UNIVERSIDADE FEDERAL DE SANTA CATARINA
CENTRO TECNOLÓGICO
DEPARTAMENTO DE AUTOMAÇÃO E SISTEMAS

Helio Nonose

Projeto do Sistema Instrumentado de Segurança para a Unidade de Experimentação de Escoamento Multifásico da UFSC baseado nas técnicas HAZOP e LOPA

Florianópolis
2017

Helio Nonose

Projeto do Sistema Instrumentado de Segurança para a Unidade de Experimentação de Escoamento Multifásico da UFSC baseado nas técnicas HAZOP e LOPA

Relatório submetido à Universidade Federal de Santa Catarina como requisito para a aprovação na disciplina **DAS 5511: Projeto de Fim de Curso** do curso de Graduação em Engenharia de Controle e Automação.
Orientador: Prof. Max Hering de Queiroz
Co-orientador: Guilhermo Keiji Saito

Florianópolis
2017

Helio Nonose

Projeto do Sistema Instrumentado de Segurança para a Unidade de Experimentação de Escoamento Multifásico da UFSC baseado nas técnicas HAZOP e LOPA

Esta monografia foi julgada no contexto da disciplina DAS5511: Projeto de Fim de Curso e aprovada na sua forma final pelo Curso de Engenharia de Controle e Automação.

Florianópolis, 03 de Agosto de 2017

Banca Examinadora:

Prof. Max Hering de Queiroz
Orientador na Empresa
UFSC

Prof. Max Hering de Queiroz
Orientador no Curso
Universidade Federal de Santa Catarina

Prof. Daniel Juan Pagano
Universidade Federal de Santa Catarina

Rafael Vendramini Savi
Universidade Federal de Santa Catarina

Vinicius Kiatkoski Neves
Universidade Federal de Santa Catarina

À aqueles que utilizam a engenharia para proteger o que é importante

AGRADECIMENTOS

Gostaria de agradecer ao Prof. Max pela oportunidade em fazer parte deste projeto. À procura de um local para realizar o meu PFC, recebi o voto de confiança do professor. Esta foi a segunda vez em que ele me ajudou em um momento bastante significativo da minha vida acadêmica.

Agradeço ao meu co-orientador Guilhermo Saito, que me acompanhou e orientou durante todas as atividades do projeto. Não teria conseguido completar este trabalho sem sua ajuda. Também agradeço aos colegas Hallan e Thales pela companhia e troca de conhecimentos. O convívio com essas pessoas enriqueceu a minha experiência não apenas no âmbito profissional mas também pessoal.

Meus agradecimentos ao meu pai, minha irmã, minhas primas/irmãs, tios e tias. Poder completar meus estudos na UFSC foi devido ao apoio incondicional recebido deles. Também agradeço aos meus parentes mais próximos que sempre me apoiaram e incentivaram o meu progresso.

Agradeço aos amigos do Shimadaiko, do Floripa Ichiban e da Associação Nipo-Catarinense que me ajudaram a manter o stress a níveis toleráveis. Estar em contato com a cultura japonesa me ajudou muito neste processo. Em especial, gostaria de agradecer ao Marcelo, ao Leonardo e ao Guilherme. Pessoas estas que eu tenho o prazer de chamar de melhores amigos.

Não posso deixar de agradecer à dois grupos japoneses. Um deles por me ensinar sobre o que é qualidade de música. Após ouvir mais de 5296 vezes, suas letras e melodias continuam me inspirando até os dias de hoje. Do segundo grupo recebi uma influência tão grande que seria difícil descrever em poucas palavras. Aprendi a confiar mais em mim mesmo, nunca esquecer meu “espírito de iniciante”, entre outras 48 coisas mais. Ambos me acompanharam diariamente em minhas jornadas de trabalho em laboratório e madrugada adentro.

RESUMO

Indústrias do setor de óleo e gás, químico, aeronáutico, militar, entre outros, trabalham constantemente com sistemas críticos. Estes são sistemas que apresentam alto risco inerente e que, portanto, necessitam de um alto grau de confiabilidade. A automação tem atuado de forma direta e imprescindível para o controle e aumento da segurança destes sistemas. Reconhece-se que é praticamente impossível alcançar níveis de zero risco. Porém, faz-se necessário um controle de riscos sistemático para a prevenção e mitigação de acidentes. O objetivo deste trabalho foi projetar um Sistema Instrumentado de Segurança (SIS) para a Unidade de Experimentação de Escoamento Multifásico (UEEM) localizada no Departamento de Automação e Sistemas (DAS) da Universidade Federal de Santa Catarina (UFSC). Para tanto, realizou-se o estudo de padrões e normas nacionais e internacionais sobre ciclo de projeto de segurança e práticas recomendadas com foco nas indústrias de óleo e gás. Aplicou-se a técnica HAZOP para a análise de riscos e a técnica LOPA para a análise de camadas de proteção e avaliação de riscos da UEEM. Baseando-se nos resultados das análises, criou-se a especificação do SIS e dos procedimentos de operação e manutenção seguindo critérios de projeto baseados em normas para unidades industriais da Petrobrás.

Palavras-chave: sistemas instrumentados de segurança. ciclo de projeto. análise de risco. hazop. lopa.

ABSTRACT

Oil and gas, chemical, aerospace, military, among other industries frequently work with critical systems. These systems hold high intrinsic risk and, thus, require high reliability. Automation engineering has worked actively to control and increase safe operation on these systems. Though it might be virtually impossible to lower risks to zero, it is necessary to have a systematic risk management for accidents' prevention and mitigation. This work objective was to develop safety requirement's specification and design a Safety Instrumented System (SIS) for the Multiphase Flow Experimental Unity (UEEM) located on UFSC's System and Automation Department (DAS). To accomplish this, national and international safety lifecycle design standards were studied and recommended practices for safety systems on oil and gas industries were followed. Hazard and Operability Studies (HAZOP) and Layer of Protection Analysis (LOPA) applied on the UEEM for risk assessment. Based on these results, SIS's specification and operability and maintenance procedures followed Petrobras' standards for industrial facilities.

Keywords: Safety Instrumented Systems. Design Lifecycle. Risk Analysis. HAZOP. LOPA

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

UFSC - Universidade Federal de Santa Catarina

DAS – Departamento de Automação e Sistemas

HAZOP – *Hazard and Operability Study*

LOPA – *Layer of Protection Analysis*

HSE – *Health and Safety Executive*

LEEM – Laboratório Experimental de Escoamento Multifásico

UEEM – Unidade de Experimentação de Escoamento Multifásico

LCA – Laboratório de Controle e Automação

ANSI – *American National Standards Institute*

ISA – *International Studies Association*

IEC – *International Electrotechnical Commission*

API – *American Petroleum Institute*

AIChE – *American Institute of Chemical Engineers*

CCPS – *Center for Chemical Process Safety*

P&ID – *Piping and Instrumentation Diagram*

IHM – Interface Homem Máquina

PSV – *Pressure safety valve*

OREDA – *Offshore & Onshore Reliability Data*

SIS – *Safety Instrumented System*

SIF – *Safety Instrumented Function*

IPL – *Independent Protection Layer*

PFD – *Probability of Failure on Demand*

RRF – *Risk Reduction Factor*

SIL – *Safety Integrity Level*

MTTFS – *Mean Time to Fail Safe*

MTBF – *Mean Time between Failures*

1oo1 – 1 *out of* 1

SSC – Sistema de Supervisão e Controle

LISTA DE SÍMBOLOS

PFD_{avg} – Probabilidade média de falha na demanda

mA – miliampère

bar – unidade de pressão

psi – *pounds per square inch* (libra força por polegada quadrada)

m^3 – metros cúbicos

m^3/h – metros cúbicos por hora

SUMÁRIO

1. INTRODUÇÃO

1.1. Motivação e Justificativa

A área de engenharia de segurança se encontra em diversos ramos da indústria devido à existência de processos críticos ou de alto grau de complexidade que trazem consigo considerável nível de risco intrínseco. A automação tem atuado de forma direta e imprescindível para o controle e aumento da segurança destes sistemas.

No entanto, a história mostra diversos casos de acidentes e, infelizmente, de muitos casos de tragédia com grandes perdas patrimoniais, ambientais e de vidas humanas. O Departamento de Segurança e Saúde da Inglaterra (HSE) publicou um estudo onde analisou acidentes causados diretamente por falhas de controle e de segurança. Foi constatado que 44% ocorreram por má ou insuficiente especificação de projeto [7]. Com o intuito de evitar tais cenários, há anos, órgãos internacionais e de diversos países buscam a criação e aperfeiçoamento de normas para a indústria.

Durante os anos, observou-se a necessidade de uma forma metódica para a identificação de riscos associados a processos e atividades. Diversas técnicas de análise e avaliação de riscos foram estudadas e desenvolvidas, podendo-se citar como exemplo o *Hazard and Operability Study* (HAZOP) e o *Layer of Protection Analysis* (LOPA), como algumas das mais difundidas na indústria.

A segurança dos operadores, a integridade da planta ou a conservação do meio ambiente são facilmente apontados como prioridade em qualquer empresa. No entanto, a mesma facilidade não existe para apontar quais ações devem ser ou são tomadas para garantir tais condições de segurança. Há diversos cenários que podem trazer perigo e também há múltiplas maneiras de tentar prevenir ou mitigar suas consequências. Reconhece-se que é praticamente impossível alcançar níveis de zero risco. Porém, não se pode aguardar a ocorrência de um desastre para adotar as devidas providências. É necessário um controle de riscos sistemático para a prevenção e mitigação de acidentes.

Sistemas Instrumentados de Segurança (SIS) são projetados para reagir às condições perigosas de um sistema ou que, se nenhuma ação for tomada, possam levar à um evento danoso. Existem padrões para o projeto de um SIS porém esta é uma tarefa nada trivial. As normas são relacionadas à performance do sistema mas

não exatamente como ele deve ser projetado, implementado e operado. Por este motivo, é necessário um cuidado extra em todas as etapas do projeto, documentação e com o envolvimento das pessoas ligadas ao processo em questão.

Os SIS são fundamentais para indústrias como a de petróleo e gás, que trabalham com riscos extremamente elevados. Seus processos exigem constante e refinado controle, além do mais, instalações *offshore* devem contar com um altíssimo grau de automatização e confiabilidade. “Acidentes são, geralmente, uma combinação de eventos raros que foram julgados independentes e que não ocorreriam simultaneamente” [7]. Quando equipamentos, procedimentos e intervenção humana falham, o SIS age como a última barreira para tentar evitar um cenário acidental.

O presente trabalho encontra-se ligado ao contexto de um projeto de parceria do Departamento de Automação e Sistemas (DAS) da Universidade Federal de Santa Catarina (UFSC) com a Petrobrás. Por esse motivo, opta-se por seguir normas e recomendações de estudo e projeto desta empresa, referência mundial na área de petróleo e gás.

1.2. Objetivos

O objetivo do presente trabalho é projetar um Sistema Instrumentado de Segurança (SIS) para a Unidade de Experimentação de Escoamento Multifásico (UEEM), localizada no DAS/UFSC, seguindo padrões e normas de ciclo de projeto de segurança e práticas recomendadas com foco nas indústrias de óleo e gás. Pretende-se realizar uma análise de riscos na unidade utilizando a técnica HAZOP e uma análise de camadas de proteção e avaliação de riscos através da técnica LOPA. Baseando-se nos resultados das análises, propõe-se especificar o SIS e procedimentos de operação e manutenção seguindo critérios de projeto detalhados em normas para unidades industriais da Petrobrás.

Conhecimentos obtidos na disciplina de Aspectos de Segurança em Sistemas de Controle e Automação são utilizados como ponto de partida para as análises e avaliações de riscos. Para o estudo da UEEM, conceitos de sistemas de controle, redes industrias e acionamentos elétricos servem de apoio à compreensão do processo. Já o conteúdo que compreende a disciplina de Instrumentação em Controle encontra-se presente em todas as etapas do projeto.

