo HAZARD AND RISK, perigo e risco, é o Estudo de Riscos e Operabilidade (HAZOP), uma análise de um processo ou operação bem definida. Através de tal estudo os riscos inseridos no processo são identificados e avaliados.

A ideia da execução do HAZOP cita que as malhas de controle são constituídas por um grande número de elementos dificultando a análise de todas as variáveis ao mesmo tempo e indica que o sistema pode ser dividido em subsistemas que permitem o exame detalhado de cada elemento. Isto permite qualificar eminentes riscos e facilita a quantificação dos mesmos (MACDONALD, 2004).

Para o exame também os desvios devem ser considerados como elementos ou parâmetros. Os tipos mais comuns são listados na Tabela 2 a seguir.

Tabela 2. Desvios mais comuns usados na elaboração do HAZOP.

DESVIOS	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.

Usando uma série de questões o HAZOP faz uma investigação acerca do possível desvio. A Tabela 3 apresenta essas questões que devem ser respondidas para cada parâmetro.

Tabela 3. Questões usadas pelo HAZOP para cada parâmetro e desvio.

QUESTÕES	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.

2.3 Quantificação de Riscos

Após o levantamento de todos os riscos existentes no processo se faz necessário a quantificação dos mesmos. A quantificação de risco pode ser definida como o processo de atribuição de uma probabilidade ao acontecimento de um evento negativo. O risco é uma variável que deve ser entendida para se criar soluções econômicas afim de se minimizar a consequência negativa com impacto mínimo e custo de usabilidade. Geralmente é considerado como incerto, incompreendido e deve ser alterado com base em circunstâncias que podem levar a consequências indesejadas (WONGVISES et al., 2017). A quantificação dos riscos dá a direção de como determinar o posterior controle sobre o risco, a ação necessária para evitar que riscos se transformem em eventos. Alguns exemplos de quantificação de riscos são dados pela Tabela 4.

Tabela 4. Métodos de Quantificação de Risco mais usadas na atualidade.

MÉTODO
Matriz de Riscos (HAZARD MATRIX) (HEAL; PAGE, 1993)
Análise de Árvore de Falhas (ABDALLAH et al., 2017)

Para o desenvolvimento a Análise de Árvore de Falhas foi utilizada, por ser um método estatístico robusto, visual e de construção simplificada.

2.3.1 Análise de Árvore de Falhas

Análise de Árvore de Falhas (AAF) é uma descrição determinística da ocorrência de um evento. Uma árvore de falhas pode ser considerada como uma expressão de lógica booleana onde o evento superior é a falha de um sistema e os eventos básicos geralmente são uma falha dos componentes (UWE, 2002).

A árvore ou diagrama mostra a estrutura dos relacionamentos para encontrar causa e efeito. O nó raiz ou o evento superior é a ocorrência do evento interessante. Os eventos intermediários também são descritos até o melhor nível de detalhe onde os eventos básicos são alcançados. Normalmente, os eventos básicos são muitas vezes baseados em deficiência de dispositivos, ferramentas, sistema de segurança, presença de seres humanos e sistema de gerenciamento (WONGVISES et al., 2017). Os símbolos que geralmente são usados em um diagrama de árvore de falhas são descritos na Tabela 5.

Tabela 5. Símbolos da Análise de Árvore de Falhas.

SÍMBOLO	NOME	DESCRIÇÃO
	AND ou E.	O evento ocorrerá se, e somente se, todos os eventos mais baixos ocorrerem.
	OR ou OU.	O evento ocorrerá se um evento mais baixo ocorrer.
	Evento Básico.	Falha no nível mais baixo.
	Evento da Árvore de Falhas.	Evento Topo.
	Evento Externo.	Um evento que ocorre usualmente.

2.4 Nível de Integridade de Segurança (SIL)

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 IEC 61508 (2010) e IEC 61511 (2014) possuem os mesmos quatro níveis de integridade: SILs 1, 2, 3 e 4. Quanto maior o SIL, mais confiável ou eficiente é o sistema (GRUHN; CHEDDIE, 2006).