1.3. Organização do Documento

Após o capítulo de introdução, segue a apresentação do tema Sistemas Instrumentados de Segurança. Neste capítulo são expostos conceitos básicos necessários para o entendimento de parâmetros utilizados para projeto, comentários sobre padrões e normas seguidas e a metodologia das técnicas LOPA e HAZOP. No capítulo 3 introduz-se o LEEM e a UEEM, comentando sobre sua estrutura física, operação básica, assim como o contexto no qual o laboratório é utilizado. O capítulo 4 descreve como foi realizada a especificação do SIS, apresentando as considerações e justificando as decisões quando necessário. Devido ao alto volume de dados, e por seguirem um mesmo padrão, optou-se por apresentar apenas parcialmente os resultados do projeto. No capítulo 5, lista-se e comenta-se sobre os relatórios gerados e sobre a finalização da especificação do SIS. Finalmente, no capítulo 6 são apresentadas as conclusões e sugestões para trabalhos futuros.

2. SISTEMAS INSTRUMENTADOS DE SEGURANÇA

Sistemas instrumentados de segurança têm como objetivo principal detectar situações de potencial risco e levar o processo a um estado considerado seguro. Alguns exemplos comuns encontrados na indústria são sistemas de intertravamento, *Emergency Shutdown* (ESD) e sistemas de fogo e gás.

Neste capítulo apresentam-se alguns tópicos relacionados ao tema nos quais será baseado o projeto do SIS.

2.1. Conceitos básicos

2.1.1. Conceito do SIS

Apesar das diversas definições de “risco”, em geral, este é considerado como uma função de uma frequência de ocorrência e um grau de severidade. Logo, reduzir o risco implica em tentar minimizar um ou ambos os parâmetros citados.

Falhas irão ocorrer, porém é impossível prever exatamente quando acontecerão principalmente devido à sua distribuição aleatória de ocorrência. Recorre-se então a algumas técnicas de estatística para estimar uma probabilidade de falha do processo.

O SIS é um sistema físico como qualquer outro, logo, também é sujeito a falhas. A ideia é, então, projetar o SIS para que possua uma probabilidade de falha menor que a do processo. Para ilustrar, toma-se como exemplo uma planta que possui uma taxa de 1 falha por ano e um SIS com uma taxa de falha de 1 falha a cada 5 anos. Em termos de probabilidade, isto representa um cenário onde o SIS protege o processo 4 vezes e apenas na quinta vez não consegue evitar danos ou acidentes na planta.

Pode-se concluir que o SIS possui duas características principais. A primeira delas é em relação às funcionalidades, ou seja, às ações realizadas para impedir um cenário indesejável. E a outra se refere às características de integridade que se referem à probabilidade do SIS responder quando ele for solicitado. Isto é relacionado ao parâmetro chamado Probabilidade de Falha na Demanda (PFD), geralmente expresso pela unidade de ocorrências por ano. O inverso do PFD é chamado de Fator de Redução de Risco (RRF) e é definido para facilitar a leitura e compreensão da variável. O PFD e o RRF dão origem à um terceiro parâmetro chamado de *Safety Integrity Level* (SIL). Muitos sistemas e instrumentos se referem apenas ao seu SIL

para identificar seu caráter de segurança. A Tabela 1 mostra as relações entre os três parâmetros.

Tabela 1 - Relação entre PFD, RRF e SIL

RRF	PFD	SIL
10 a 100	10^{-1} a 10^{-2}	SIL 1
101 a 1000	10^{-2} a 10^{-3}	SIL 2
1001 a 10000	10^{-3} a 10^{-4}	SIL 3
10001 a 100000	10^{-4} a 10^{-5}	SIL 4

2.1.2. Modos de Falhas

Como visto na seção anterior, um fator importante são as falhas. No contexto de SIS, estas são divididas em 4 categorias diferentes:

- Falhas seguras (λ_S), são aquelas que ocorrem no SIS mas que não o impedem de atingir o estado seguro;
- Falhas perigosas (λ_D) são aquelas que ocorrem no SIS e que o fazem perder a capacidade de realizar sua função;
- Falhas detectáveis (λ_d) estão relacionadas ao auto diagnóstico do SIS para identificar problemas internos. Uma métrica para detecção é o chamado fator de cobertura ou cobertura de diagnóstico;
- Falhas não detectáveis (λ_u) são aquelas que o SIS não consegue reconhecer sem atuar de fato no dispositivo;

Ao analisar as categorias acima citadas, logo se percebe que uma falha perigosa e não detectável (λ_{Du}) é a situação que se deve tomar mais cuidado pois são nestes casos que o SIS não consegue realizar suas funções. Esta falha introduz um novo parâmetro chamado *Mean Time Before Failure* (MTBF) que pode ser expresso como sendo o inverso de λ_{Du} com certas condições atendidas [7].

Quando uma “falha segura” ocorre, isto pode fazer com que o SIS responda achando que houve uma demanda real. Esses casos são chamados de “*trips*

espúrios” ou “*trips* seguros”. Apesar do nome “seguro”, uma interrupção desse tipo pode causar prejuízos devido ao tempo parado de produção, eventual danos a equipamentos, entre outros. A ocorrência muito frequente de *trips* espúrios também pode levar o operador a confiar menos no SIS e utilizar artifícios de *bypass* indiscriminadamente, deixando a planta exposta a perigos. Por esse motivo, o parâmetro *Mean Time To Fail Safe* (MTTFS) muitas vezes também deve ser considerado.

2.1.3. Controle de Processo e SIS

O SIS se diferencia do controle de processos em diversos pontos. A dinâmica do processo exige constantemente uma resposta por parte de sua malha de controle. Diferentemente do SIS, que permanece dormente até que uma situação de risco demande uma resposta. Outro fator é a flexibilidade que o operador precisa ter para alterar parâmetros de controle, pontos de operação, entre outros. No caso do SIS, enquanto não houver mudanças estruturais na planta, não há motivos para modificar sua configuração. Para citar mais um exemplo, o controle de processo é considerado como a primeira camada de proteção pois mantém a operação dentro da faixa esperada. Já o SIS, pode ser considerado a última camada pois atua apenas quando todas as demais precauções falharem, inclusive a resposta do operador.

Como pode-se imaginar pelos exemplos citados acima, é recomendado que o SIS e o controle do processo sejam implementados separadamente. Numa análise breve, pode-se observar que manter uma segregação completa e uma diversificação de componentes possibilita minimizar a probabilidade de falhas simultâneas e de causa comum. No entanto, é necessário um investimento maior na quantidade e qualidade de equipamentos e no treinamento dos operadores com as diferentes tecnologias. Era de se esperar que indústrias e fornecedores buscassem um balanço entre as duas opções portanto, atualmente, existem dispositivos que embarcam o SIS e o controle do processo sob uma mesma interface porém são ditos separados internamente. Assim, passou-se então a responsabilidade pela escolha para as empresa e indústrias que utilizarão o equipamento.

2.1.4. Tecnologias para SIS

Equipamentos voltados para SIS passam por testes e são certificados por empresas especializadas. Através da certificação, dados de interesse para a segurança são levantados para aquele instrumento em particular. Geralmente isto inclui os modos de falha e cobertura de diagnóstico.

Como o SIL é uma medida de desempenho do sistema, não faz sentido atribuir este parâmetro a um dispositivo em particular. Instrumentos de campo com certificação SIL indicam que estes são capazes de alcançar os níveis de desempenho se as condições descritas em seu certificado forem atendidas.

Não há um padrão publicado oficialmente para redes de campo. A ANSI/ISA tem em aberto um grupo para a criação de tal padrão porém este é um processo lento e que vem se estendendo por diversos anos. Para preencher esta lacuna, diversas empresas globais uniram esforços para a criação da FOUNDATION *Fieldbus*. Esta iniciativa privada recebeu o apoio inclusive da própria ISA, que expressou que iria continuar a criação do padrão de rede baseado na FOUNDATION *Fieldbus*.

2.2. ANSI/ISA-84.00.01-2004 (IEC 61511 Mod)

Buscando criar um padrão para todos os tipos de indústria, a IEC publicou a versão final da 61511 em 2003. Seu objetivo inicial era criar uma base para cobrir a utilização de instrumentos de campo e sistemas lógicos na indústria e se inspirou num padrão da ISA que tinha como foco os controladores lógicos programáveis. Este padrão da ISA estava previsto para ser revisado a cada 5 anos para se adaptar às novas tecnologias. Porém, ao invés de revisar o padrão inteiro, a ANSI/ISA optou por unir forças com a IEC e adotar o 61511 praticamente inteiro.

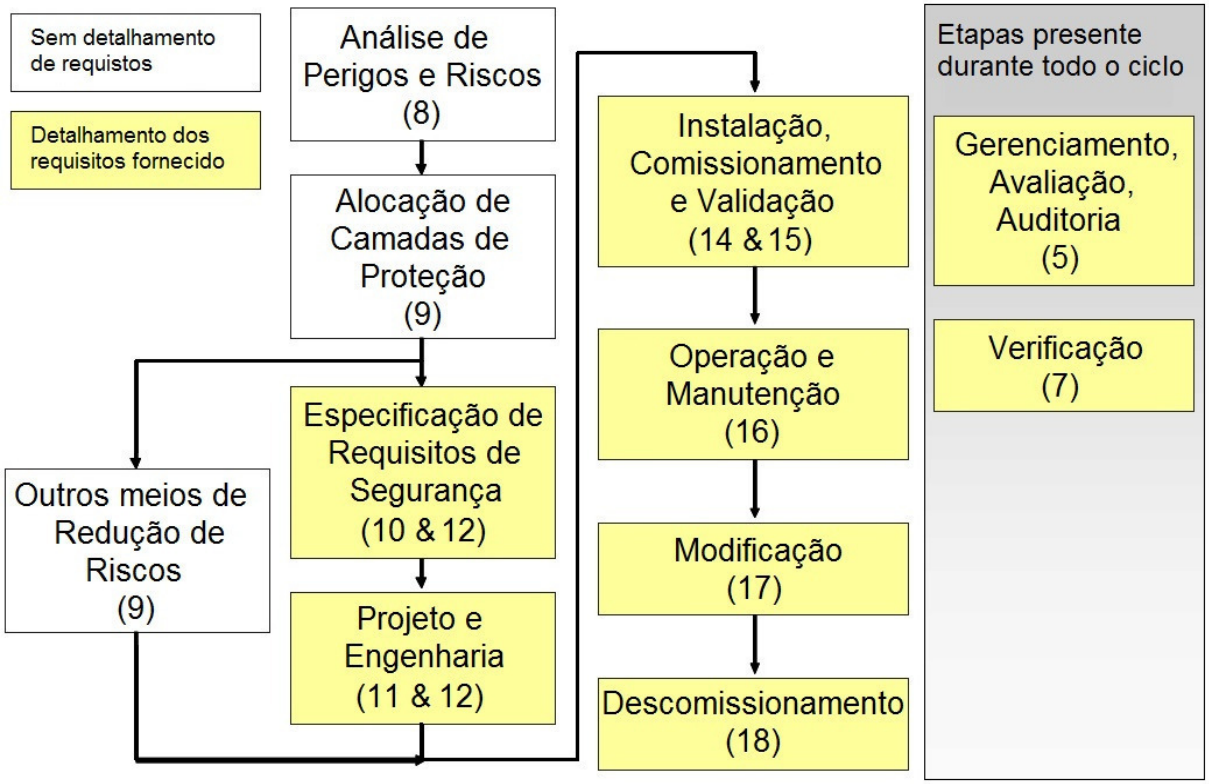
A 84.00.01 define requisitos para o projeto de um SIS através de um ciclo de vida de segurança. Para sistemas de relativo tamanho e complexidade, é necessário um processo metódico para evitar que detalhes importantes sejam esquecidos. Um exemplo de esquemático do ciclo proposto pode ser visto na Figura 1.