Para se determinar o nível de integridade desejado para um SIS, de acordo com IEC 61511 (2014), 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.

2.5 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 (BKOWSKI; GOBLE, 2017). 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 de que cada malha possui um SIL específico, o qual 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 arquitetura de uma SIF é decidida pela tolerância de falhas de seus componentes (*HARDWARE FAULT TOLERANCE - 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.

2.5 Relação entre SIS, SIF e SIL

A confiabilidade de um sistema é dada como a capacidade de executar sua função dentro dos limites e das condições de operação (GRUHN; CHEDDIE, 2006). É quantificada de acordo com o tempo médio entre as falhas que ocorrem no sistema. A disponibilidade mede a proporção de tempo em que o instrumento funciona sem falhas. A falha de probabilidade sob demanda (PFD) é um atributo de confiabilidade que indica a probabilidade de um componente não executar uma ação previamente especificada no momento da requisição. É o indicador apropriado para os sistemas de segurança. Já o Fator de Redução de Risco (RRF), matematicamente calculado como o inverso do PFD, expressa a magnitude da redução de risco que pode ser alcançada com a inserção de uma determinada função de segurança (GOBLE; CHEDDIE, 2005).

O Sistema de Instrumentado de Segurança (SIS) foi projetado com diferentes Níveis de Integridade de Segurança (SIL), de acordo com o risco no processo. O SIL é usado para medir a confiabilidade do SIS e é calculado através de uma Probabilidade de Falha a Pedido (PFD). A Tabela 6 apresenta a relação entre SIL, PFD e RRF.

Tabela 6. Relação entre SIL, PFD e RRF.

SIL	PFD	RRF
4	$\geq 10^{-5} < 10^{-4}$	>10000 ≤100000
3	$\geq 10^{-4} < 10^{-3}$	>1000 ≤10000
2	$\geq 10^{-3} < 10^{-2}$	>100 ≤1000
1	$\geq 10^{-2} < 10^{-1}$	>10 ≤100

Várias ações (ou funções) de proteção podem ser implementadas pelo SIS contra os vários riscos de um processo. Portanto, a função instrumentada de segurança (SIF) é uma função com um SIL específico, que é implementado pelo SIS. A relação entre SIF, SIL e SIS é mostrada na Figura 1. Cada SIS tem um (ou mais) SIF com um SIL específico.

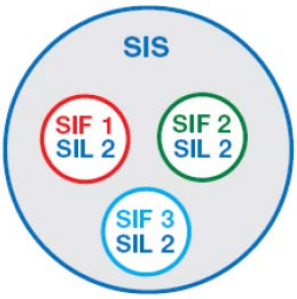

Figura 1. Relação SIS, SIF e SIL.

3 Desenvolvimento da Ferramenta

3.1 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. 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 2 mostra a divisão implementada e o fluxograma de funcionamento da ferramenta.

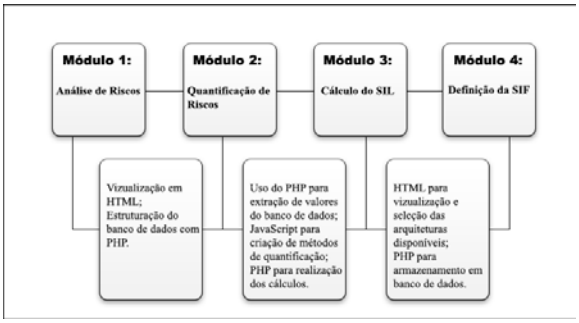

Figura 2. Fluxograma dos Módulos da Ferramenta.

Figura 3. SISTool: Tela Principal.

3.1.1 Módulos de Ferramenta

- *Módulo 1 – Análise de Riscos*: Este módulo usa as questões fornecidas por Oreda (2009), apresentadas pela Tabela 3. 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 estuda a necessidade do SIS.
- *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. 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.
- *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.
- *Módulo 4 – Definição da SIF:* Com um valor calculado do SIL, é possível escolher a votação de redundância para a definição de uma SIF consistente a ser implementada pelo SIS.