Primeiramente é preciso entender e identificar quais os riscos aos quais o processo está exposto. Em seguida, sugere-se que sejam analisadas maneiras de prevenir ou mitigar possíveis cenários indesejáveis, etapa esta chamada de alocação de camadas de segurança. Apenas após verificada a impossibilidade de proteger a

planta com outros dispositivos, inicia-se a especificação de Funções Instrumentadas de Segurança (SIFs) e seus requisitos. A partir de então, são detalhados os componentes que farão parte do SIS.

As etapas seguintes cobrem o fechamento do ciclo de projeto mas não fazem parte do escopo deste trabalho e, portanto, não serão apresentadas em detalhes.

Figura 1 - Ciclo de vida de projeto de SIS (com número das cláusulas da IEC 61511)



Fonte: *Safety Instrumented Systems* [7]

2.3. API RP 14C

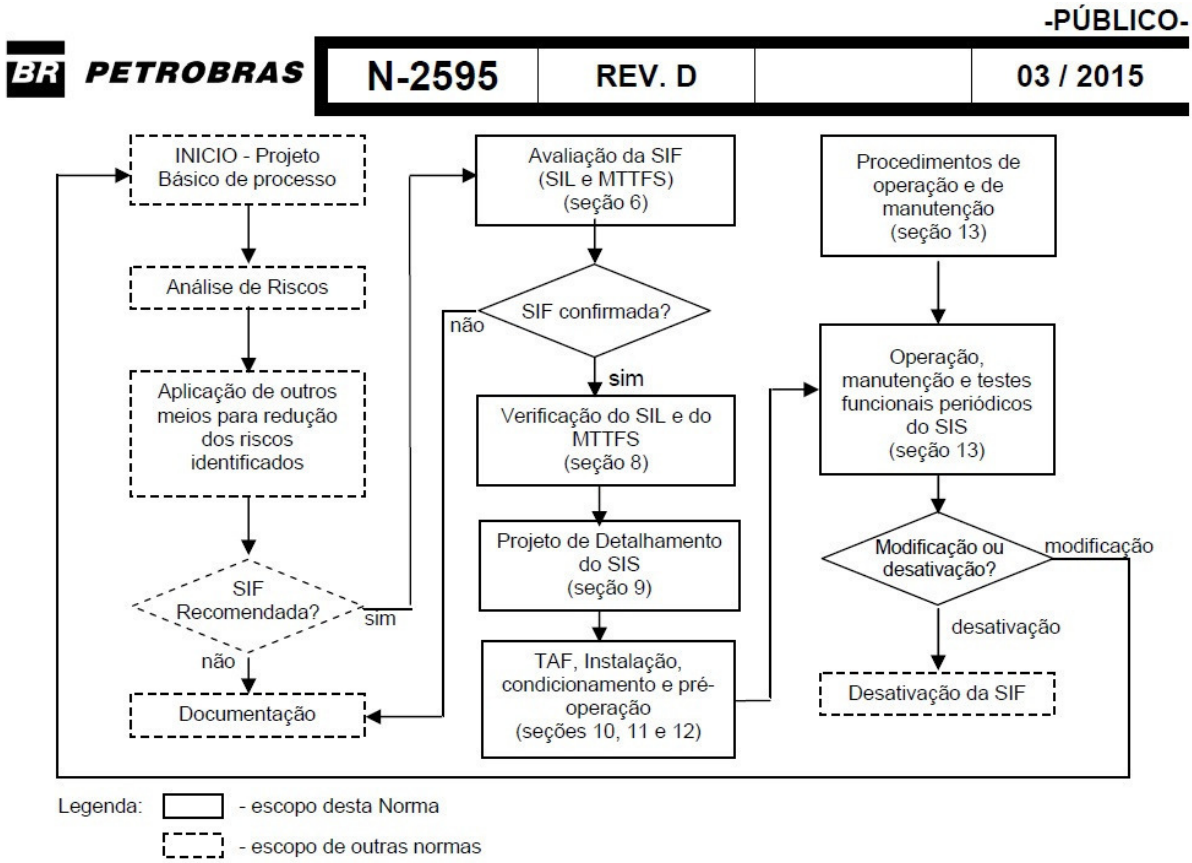
Este documento apresenta práticas recomendadas sobre projeto, instalação e testes de sistemas de segurança em plataformas offshore.

Nela, além da descrição de um padrão de identificação de componentes através de identidades alfanuméricas, é apresentada uma análise de sistemas e desvios encontrados comumente na indústria de óleo e gás. Também são citadas algumas recomendações de instrumentação e comentados outros conceitos de proteção e análise de segurança.

2.4. Petrobrás N-2595

A N-2595 é uma norma da Petrobrás de acesso público e se refere a critérios de projeto, operação e manutenção de SIS para unidades industriais. Esta norma contém, entre outras definições e recomendações, um modelo para o ciclo de vida de SIS, mostrado na Figura 2, baseado no padrão ANSI/ISA. A ideia geral do ciclo de projeto foi apresentada anteriormente, portanto serão comentados apenas os pontos específicos da N-2595.

Figura 2 - Modelo de Ciclo de Vida de um SIS



Fonte: Norma N-2595 [12]

Como pode ser observado pela figura, as etapas de análise de riscos e identificação de SIF não fazem parte do escopo desta norma porém algumas recomendações, como a utilização do HAZOP, são descritas em capítulo introdutório. Portanto, para começar a utilização desta norma, é necessário ter completado as etapas anteriores e possuir pelo menos uma lista preliminar de SIFs.

A alocação de camadas de proteção previsto pelo padrão ANSI/ISA é realizado durante a etapa de Avaliação das SIFs da N-2595. É recomendada a aplicação do método LOPA para a avaliação de camadas e obtenção de valores alvo de SIL e MTTFS. Mais detalhes sobre o LOPA são apresentados na seção seguinte.

A etapa de Verificação de SIL e MTTFS é responsável por encontrar uma arquitetura de SIF compatível com os parâmetros alvo. Isto é realizado através de cálculos de estimação de PFD para diferentes arquiteturas.

Durante o Projeto de Detalhamento são apresentados diversos requisitos para implementação de cada componentes do SIS. É apresentado e recomendada a utilização de um modelo de folha de especificação de SIF. Manter as principais características registradas e centralizadas em um documento facilita sua utilização. Nota-se que os instrumentos e elementos finais do SIS nem sempre se encontram instalados num mesmo local e, portanto, não são de identificação direta num *Piping and Instrumentation Diagram* (P&ID), por exemplo.

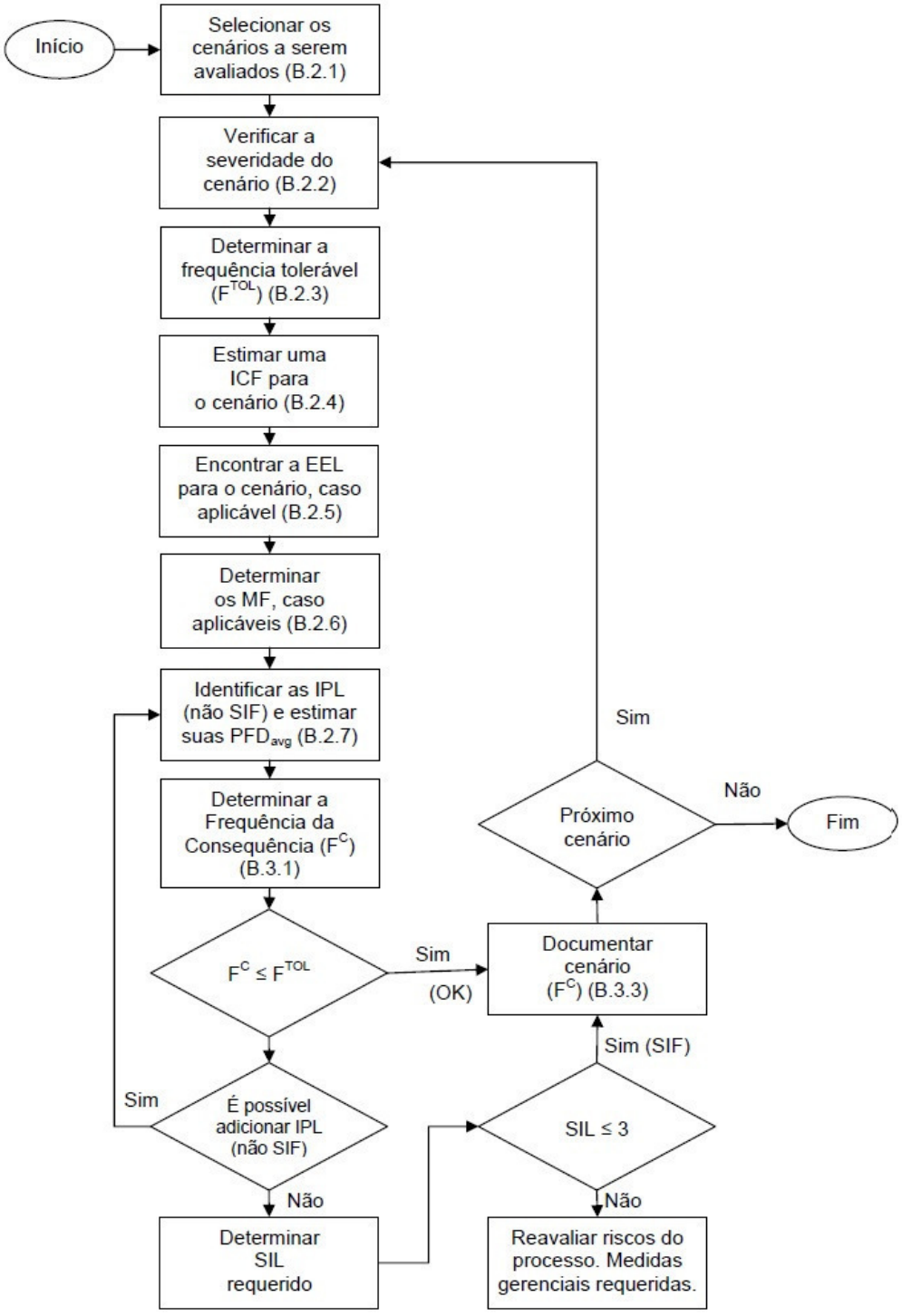
Outros detalhes de implementação também são bem detalhados. As etapas seguintes não foram contempladas no escopo do presente projeto porém, a adequação da documentação à norma facilita a continuação do ciclo de segurança para trabalhos futuros.

2.4.1. Método de Análise de Camadas de Proteção - LOPA

O LOPA é descrito no livro conceito "*Layer of Protection Analysis: Simplified Process Risk Assessment*", 2001 da AIChE/CCPS. Considerado um método semiquantitativo, o LOPA tem por objetivo avaliar se as medidas de proteção presentes são suficientes para reduzir o risco de um evento indesejável a níveis toleráveis. Isto é realizado comparando-se a frequência de ocorrência das possíveis causas iniciadoras com as probabilidades médias de falha na demanda (PFD_{avg}) de cada camada de proteção presente. Desta forma, obtém-se um valor para o risco residual e este é comparado com o valor tolerável para aquele cenário.

A metodologia sugerida pela N-2595 é representada pela Figura 3 e cada etapa é comentada em seguida.

Figura 3 - Fluxo de procedimento LOPA



Fonte: Norma N-2595 [12]

Os cenários a serem avaliados devem ser resultado de uma análise de riscos realizada previamente. A norma recomenda a utilização da técnica HAZOP.

Para a categorização de severidade, sugere-se a consulta da Matriz de Tolerabilidade de Riscos mostrada na Figura 4.