3.2 Descrição de Funcionamento da Ferramenta

O SISTool possui uma tela inicial na qual o usuário registrado pode acessar a interface usando qualquer navegador de Internet. Esta primeira tela dará acesso à tela principal que tem os links para os procedimentos normativos para análise de risco e cálculo de SIL, como mostrado na Figura 3.

Uma vez tendo acesso ao programa, o usuário deve iniciar um projeto. O SISTool tem um painel visual, que é dinâmico e fácil de entender, permitindo aos usuários a criação de novos projetos. Este passo é simples, mas importante na estruturação do banco de dados.

Cada projeto deve receber um NOME, se outros projetos tiverem os mesmos nomes, o programa usará o campo ÁREA como um diferenciador para posterior seleção do projeto. Se NOME e ÁREA possuírem as mesmas identificações em dois projetos distintos, então a DATA será usada como diferencial. Todos os projetos criados são disponibilizados na guia "Projetos salvos" e os usuários podem carregá-los e até mesmo excluí-los, se necessário.

Após a criação do projeto, o Módulo 1 implementa o estudo HAZOP, no qual deverão ser inseridos o parâmetro e o respectivo desvio, afim de se realizar o questionário com as perguntas, mostradas pela Tabela 3, permitindo que o projetista identifique toda a informação de possíveis erros e falhas inerentes ao processo salvando-os no banco de dados. No banco de dados, todas as informações relevantes para o projeto são inseridas, permitindo a edição a qualquer momento, como pode ser visto na Figura 4. O SISTool também gera um relatório de análise de risco para a parte do sistema que está sendo examinada. Este relatório de análise de risco é um requisito para a implantação do SIS.

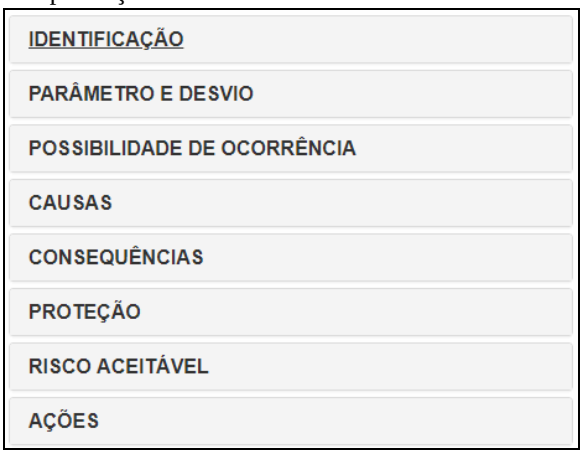

Figura 4. SISTool: Campos do HAZOP.

O próximo passo do SISTool está relacionado à execução do Módulo 2 da Análise de Árvore de Falhas (AAF). A AAF foi implementada em JavaScript

e estuda todas as possibilidades de ocorrência de um evento. Nesta etapa, a ferramenta é capaz de desenvolver uma árvore de falhas visual através de um diagrama com entradas, saídas e elementos lógicos. A Figura 5 apresenta um exemplo do desenvolvimento da árvore de falhas descrita

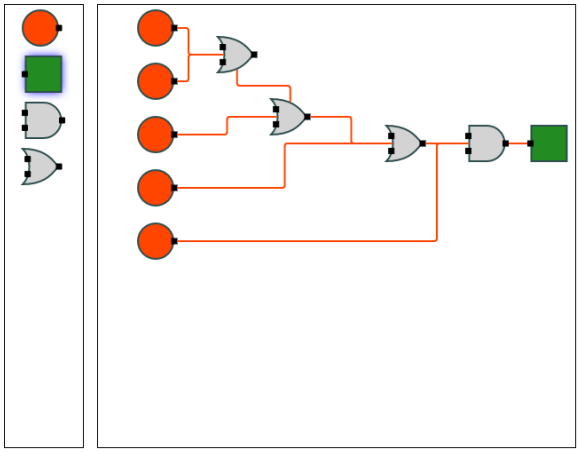

Figura 5. SISTool: Árvore de Falhas.