Figura 4 - Matriz de Tolerabilidade

Freqüência do cenário (por ano)							10^{-5}	10^{-4}	10^{-3}	10^{-2}	10^{-1}	1
			Descrição / características				A Extremamente remota	B Remota	C Pouco provável	D Possível	E Freqüente	
			Pessoas	Patrimônio / continuidade operacional	Meio ambiente (ver Nota 1)	Imagem	Conceitualmente possível, mas sem referências na indústria	Não esperado ocorrer, apesar de haver referências em instalações similares na indústria	Pouco provável de ocorrer durante a vida útil de um conjunto de unidades similares	Possível de ocorrer uma vez durante a vida útil da instalação	Possível de ocorrer muitas vezes durante a vida útil da instalação	
Categorias de Severidade das Consequências	V	Catastrófica	Múltiplas fatalidades intramuros ou fatalidade extramuros	Danos catastróficos podendo levar à perda da instalação industrial	Danos severos em áreas sensíveis ou se estendendo para outros locais	Impacto internacional	M	M	NT	NT	NT	
	IV	Crítica	Até 3 fatalidades intramuros ou lesões graves extramuros	Danos severos a sistemas (reparação lenta)	Danos severos com efeito localizado	Impacto nacional	T	M	M	NT	NT	
	III	Média	Lesões graves intramuros ou lesões leves extramuros	Danos moderados a sistemas	Danos moderados	Impacto regional	T	T	M	M	NT	
	II	Marginal	Lesões leves	Danos leves a sistemas / equipamentos	Danos leves	Impacto local	T	T	T	M	M	
	I	Desprezível	Sem lesões ou, no máximo, casos de primeiros socorros	Danos leves a equipamentos sem comprometimento da continuidade operacional	Danos insignificantes	Impacto insignificante	T	T	T	T	M	

Fonte: Diretriz de segurança da Petrobrás [11]

Um determinado cenário pode apresentar diferentes impactos dependendo de quem ou o que é afetado: Pessoas, Patrimônio ou Continuidade Operacional, Meio Ambiente e Imagem da empresa. O impacto sentido por cada um deles é classificado com um grau de severidade e o maior dentre os graus levantados é associado ao cenário em questão. Dependendo da classificação da severidade, uma Frequência Tolerável é associada a partir da Tabela 2.

Tabela 2 - Categoria de Severidade e Frequência Tolerável

Categoria de severidade	F^{TOL} (evento/ano)
V	$1x10^{-5}$
IV	$1x10^{-4}$
III	$1x10^{-3}$
II	$1x10^{-2}$
I	$1x10^{-1}$

Fonte: N-2595 [12]

A Causa Iniciadora corresponde ao motivo pelo qual ocorreu o desvio. Para a determinação de sua frequência (ICF), não deve ser considerada a existência de camadas de proteção ou qualquer outro fator. Esses valores podem ser extraídos de outras fontes além do histórico da planta, porém devem ser devidamente documentados e justificados. Falhas de equipamentos de segurança não são considerados como Causas Iniciadoras uma vez que outros eventos devem iniciar o cenário antes que estas possam receber uma demanda.

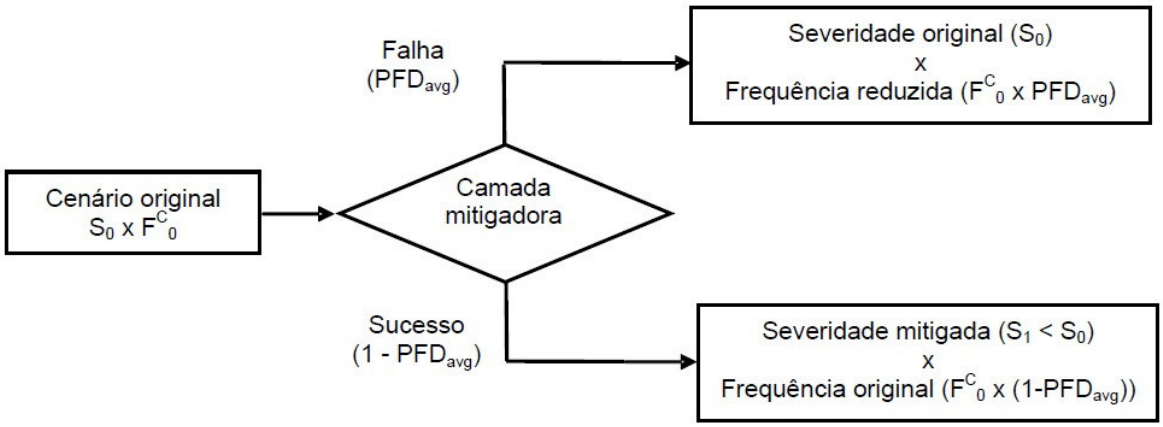
Condição Habilitadora (EE) é uma ação ou estado que não causa o cenário diretamente, mas que precisa existir para que a causa iniciadora gere a consequência considerada. O exemplo mais comum é o Tempo de Existência do Risco (*Time at Risk*) que considera que o perigo só existe em períodos específicos, como por exemplo, durante fases específicas do processo, como manutenção.

Fatores Modificadores (MF) também podem ser aplicados e consideram que existam certas condições específicas para que ocorra o dano, como por exemplo, a presença de pessoas ou fonte de ignição na área de perigo. Há diversos fatores que podem ser considerados e são detalhados na norma.

Estes dois últimos fatores são utilizados para ponderar o resultado da frequência da consequência. Porém, devem ser utilizados apenas quando seja possível garantir a veracidade de tais considerações durante toda o ciclo de vida do processo. Maiores detalhes sobre Condição Habilitadora e Fatores Modificadores, são descritos na N-2595.

Diversos requisitos devem ser atendidos porém uma das principais características de uma Camada de Proteção Independente (IPL) é que ela deva conseguir impedir a ocorrência do evento perigoso independentemente de outras condições ou salvaguardas. Casos especiais em que a IPL visa reduzir a severidade da consequência, seja limitando sua intensidade ou impedindo efeitos secundários são denominados de IPLs mitigadoras e seu esquemático é mostrado na Figura 5. Para maiores detalhes e para valores típicos de PFD_{avg}, deve-se consultar a N-2595.

Figura 5 - Camada de Proteção Mitigadora



Fonte: N-2595 [12]

A partir de todos os fatores apresentados nesta seção, pode-se estimar o valor para o Risco Residual através da fórmula:

$$F^c = ICF \times EEL \times \prod_i MF_i \times \prod_j IPL_j$$

Onde:

$F^c = Frequência\ da\ Consequência$

$ICF = Frequência\ da\ Causa\ Iniciadora$

$EEL = Probabilidade\ da\ Condição\ Habilitadora$

$MF_i = iésimo\ Fator\ Modificador$

$IPL_j = PFD_{avg}\ da\ jésima\ IPL\ (não\ SIF)\ associada$ à $Causa\ Iniciadora$

A partir deste resultado, julga-se a aceitação do risco, a possibilidade de alocação de outra camada de proteção ou da necessidade da implementação de uma SIF.

2.5. Método de Análise de Riscos – HAZOP

Hazard and Operability Study (HAZOP), também conhecido como Estudo de Perigos e Operabilidade, é uma técnica que tem por objetivo identificar possíveis desvios num sistema que possam evoluir para cenários considerados perigosos.

Uma equipe multidisciplinar é designada para realizar sessões de *brainstorm* e estudar o sistema de modo metódico. Este formato traz grandes vantagens pois explora de maneira sistemática o processo através de diversos pontos de vista. Devido a isso, a produtividade das reuniões depende diretamente da familiaridade de seus participantes com o método e com o processo em pauta. Questões relacionadas ao tempo máximo de reunião devido ao esgotamento da criatividade, entre outras características próprias de sessões de *brainstorm*, também devem ser consideradas. Em muitos casos, é até solicitado um consultor de empresa especializada para mediar as reuniões.

Antes de iniciar o estudo, é fundamental ter acesso à toda a documentação de interesse do sistema em seu formato mais atualizado. Realizar reuniões com informações desatualizadas pode ser pouco produtivo ou até mesmo perigoso do ponto de vista da utilização posterior da análise.

Outro parâmetro importante a ser definido são as palavras guia. Um exemplo é mostrado pela Figura 6. Sua utilização é o que permite a busca exaustiva por desvios no sistema.

Figura 6 - Palavras guia para o HAZOP

PARÂMETRO	PALAVRAS GUIAS			
Pressão	Maior	Menor		
Temperatura	Maior	Menor		
Fluxo	Maior	Menor	Nulo	Reverso
Contaminação				
Nível	Maior	Menor		
Nível de interface	Maior	Menor		

Fonte: Diretriz de segurança da Petrobrás [11]

Estas e outras informações podem ser levantadas antes das reuniões começarem de fato. Isto aumenta a produtividade e, inclusive, recomenda-se que os participantes realizem um estudo prévio da documentação disponível.

Para iniciar o estudo em si, identificam-se os “nós” do processo a partir de seu P&ID. Cada nó é estudado separadamente e pode ser composto por um grupo ou mesmo um único equipamento, dependendo da complexidade e da importância atribuída a ele. A escolha dos nós é livre e tem influência direta na quantidade de tabelas geradas. No entanto, o resultado final da análise deve ser independente.

Decidido quais serão os nós, investiga-se a possível ocorrência de parâmetro por parâmetro, com respectiva palavra guia, em cada equipamento à procura de desvios. É importante lembrar que o desvio é uma situação além do especificado. Um tanque pode assumir níveis maiores que o esperado devido a oscilações no processo, por exemplo. No entanto, deve ser considerado como desvio, por exemplo, os casos em que uma variável assume valores considerados fora da faixa segura de operação. Um mesmo desvio pode ter diversas causas, que devem ser anotadas e analisadas separadamente.

Identificado um desvio, investiga-se qual seria a consequência gerada. Geralmente, a consequência não leva em conta a ação de sistemas ou dispositivos de segurança. Desse modo, é possível contemplar o “pior caso” do respectivo cenário.

Outros parâmetros podem se analisados a critério da equipe, como por exemplo: salvaguardas, sugestões, observações, descrição do cenário, etc. Todas as informações são levantadas e anotadas em tabelas.

Este processo é repetido sistematicamente em cada nó e, como resultado, monta-se um relatório final contendo recomendações de quais providências devem ser tomadas (mudança no design do processo, instalação de válvulas de alívio, definição de regras ou procedimentos de segurança, etc.).

Antes e durante o estudo, pode ser necessário fazer considerações a respeito do processo, de resposta do operador, de condições ambientais ou financeiras, entre outras. Estas considerações devem ser anotadas e incluídas no relatório final pois são fundamentais para descrever o contexto em que foi realizado o HAZOP. Esta documentação é de grande importância para contribuir para a auditabilidade e deve ser lembrado que, geralmente, não cabe ao grupo que realizou o HAZOP a implementação das recomendações, mas sim a cada departamento ou grupo da área na qual é responsável.

2.6. Conclusão do Capítulo

O projeto do SIS é um processo longo e envolve diversas áreas diferentes. Mesmo em um processo de média complexidade, isto se mostra nada trivial devido à necessidade de trabalhar com conceitos de probabilidade, análise de riscos, instrumentação, controle de processo, assim como outros introduzidos pelo tema.

Observa-se, então, a importância em ser adotada uma metodologia para evitar a possibilidade de falhas durante a fase de especificação. Dentro do ciclo de projeto, nem o padrão nem a norma são restritivos com relação ao método de análise de riscos. Porém, observa-se uma afinidade entre o HAZOP e o LOPA e compreende-se o porquê de sua recomendação de uso.

Normas e padrões possuem uma característica de ser orientadas à performance, ou seja, descrevem quão bem um sistema deve responder. Por um lado, isso permite que cada indústria aplique implementações otimizadas para o seu setor. Por outro, essa flexibilidade pode levantar dúvidas e confusão devido à grande gama de possibilidades, estratégias e tecnologias disponíveis no mercado

Nesse sentido, desenvolver e manter uma cultura interna e registrar o histórico da planta são práticas recomendadas para obter uma maior precisão em dados e padronização de equipamentos e procedimentos. Estes fatores influenciam e podem melhorar a performance do SIS e facilitar o gerenciamento de riscos do processo.

3. O LABORATÓRIO LEEM

O Laboratório Experimental de Escoamento Multifásico (LEEM) localiza-se no campus Trindade da UFSC, fazendo parte do Departamento de Automação e Sistemas (DAS). Seu objetivo principal, como indica seu nome, é realizar experimentos com escoamentos multifásicos. O laboratório possui duas instalações distintas, como mostra a Figura 7. Uma delas é a sala de medições, localizada junto ao Laboratório de Controle e Automação (LCA), e a outra é a casa de utilidades, localizada ao lado do prédio do DAS.

Figura 7 - Instalações físicas do LEEM

Fonte: Fotos de arquivo pessoal e figura extraída de [1]

Diversos estudos já foram realizados neste laboratório. Para citar alguns, em 2015, Mônica Aparecida Dias realizou o projeto e a implementação da automatização do sistema de controle local e supervisório utilizando a tecnologia FOUNDATION *Fieldbus* e também o projeto de um sistema de intertravamento e de segurança [5]. Em 2011, Shana Geyger Boff apresentou estudos com relação à operação da planta e uma implementação de sistema instrumentado de segurança [3]. Em 2009, Cleiton Moya de Almeida realizou o projeto básico e detalhado dos equipamentos e instrumentos da UEEM [1].

3.1. A UEEM

O LEEM é equipado com uma Unidade de Experimentação de Escoamento Multifásico (UEEM) capaz de simular diferentes perfis de escoamentos através da combinação entre água, óleo e ar.

Figura 8 - P&ID da UEEM

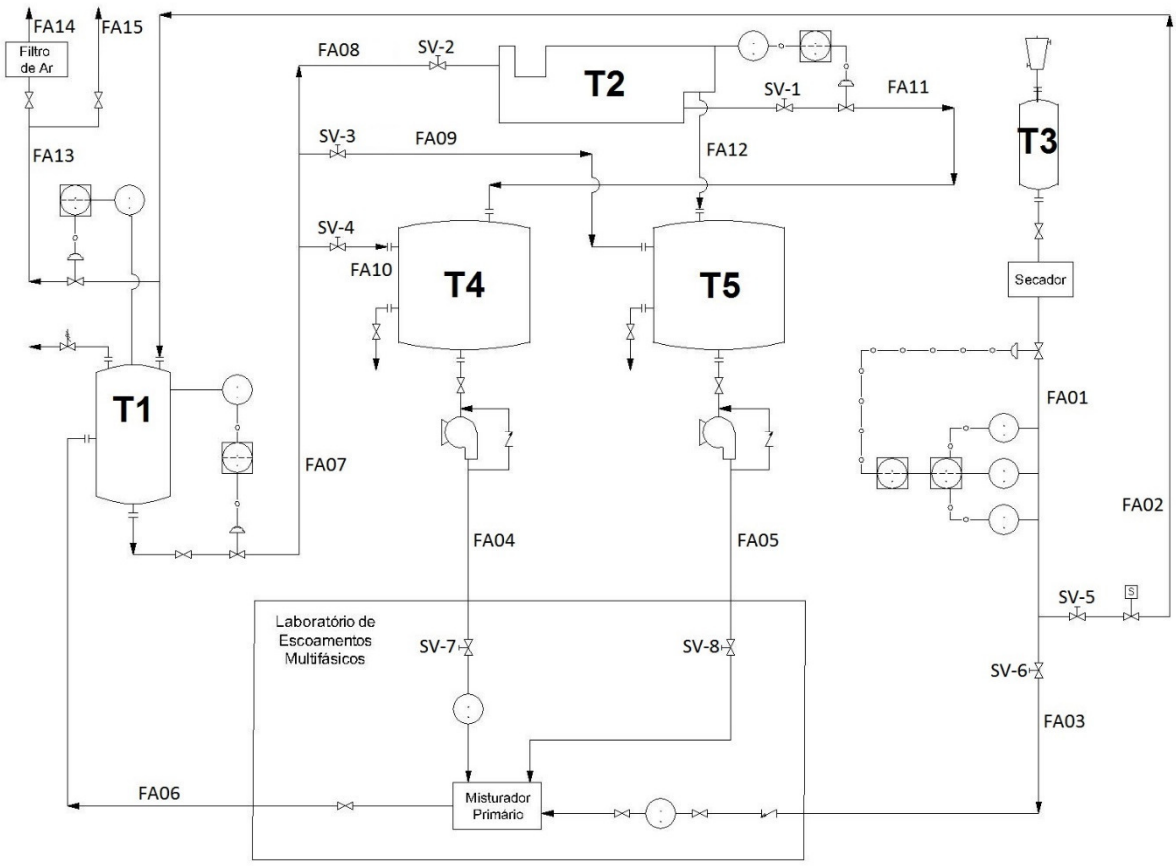
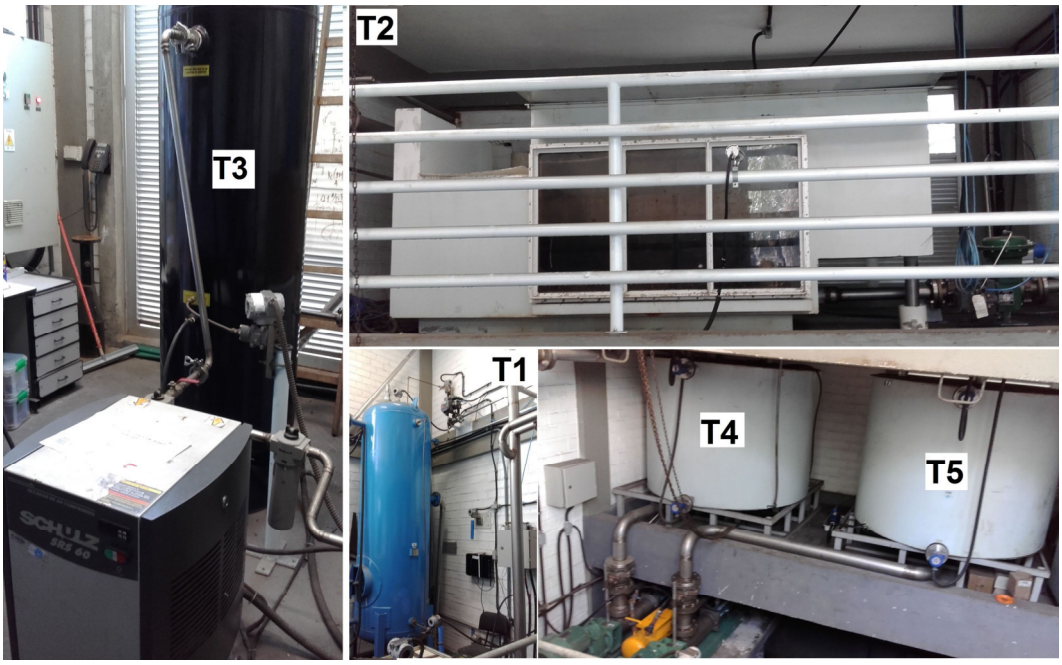


Figura 9 - Tanques e equipamentos da casa de utilidades da UEEM



Fonte: Arquivo pessoal

Figura 10 - Sala de medições da UEEM com um destaque para instrumentos e válvulas

Fonte: Arquivo pessoal

O diagrama P&ID do processo inteiro é mostrado na Figura 8. Fotos dos equipamentos da casa de utilidades e da sala de medições são mostrados nas Figuras 9 e 10, respectivamente.

Linhas individuais direcionam cada fluido para o misturador primário localizado na sala de medições. Uma vez misturados, os fluidos seguem para o tanque de pressão (T1), localizado na casa de utilidades. Este tanque tem por objetivo separar o ar comprimido, enviar os líquidos para o tanque de separação (T2) sem o auxílio de uma bomba extra e também rejeitar perturbações no fluxo de entrada de T2. Por sua vez, o tanque de separação tem por objetivo separar o óleo e a água através da gravidade e do auxílio de placas coalescedoras [1]. A partir deste ponto, cada fluido retorna para seu respectivo tanque de armazenamento e o ciclo é fechado. O funcionamento específico de cada subsistema do processo é descrito nos trabalhos da Mônica e do Cleiton.

A Tabela 3 descreve os equipamentos da UEEM e algumas de suas características:

Tabela 3 - Equipamentos da UEEM e suas características

Tanques	**Capacidade (m^3)**	**Pressão de Trabalho**
T1	1,5	6,71 bar (máximo)
T2	2,152	Atmosférica
T3	(sem dados)	17 bar (máximo)
T4 / T5	2,412	Atmosférica
Linhas	**Diâmetro (polegadas)**	**Comprimento (metros)**
Ar	1	15
Água	2	15
Óleo	3	15
Retorno do LCA	3,5	30
Saída T1	4	7
Saída T2	3,5	4

O projeto original contempla alguns pontos de operação nominais que são os mostrados na Tabela 4.

Tabela 4 - Valores nominais de operação

Vazão máxima de trabalho	15 m^3/h
Altura Nível em T1	50%
Pressão em T1	20 psi (1,38 bar)
Altura do Nível de Interface em T2	60%

A UEEM conta com malhas de controle para pressão em T1, nível em T1 e nível de interface em T2. Também há instrumentação para uma malha para o fornecimento de ar comprimido através de T3, porém atualmente não se encontra ativo. O controle e o sistema supervisório operam através da rede FOUNDATION *Fieldbus*.

É possível trabalhar com diferentes tipos de escoamento na UEEM realizando a combinação entre água, óleo e ar. Para a mudança do modo de operação, é necessário configurar 8 válvulas (SV-1 a SV-8) presentes nas linhas da planta [5].

Atualmente, esta seleção é realizada manualmente porém este projeto de SIS já comtempla a automatização destas válvulas. Para maiores detalhes sobre as posições das válvulas e os modos de operação, deve-se consultar o trabalho da Mônica [5].

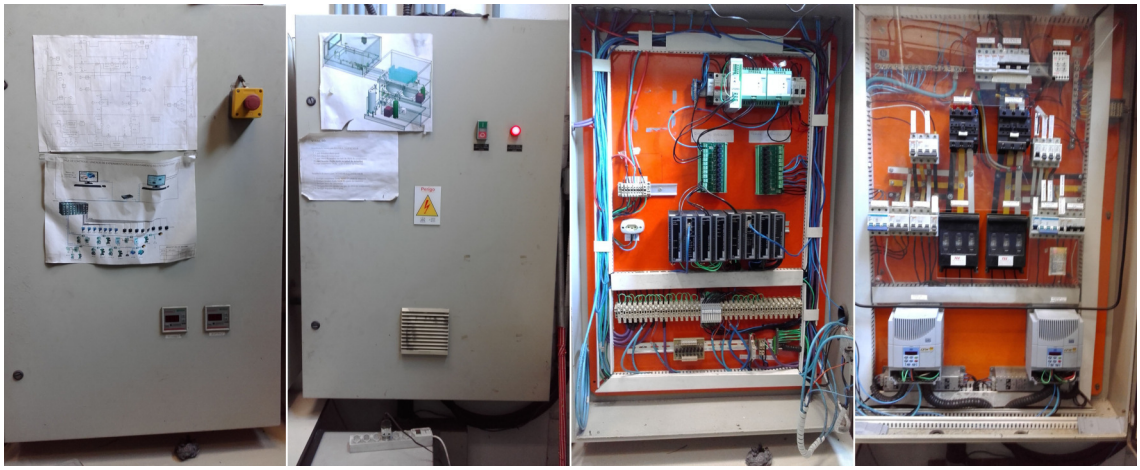
A unidade foi projetada para ser auto suficiente com relação aos fluidos de trabalho. Ou seja, não é previsto nenhum reabastecimento dos tanques de armazenamento após a inicialização do processo. Com base no trabalho da Shana [3], o volume de fluido que circula na planta em escoamentos trifásicos é mostrado na Tabela 5.

Tabela 5 - Volume total de fluido para escoamentos trifásicos [3]

Fluido	Volume total (m^3)
Água	2,0646
Óleo	1,7448

Logo na entrada do LEEM, existem 2 quadros gerais de energia, mostrados na Figura 10, onde estão instalados os módulos do controlador, circuitos de alimentação e comunicação e os inversores das bombas. Nota-se também a presença de circuitos de equipamentos de outros processos.