A terceira etapa do SISTool está relacionada com o Módulo 3 do Cálculo SIL. Esta etapa envolve o cálculo sistemático do fator de redução de risco (RRF) e a seleção do valor SIL apropriado para a parte do projeto em questão. Esses dois são apresentados na Figura 6.

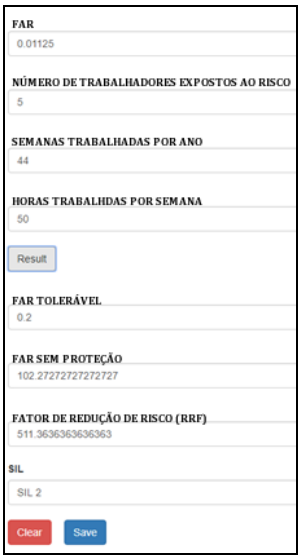

Figura 6. SISTool: Cálculo do SIL.

O último módulo, Módulo 4, usa dados armazenados, como o SIL calculado e o HFT dos equipamentos para a definição SIF. Neste módulo, a redundância necessária é selecionada para cada peça de equipamento em cada subsistema (sensor, lógico e elemento final).

4 Validação

4.1 Validação

Com a intenção de validar a ferramenta, foi selecionado um caso de um reator de uma indústria química, encontrado em Goble e Cheddie (2005). Os reatores são usados em plantas químicas para produzir uma grande variedade de produtos. A necessidade de um SIS foi identificada no sistema apresentado na Figura 7. É importante citar que um vídeo tutorial foi elaborado (https://youtu.be/jRf5msfsFDI) sobre esse estudo de caso para ilustrar o funcionamento completo da ferramenta.

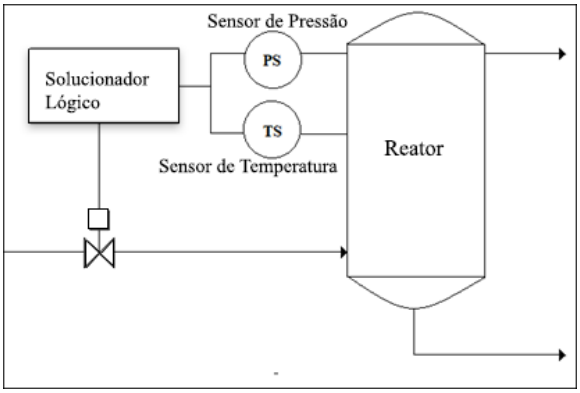

Figura 7. Sistema do Reator.

A análise de risco do reator indicou que tanto a alta temperatura como a alta pressão são uma indicação de um potencial risco que pode resultar em uma explosão. A Tabela 7 mostra a análise de risco desenvolvida pelos autores.

Tabela 7. Análise de Riscos do Reator.

INICIADORES	EVENTO PERIGOSO	SINAIS DE ENTRADA
Alta temperatura e / ou pressão no reator causada pelo bloqueio da linha de saída do reator.	Ruptura de casco causando a liberação de gás inflamável para atmosfera, resultando em explosão e danos ao equipamento.	PS e TS.

Na ferramenta, um novo projeto Reator é criado. A análise de risco é realizada pelo estudo HAZOP. Este estudo analisa as possíveis falhas por cada parâmetro e desvio. Portanto, a análise deve ser separada em Temperatura e Pressão. Os HAZOP de temperatura e pressão são apresentados na Tabela 8.

Tabela 8. HAZOP para Pressão e Temperatura no SISTool.

IDENTIFICAÇÃO	PARÂMETRO E DESVIO	OCORRÊNCIA
Parte: Reator; Local: Indústria Química; Elemento: Elementos dentro do reator; Efeito: Alta Temperatura.	Parâmetro: Temperatura; Desvio: Mais; Parâmetro: Pressão; Desvio: Mais.	Ocorrência: Sim.