Figura 11 - Quadros de energia do LEEM mostrados fechados (à esq.) e abertos (à dir.)



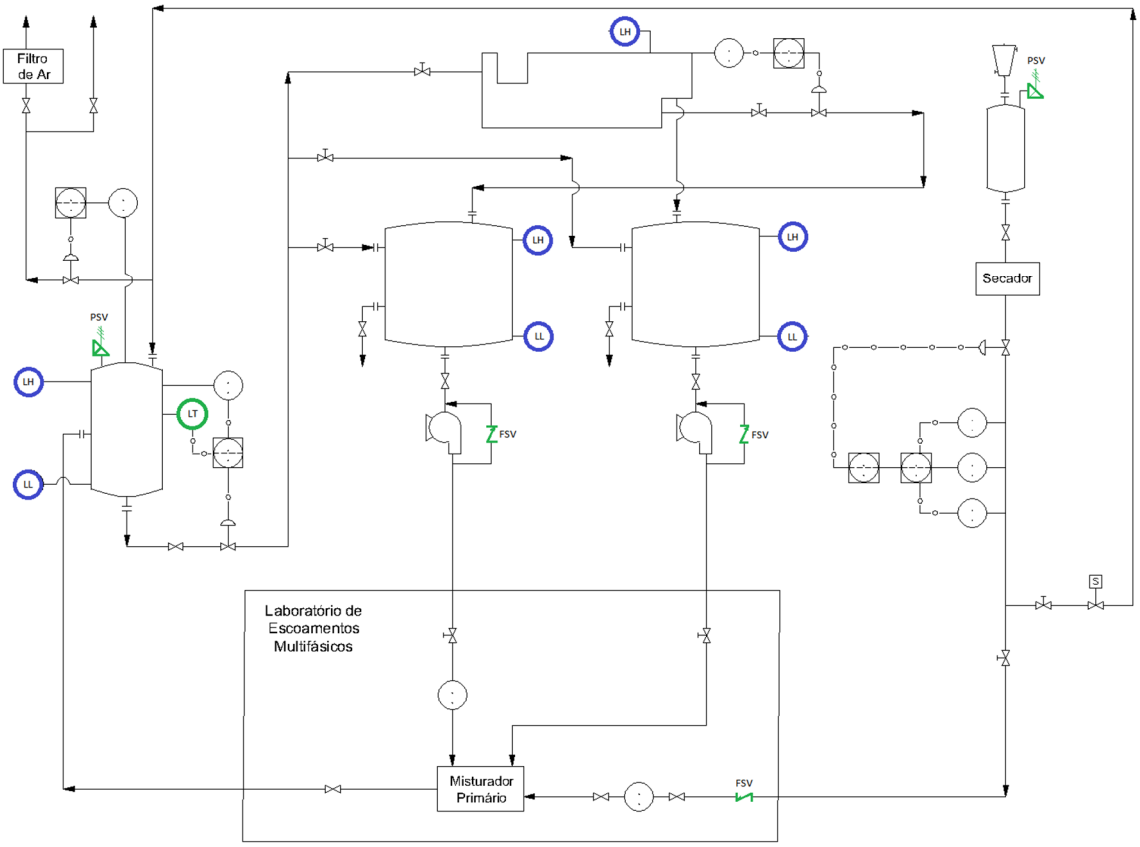
Fonte: Arquivo pessoal

O LEEM conta também com um sistema de ar comprimido para instrumentação que é compartilhado com outros processos.

3.2. Sistema de Segurança

Em trabalhos anteriores, observa-se que houve, desde o começo, uma preocupação com a operação segura da UEEM. Foram instalados instrumentos de medição, dispositivos de alívio e um CLP prevendo o intertravamento da planta. Também há a presença de um sensor de nível redundante em T1 e uma função automática implementada dentro da lógica do supervisório para diminuir a rotação das bombas quando for detectado nível alto em T1 [5]. Estes dispositivos podem ser vistos em destaque na Figura 11. Bombas, compressor e alguns instrumentos também possuem seu próprio sistema local de proteção.

Figura 12 - P&ID com destaque dos instrumentos de segurança



O SIS utiliza um CLP modular que apresenta redundância ou a possibilidade de sua implementação em todos os níveis (entradas/saídas, processador, cabeamento, fonte de alimentação, entre outros). Porém, este não é específico para sistemas de segurança.

Em termos de segurança, vale mencionar também a rede FOUNDATION *fieldbus* que é utilizada para detectar falhas em instrumentos do processo, gerar alarmes, entre outras funcionalidades que facilitam o diagnóstico e a ação preventiva e corretiva.

No entanto, não foram encontrados registros com relação a estudos de análise de riscos ou documentação detalhada de como foi projetado o SIS. Sem uma divisão clara entre as camadas de proteção pode-se gerar confusão entre os usuários e criar dificuldades para se manter o controle da segurança da planta.

3.3. Utilização

Devido a seu caráter acadêmico, a UEEM possui uma frequência de utilização irregular. Isto implica que há períodos em que os equipamentos ficam parados, diferente do ambiente industrial onde tenta-se maximizar o tempo de operação da planta. De certa forma pode ser contra intuitivo porém, quanto menos os instrumentos estiverem ativos, maior a probabilidade de ocorrência de falhas. Isto é comumente observado em instrumentos considerados dinâmicos. Válvulas podem sofrer oxidação, bombas podem sofrer desalinhamento, entre outros cenários que podem apresentar situações de falha prematura.

Com o foco no aprendizado, é esperado que diferentes técnicas de controle e configurações de instrumentos sejam testadas e utilizadas. Portanto, o nível de acesso para alterações nos equipamentos é praticamente livre, o que é indesejável do ponto de vista de um sistema de segurança.

Outro fator a ser observado é a alta rotatividade de usuários. Pelo mesmo motivo apresentado anteriormente, um mesmo operador passa pouco tempo em contato com a planta. Isto também implica que há pouco tempo para o treinamento e capacitação destas pessoas. Consequentemente, a probabilidade de erros humanos tende a aumentar consideravelmente. Para agravar o caso, é natural que não haja um operador experiente para dar suporte ou treinamento para os novos usuários.

Nota-se também que o laboratório pode ser utilizado por diferentes pessoas ao mesmo tempo. Isto aumenta os riscos de uma falha de comunicação entre os usuários, aumenta o grau de exposição ao perigo e potencializa a ocorrência de erros operacionais.

3.4. Conclusão do capítulo

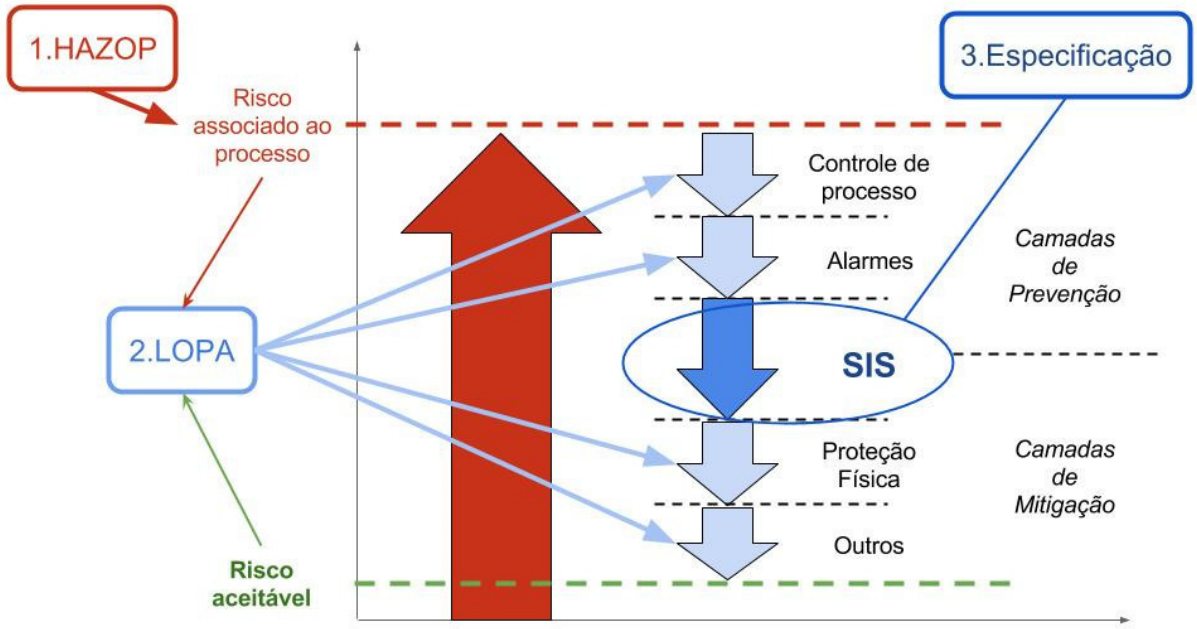
Durante o estudo da UEEM nota-se que há uma margem para questões de segurança ainda não identificadas ou não abordadas. Todas as situações de perigo estão cobertas? Como verificar se a instrumentação existente é eficiente ou mesmo suficiente para evitar acidentes? Essas são algumas questões que se pretende abordar baseando-se o projeto do SIS nos padrões e normas existentes.

Além do risco inerente que o processo pode carregar, há ainda um fator complicador que é o perfil de utilização do laboratório. Aliado à complexidade não acadêmica dos instrumentos e de sua configuração, a curva de aprendizado para a operação da planta se mostra grande e, consequentemente, implicam em maiores chances de falhas humanas. Por esse motivo, verifica-se e reafirma-se a importância da presença do SIS e também de sua documentação para a operação segura da planta.

4. PROJETO DO SIS NA UEEM

Tomando como base o ciclo de projeto de SIS, ilustra-se com a Figura 13 a metodologia seguida neste trabalho:

Figura 13 - Metodologia a ser seguida para o Projeto do SIS



Primeiramente, identifica-se quais os riscos associados ao processo. Para tanto, utiliza-se a técnica HAZOP, que levanta causas, consequências e os cenários de risco da UEEM.

Com o intuito de se obter uma métrica, analisa-se de forma minimamente quantitativa os riscos levantados pelo HAZOP e estes resultados são comparados a um risco aceitável fixado. Nas situações onde o risco encontrado se mostra maior que o aceitável, são avaliadas a adoção de camadas de proteção com o objetivo de se alcançar o nível visado. Para toda esta etapa, é utilizada a técnica LOPA.

Quando não for possível a inclusão de nenhuma outra camada de proteção para alcançar o risco aceitável, uma *Safety Instrumented Functions* (SIF) é especificada para o respectivo cenário. A especificação das SIFs e o projeto do SIS são baseados na norma N-2595 da Petrobrás.

A metodologia utilizada é exemplificada através de alguns casos representativos resultantes do projeto. As tabelas resultantes podem ser consultadas nos apêndices.

4.1. Estudo do sistema atual

Para compreender o funcionamento da planta, foi necessário realizar o levantamento da documentação de trabalhos realizados no laboratório, conversar com atuais usuários e professores ligados ao LEEM. Estas informações formaram a base de conhecimento para a aplicação do HAZOP.

4.2. Aplicação do HAZOP

Como regra geral, foram seguidas as recomendações para o HAZOP das diretrizes de segurança da Petrobrás. O estudo foi realizado com técnicas de *brainstorm* porém não foi possível formar uma equipe multidisciplinar exclusiva para realizar tais reuniões. A metodologia e as considerações estão descritas integralmente no relatório técnico do HAZOP. Para exemplificar, citam-se três considerações feitas:

- Falhas simultâneas de diferentes camadas de proteção não foram contemplados. A sugestão é que estes cenários sejam considerados apenas caso haja no histórico da planta registros deste tipo de ocorrência [11];
- A resposta do operador aos alarmes não foi considerada salvaguarda por não ter sido encontrado um documento com procedimentos de reação específicos para os respectivos alarmes;
- Considerou-se que a planta se encontra funcional e com todos os instrumentos calibrados e configurados corretamente;

Os desvios e as palavras guia utilizados são os mesmos indicados pelas diretrizes de segurança da Petrobrás e já foram mostrados na Tabela 3.

O formato da tabela escolhida foi baseado no padrão utilizado pela Petrobrás que conta com as colunas Desvio, Causa, Consequência, Detecção/Salvaguarda, Recomendações/Observações e Cenário. Um exemplo pode ser visto na Figura 15. As colunas desvio, causa e consequência são de entendimento direto. A seguir, comenta-se brevemente as demais colunas.

Anotar a forma de detecção para o desvio é justificado por ajudar a identificar dependências. Ou seja, em uma eventual falha do dispositivo de detecção, não seria possível reconhecer o respectivo desvio. Isto facilita o raciocínio tanto para quem está montando a tabela quanto para quem irá utilizá-la posteriormente.

Salvaguarda refere-se a dispositivos ou procedimentos de segurança que agem, passiva ou ativamente, para evitar a evolução do cenário para a consequência perigosa. A empresa ou instituição geralmente define uma série de requisitos do que pode ser considerado como salvaguarda. Por exemplo, nas diretrizes de segurança da Petrobrás define-se que “Procedimento operacional não poderá ser considerado como única salvaguarda de um cenário acidental” [11].

Observações e recomendações também são anotadas e são bastante importantes para guiar as providências a serem tomadas após o estudo. Também pode-se indicar a necessidade de investigação mais detalhada quando as informações forem julgadas insuficientes para a análise.

A coluna de cenário contém a descrição de como ocorre a evolução dos eventos após a ocorrência da causa iniciadora. Em outros casos, também poderia conter informações sobre o contexto em que ocorre o desvio.

Após decidido o formato da tabela, iniciou-se o estudo identificando os nós do processo. A divisão levou em conta a funcionalidade dos instrumentos e equipamentos e é ilustrada pela Figura 14.

Concentra-se, então, em cada nó separadamente e estuda-se os possíveis desvios, seguindo as palavras guia. Por exemplo, para o nó T1, analisou-se a possibilidade de ocorrência de algum cenário em que a pressão em algum equipamento alcançasse um valor maior do que o esperado. O tanque T1 suporta um máximo de 6,71 bar e a malha de controle local mantém a pressão interna próxima do ponto de operação. Nesse caso, se a válvula de controle falhar e fechar inesperadamente, não haverá possibilidade de aliviar a pressão interna. Esta, então, irá aumentar livremente. Portanto, considera-se a falha da válvula na posição fechada como uma causa para o desvio de pressão maior em T1. Não contando com a ação da salvaguarda PSV, a pressão subiria até haver o rompimento das conexões dos instrumentos, dos dutos ou, para o pior caso, fissura e explosão do tanque de pressão. Estas informações podem ser vistas pela Figura 15, que apresenta uma linha da tabela de HAZOP.

Figura 14 - Nós selecionados para o HAZOP

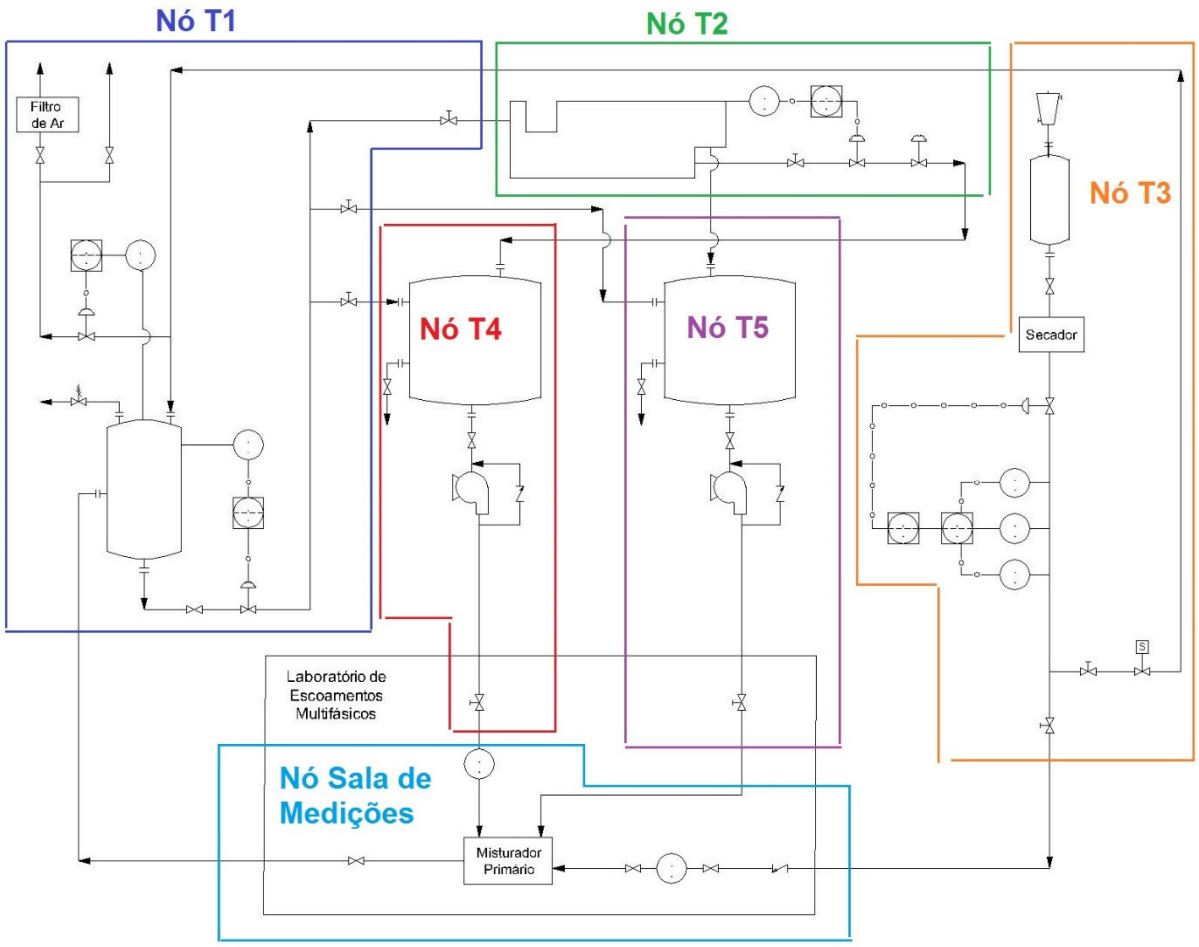


Figura 15 - Exemplo de um cenário do HAZOP

	HAZOP - ESTUDO DE PERIGOS E OPERABILIDADE			Data:	
Unidade:	LEEM	Processo:	UEEM	Página:	
Nó:	T1		Documento (com revisão):		1
Desvio	Causas	Consequências	(D) Detecção (S) Salvaguarda	Recomendações Observações	Cenário
PRESSÃO MAIOR	Válvula de controle de pressão falha CLOSED	Danos aos instrumentos; ruptura tubulação; ruptura e explosão do tanque	(D) SSC indicador de pressão (S) PSV	#001; #002; #003; #004	FF detecta Device Failure em T1; FF troca controle para Manual; sem possibilidade de aliviar pressão; pressão excede o limite;

Algumas recomendações são feitas para o cenário utilizado como exemplo. Observou-se que não há um sistema de alarmes dentro da casa de utilidades portanto uma das sugestões é a implementação de tal sistema; Com a implementação de IHM para o controle da planta, deve-se lembrar de incluir os alarmes de falhas detectáveis aproveitando-se da capacidade de diagnóstico dos sensores e atuadores inteligentes e da rede FOUNDATION *fieldbus*; Devido à severidade da consequência, recomenda-se a especificação de uma SIF para este cenário; Por último, recomenda-se o redimensionamento da válvula de alívio para permitir uma faixa maior de operação da pressão do tanque T1.

Neste cenário, a rede de campo identifica a falha no atuador e troca automaticamente o modo de controle para manual. Mesmo assim, o operador não teria meios para atuar no sistema de modo a aliviar a pressão do tanque T1. Portanto, a pressão cresceria e o cenário apresentaria as consequências levantadas.

Como resultado do HAZOP, um relatório técnico foi criado contendo a metodologia, as considerações realizadas para o estudo, a compilação das recomendações e das observações e todas as tabelas geradas.

Para o contexto deste projeto, as recomendações relacionadas ao SIS são levadas adiante enquanto que as demais ficam registradas como sugestão para implementações futuras.

4.3. Aplicação do LOPA

O LOPA consegue herdar diretamente do HAZOP a descrição das causas, das consequências e dos cenários, como pode ser visto na Figura 16.

Figura 16 - Exemplo de tabela LOPA

#	ID	Descrição			Severidade Maxima	Frequência Tolerável	Frequencia do cenário	IPL	PFD da IPL	Frequência da Consequência
001		Falha CLOSED da válvula de controle de pressão	tanque T3 continua a enviar ar comprimido, pressão interna em T1 aumenta além da capacidade máxima, danos aos instrumentos em T1	explosão do tanque T1, danos estruturais ao laboratório, danos a outros equipamentos do laboratório, fatalidades	V	1.0E-5	.04555	PSV	0.01	0.0004555
002										
003		Falha sensor de pressão em T1			V	1.0E-5	.00555	PSV	0.01	0.0000555
004										

Atribui-se a severidade de acordo com o impacto da consequência para cada categoria e o maior dentre os quatro valores foi associado ao cenário, como pode ser

observado na Figura 17. O valor de frequência tolerável relacionada à respectiva severidade foi obtida a partir da Tabela 2, apresentada no capítulo 2.

Figura 17 - Classificação de severidades para cada categoria

			Severidade				
#	ID	Descrição	Pessoas	Patrimônio	Meio Ambiente	Imagem	Maximo
001	a	Falha CLOSED da válvula de controle de pressão	V	V	III	IV	V

Determinar a frequência do cenário não é uma tarefa trivial pois geralmente envolve dados de taxas de falhas dos equipamentos que, por sua vez, podem depender de inúmeros fatores. De acordo com [7], a fonte mais confiável para estes dados é o histórico da própria planta. Em seguida, são os *handbooks* e por último são os dados dos fornecedores. Isto se deve às condições específicas de cada processo e da metodologia de cálculo utilizada. Neste projeto, devido à falta de um histórico completo, optou-se por utilizar dados apresentados no *handbook* da OREDA [10].

Para as IPLs, os dados foram retirados da tabela da norma N-2595 apresentada parcialmente na Figura 18.

Figura 18 - IPL e suas PFD_{avg} típicas

Camada de Proteção Independente (IPL)	Probabilidade média de falha na demanda (PFD_{avg})
Função automática no SSC (B.2.7.4.1)	1×10^{-1}
Resposta do operador ao alarme (B.2.7.4.2)	1×10^{-1}
Dispositivo mecânico de alívio / válvula de segurança e alívio (B.2.7.5)	1×10^{-2}
Múltiplos dispositivos de alívio independentes (bocais, descargas etc.), porém mais de um precisa atuar para atender a 100 % do cenário (exemplo: PSV estagiadas). (B.2.7.5)	1×10^{-1}
Dispositivo mecânico interno de segurança independente do SIS e do SSC (p.ex. desarme mecânico de turbina)	1×10^{-1}

Fonte: N-2595 [12]

A partir destes dados, foi calculado o risco residual para cada cenário. Para os casos em que a frequência tolerável não foi alcançada, avaliou-se a possibilidade da

utilização de outras camadas de proteção. Não mostrando-se possível, só então foi designada uma SIF.

A identificação da SIF é praticamente direta. Ela deve agir no processo para impedir que o desvio de respectivo cenário alcance a consequência descrita.