Os autores encontraram para esse caso do reator um valor de SIL 2. Dessa maneira buscando o cálculo do SIL através da ferramenta, uma AAF foi elaborada. Os resultados podem ser vistos na Figura 8. A ferramenta SISTool apresentou o mesmo resultado para SIL se comparado com Goble e Cheddie (2005) para ambos os parâmetros.

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

SIL

Figura 8. SISTool: Resultado de FAR, RRF e SIL para temperatura e pressão.

Com relação a SIF, os autores utilizaram uma arquitetura 1oo2 para os sensores (Pressão e Temperatura) e 1oo1 para os subsistema lógico e elemento final. O SISTool oferece um construtor virtual para SIF que pode ser selecionado pelo usuário, oferecendo possibilidades de arquiteturas para cada equipamento envolvido. Desta maneira a mesma arquitetura foi selecionada para o reator, obtendo-se o resultado final mostrado na Figura 9.

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									

Figura 9. SISTool: Resultado Final com a Arquitetura.

Em comparação com o estudo de caso de Goble e Cheddie (2005), verificou-se que os parâmetros são divididos para serem analisados individualmente, portanto, o SISTool facilita a análise de risco e a construção da árvore de falhas. Quanto aos resultados da análise de risco e projeto do SIS, a ferramenta forneceu os mesmos em valores encontrados pelos autores.

5 Conclusões

Neste artigo, foi desenvolvida uma ferramenta, usando HTML, PHP e JavaScript, para analisar e projetar Sistemas Instrumentados de Segurança (SIS). Para o desenvolvimento do SISTool, foi necessário sistematizar uma metodologia de análise de risco, seleção do Nível de Integridade de Segurança (SIL) e da Função de Integridade de Segurança (SIF), definidas de acordo com normas de segurança. O procedimento utilizado foi dividido em quatro módulos com funcionalidades específicas e compatíveis com o desenvolvimento de um projeto SIS.

A ferramenta desenvolvida é inovadora e representa uma importante contribuição para esta área de estudo da automação, pois não foi encontrada qualquer ferramenta em literatura que incluísse todos os procedimentos necessários para analisar e projetar SIS. Fato que representa um diferencial da ferramenta proposta em relação a outras soluções disponíveis na literatura, pois automatiza e auxilia as fases de projeto de um SIS, principalmente reduzindo o tempo para executar essas tarefas. Outro fator crucial é que a ferramenta foi desenvolvida em um ambiente da Web, o que facilita seu uso e disseminação (sem necessidade de instalação de software ou gerenciamento de permissões de acesso).

Os resultados verificaram o desenvolvimento correto do SISTool, que foi validado usando dados de um estudo de caso do SIS. Os valores obtidos pela ferramenta para todos os índices, tais como a Taxa de Acidente Fatal (FAR), o Fator de Redução de Risco (RRF) e o Nível de Integridade de Segurança (SIL) foram os mesmos que os calculados na referência. Assim, observa-se a eficácia da ferramenta, bem como a automação e simplificação de um procedimento anteriormente manual.

Referências Bibliográficas

Abdallah, R., Kouta, R., Sarraf, C., Gaber, J. and Wack, M., 2017 "Fault tree analysis for the communication of a fleet formation flight of UAVs," 2017 2nd International Conference on System Reliability and Safety (ICSRS), Milan, 2017, pp. 202-206.

Bukowski, J. V. and Goble, W. M., 2017, "Properly crediting diagnostics in safety instrumented functions for high demand processes," 2017 Annual Reliability and Maintainability Symposium (RAMS), Orlando, FL, 2017, pp. 1-6.

Catelani, M., Ciani, L. and Luongo, V., 2012, "A new proposal for the analysis of safety instrumented systems," 2012 IEEE International

Instrumentation and Measurement Technology Conference Proceedings, Graz, 2012, pp. 1612-1616.

Catelani, M., Ciani, L. and Luongo, V., 2013, "Safety analysis in oil & gas industry in compliance with standards IEC61508 and IEC61511: Methods and applications," 2013 IEEE International Instrumentation and Measurement Technology Conference (I2MTC), Minneapolis, MN, 2013, pp. 686-690.

Cruz-Campa, J. and Cruz-Gomes, J., 2009, "Determine SIS and SIL using HAZOPs", Process Safety Progress, Vol 29, pp. 22-31, 2009.

Durocher, D. B. and Kay, L. A., 2017, "A journey toward electrical workplace safety and production reliability," 2017 IEEE-IAS/PCA Cement Industry Technical Conference, Calgary, AB, 2017, pp. 1-10.

Gabriel, A., 2017. Design and evaluation of safety instrumented systems: A simplified and enhanced approach. IEEE Access 5, 3813–3823.

Goble, W. and Cheddie, H., 2005, "Safety Instrumented Systems Verification – Pratical Probabilistic Calculations". 1st ed. 2005 Durham: ISA.

Gruhn, P. and Cheddie, H., 2006, "Safety Instrumented Systems: Design, Analysis and Justification". 2nd ed. 2006 Durham: ISA.

Guenab, F., Boulanger, J. L. and Schon, W., 2008, "Safety of railway control systems: A new Preliminary risk analysis approach," 2008 IEEE International Conference on Industrial Engineering and Engineering Management, Singapore, 2008, pp. 1309-1313.

Haddad, A. N., Morgado, C. V. and DeSouza, D. I., 2008, "Health, safety and environmental management risk evaluation strategy: Hazard Matrix application case studies," 2008 IEEE International Conference on Industrial Engineering and Engineering Management, Singapore, 2008, pp. 1314-1318.

Heal, B. W. and Page, R. M. R., 1993, "SIMD matrix methods for detecting hazards in logic circuits," in IEE Proceedings E - Computers and Digital Techniques, vol. 140, no. 4, pp. 201-204, Jul 1993.

Huang, J., Chen, G., and Li, D., 2012, "The SIS improvement in hydrogen furnace based on SIL," 2012 International Conference on Quality, Reliability, Risk, Maintenance, and Safety Engineering, Chengdu, 2012, pp. 1443-1447.

IEC 61508, 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-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, 2014.

Ke, J., Dong, H., Tan, C. and Liang, Y., 2017, "PBWA: A Provenance-Based What-If Analysis Approach for Data Mining Processes," in *Chinese Journal of Electronics*, vol. 26, no. 5, pp. 986-992, 9 2017.

Long, W., Yue, L., Yanling Q., Tengfei X. and Minhao, W., 2017 "A method of testability analysis and design based on FMEA extension," 2017 13th IEEE International Conference on Electronic Measurement & Instruments (ICEMI), Yangzhou, 2017, pp. 361-367.

MacDonald, D., 2004," Pratical Hazops, Trips and Alarms", Elsevier, Burlington.

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

Omeiri, H., Hamaidi, B., Innal, F., Chebila, M., Dutuit, Y., Oct 2017. Verification of dangerous and safe behaviors independence in safety instrumented systems. In: 2017 5th International Conference on Electrical Engineering - Boumerdes (ICEE-B). pp. 1–7.

Oreda Handobbok, 2009, "Offshore Reliability Data", 5th edition, 2009, Norway.

Squillante, R., dos Santos, D. J., Junqueira, F. , and Eigi, P., 2011, "Development of Control Systems for Safety Instrumented Systems," in IEEE Latin America Transactions, vol. 9, no. 4, pp. 451-457, July 2011.

Stix, G., 1989, "Bhopal: a tragedy in waiting," in IEEE Spectrum, vol. 26, no. 6, pp. 47-50, June 1989.

Uwe, J., 2002, "Probabilistic risk analysis: foundations and methods",(2002): 925-925.

Wongvises, C., Khurat, A., Fall, D. and Kashihara, S., 2017, "Fault tree analysis-based risk quantification of smart homes," 2017 2nd International Conference on Information Technology (INCIT), Nakhonpathom, 2017, pp. 1-6.