Durante a aplicação do LOPA, os cenários de desvios de pressão baixa em T1 exigiram uma atenção diferente. Identificou-se que estes cenários não traziam nenhuma consequência perigosa de maneira direta. Porém, sem pressão, o líquido não consegue ser enviado para o tanque T2 e, portanto, começa a aparecer um desvio de nível em T1. Por esse motivo, para a análise, considerou-se “Pressão Insuficiente” como uma das causas para o cenário de “Nível Maior” em T1, como mostrado na Figura 19. Para a quantificação da frequência deste cenário, somou-se as frequências de todas as causas de “Pressão Menor” levantadas. Em outras palavras, fez-se uma operação lógica OU de todas as frequências das causas do desvio em questão.

Figura 19 - Cenário de Nível Maior com causa Pressão Insuficiente

#	ID	Descrição			Severidade Maxima	Frequência Tolerável	Frequencia do cenário	IPL	PFD da IPL	Frequência da Consequência
029		Pressão insuficiente em T1	nivel em T1 aumenta de acordo com variação de entrada/saída de fluido	tanque de armazenamento T4/T5 esvazia(m), danos às bombas, fluxo de entrada de fluido em T1 interrompido	IV	1.0E-4	.91325			0.9132478
030				alcançada capacidade máxima, invasão do duto de ar por liquido, aumento da pressão interna nas linhas, danos aos instrumentos em T1, vazamento por fissuras em conexões/equipamentos, inundação do laboratório, danos a outros equipamentos do laboratório	IV	1.0E-4	.91325	Função Automática de Nivel	0.1	0.0913248

Porém, observa-se que a frequência da consequência resultante é extremamente alta comparada com a tolerável. Isto se deve à alta frequência de ocorrência do cenário e a ausência de qualquer IPL. Observou-se que o fator que mais contribuía para isto era a elevada frequência de falhas do compressor de ar localizado no nó T3. Para tentar diminuir este valor, projetou-se uma SIF para atuar como IPL mitigadora.

Atualmente, não há instrumentos de medição do compressor conectados ao sistema. Portanto, o processo só sentirá os efeitos de sua falha depois que o tanque de ar comprimido do compressor esvaziar e a malha de controle em T1 não conseguir

mais controlar a pressão interna. Por isso, a ideia é monitorar a situação do nó T3 e agir no processo antes que o tanque T1 seja influenciado.

A arquitetura e o valor de PFD_{avg} são calculados apenas na etapa seguinte. Porém, para manter a linha de raciocínio, os valores após a adoção da IPL mitigadora são adiantados e mostrados na Figura 20.

Figura 20 - Cenário de Nível Maior com causa Pressão Insuficiente após adoção de IPL mitigadora

#	ID	Descrição			Severidade Maxima	Frequência Tolerável	Frequencia do cenário	IPL	PFD da IPL	Frequência da Consequência
029		Pressão insuficiente em T1	nivel em T1 aumenta de acordo com variação de entrada/saída de fluido	tanque de armazenamento T4/T5 esvazia(m), danos às bombas, fluxo de entrada de fluido em T1 interrompido	IV	1.0E-4	.33778		0.01	0.0033778
030				alcançada capacidade máxima, invasão do duto de ar por liquido, aumento da pressão interna nas linhas, danos aos instrumentos em T1, vazamento por fissuras em conexões/equipamentos, inundação do laboratório, danos a outros equipamentos do laboratório	IV	1.0E-4	.33778	Função Automática de Nivel; Válvula de retenção	0.099	0.0334401

Após a análise de todos os cenários, montou-se um relatório técnico contendo todas as considerações feitas, resultados dos cálculos e a tabela gerada.

4.4. Especificação das SIFs

A especificação das SIFs tem como base as indicações da norma N-2595 e tem como objetivo levantar principalmente os parâmetros SIL e MTTFS. Aproveita-se também para obter o primeiro esboço da arquitetura da SIF.

O RRF de cada SIF é obtido pela divisão da frequência da consequência e da frequência tolerável apresentados pelo LOPA. E, utilizando a Tabela 1, pode-se encontrar o respectivo valor de SIL. Uma mesma SIF geralmente pode ser utilizada para proteger múltiplos cenários. Por isso, sua RRF deve atender, pelo menos, o maior valor de RRF apresentado pelos cenários para o qual foi projetada. Ou seja, deve sempre atender ao “pior caso”.

A N-2595 recomenda que a determinação do MTTFS aceitável seja realizada seguindo uma tabela que relaciona os custos financeiros envolvidos em um cenário de parada espúria. Devido ao perfil de utilização da UEEM, optou-se por não especificar um valor alvo para o MTTFS de cada SIF. Considerou-se que uma parada

espúria não traria nenhum risco, dano ou prejuízo financeiro, apenas uma perda de tempo de ensaio. Espera-se apenas que este parâmetro seja maior que o período entre testes para não atrapalhar a operação normal da planta.

Nesta etapa, também se averiguou os estados seguros do processo. Estes são caracterizados por estados a partir dos quais não há possibilidade do sistema evoluir para uma situação de perigo. Cada cenário foi analisado e as ações necessárias para levar o processo à este ponto formaram a lógica da SIF. Ações secundárias também são levantadas de forma a evitar situações de desperdício e auxiliar a operação.

Em primeira instância, essas funcionalidades estão em formato genérico, como por exemplo “interromper fluxo de ar comprimido”. A escolha da estratégia de implementação destas funcionalidades é mostrada na Tabela 6.

Tabela 6 - Escolha de implementação das funcionalidades

Funcionalidade requerida	**Implementação escolhida**
Interromper fluxo de ar comprimido	Fechar válvula de bloqueio na linha FA01
Interromper fluxo de entrada de T1	Interromper fluxo de saída de T4, de T5 e de ar comprimido
Interromper fluxo de saída de T1	Fechar válvula de bloqueio na linha FA07
Interromper fluxo de entrada de T2	Interromper fluxo de saída de T1
Interromper fluxo de saída de T2	Fechar válvula de bloqueio na linha FA11
Interromper fluxo de saída de T4	Desligar bomba B1
Interromper fluxo de saída de T5	Desligar bomba B2

Seguindo recomendações da API-14C, a interrupção de fluxo de entrada deve ser realizada, de preferência, na sua fonte primária [2].

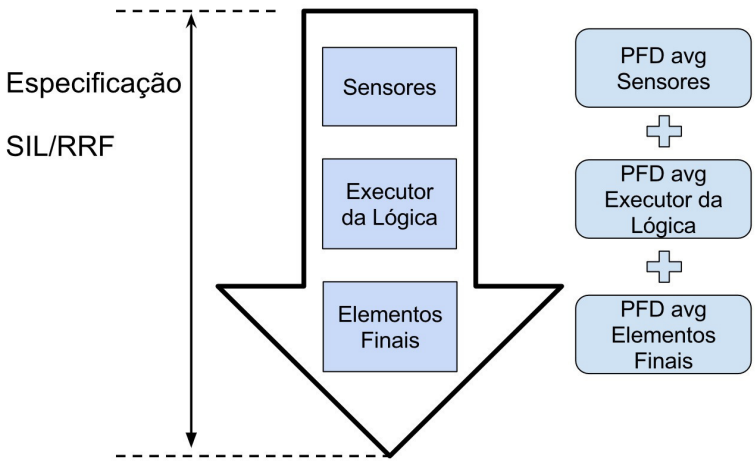
A utilização das válvulas da linha de agua (FA04) e de óleo (FA05) para interrupção do fluxo enquanto as bombas estiverem ligadas não é recomendado por causar pressão desnecessária nas válvulas, forçar a utilização do circuito de recirculação, além de poder causar o efeito de *water hammer*. Ao interromper repentinamente o fluxo, a porção de fluido que ainda não atingiu o ponto de interrupção cria uma onda de pressão dentro do duto que pode chegar a rompê-lo. Quanto maior for a distância entre a fonte do fluxo e o ponto de interrupção, maior é o pico de pressão criado.

A partir disso, foi possível ter uma ideia inicial de quais sensores e elementos finais deverão compor cada SIF. Esta informação será utilizada e aprofundada na etapa seguinte.

4.5. Verificação do SIL e escolha da arquitetura de SIF

A partir da seção anterior, pode-se observar que uma SIF é composta basicamente por iniciadores, executores de lógica e elementos finais. São estes três elementos em conjunto que devem ser capazes de atender o valor de RRF e de SIL especificados, como ilustrado pela Figura 21.

Figura 21 - O somatório dos PFD_{avg} deve ser capaz de alcançar o SIL especificado



Caso os valores especificados não sejam alcançados, pode-se utilizar diferentes recursos, tais como: diminuição no intervalo de tempo entre testes, utilização de equipamentos com uma taxa de falha menor (PFD menor) ou adição de redundância.

Diminuir o tempo mínimo de intervalo entre testes pode ser bastante efetivo, mas também pode chegar a níveis impraticáveis ou até tornar o sistema menos seguro devido a constante operações de *bypass,* desligamento e reinício do processo. A incerteza na determinação de taxa de falhas de instrumentos já foi discutida anteriormente e sabe-se que não é um parâmetro tão simples de se utilizar. Portanto, opta-se por mudar a arquitetura da SIF adicionando redundância de componentes.

Ao adicionar um componente redundante, a probabilidade de falha do novo conjunto diminui pois agora é necessário que ocorra a falha simultânea de ambos os componentes para que a SIF fique indisponível. No entanto, isto também adiciona outra questão. Caso haja diferença entre os sinais, como julgar qual é o correto? A não ser que os instrumentos sejam capazes de realizar autodiagnóstico, é necessário interromper o sistema e testá-los. Sua arquitetura com 2 elementos redundantes, chamada de votação *1 out of 2* (1oo2), permite que a SIF tenha uma probabilidade menor de ficar indisponível porém agora inclui o evento de *trip* espúrio.

Para evitar o *trip* espúrio, poderia ser utilizada uma arquitetura de votação *2 out of 2* (2oo2). Isto implica que ambos os sensores precisam acusar um desvio no processo para que a SIF seja ativada, retirando o fator de dúvida na ocorrência de diferença entre sinais. Por outro lado, a SIF não será ativada no caso de um dos sensores falhar ao não indicar um desvio. Ou seja, este tipo de votação diminui a probabilidade de *trip* seguro porém é "menos seguro" visto que a probabilidade da SIF não responder a uma demanda real aumenta.

De forma análoga, para 1oo3, 2oo3 e demais votações, as arquiteturas apresentam sempre um compromisso entre disponibilidade da SIF (PFD) e intervalo entre *trips* seguros (MTTFS).

Antes de partir diretamente para uma complexidade alta, a sugestão da N-2595, é que se inicie a verificação a partir da arquitetura mais simples com esquema de votação 1oo1.

Para os cálculos de verificação de SIL, utilizou-se o método apresentado pela ISA 84.00.02 que se refere à utilização das equações simplificadas do modelo de Markov. Algumas considerações devem ser levadas em conta para a sua utilização e seus detalhes são comentados na ISA 84.00.02-part 2 [9].

Devido à dificuldade em garantir a existência de condições habilitadoras (EE) e de fatores modificadores (MF) durante todo o ciclo de vida da planta, estes dois parâmetros foram omitidos, atribuindo-lhes o valor 1. Em outras palavras, não há ponderação do risco residual devido a outros fatores além das causas iniciadoras levantadas.

A Figura 23 mostra os cálculos de verificação de PFD_{avg} para a SIF001 com a arquitetura 1oo1 para todos seus componentes, mostrada na Figura 22. Para a taxa de falha do CLP, assumiu-se valores típicos. Não houve tanta preocupação com a

precisão de seu valor porque tipicamente os sensores e elementos finais possuem uma influência maior nos cálculos e são considerados elementos mais críticos para a segurança [7]. As taxas de falhas de sensores e elementos finais foram obtidas a partir do OREDA [10]. A taxa de falha para os circuitos de desarme das bombas é baseado em valores típicos de relés obtidos em [8]. A fórmula para a arquitetura 1oo1 [9] é apresentada a seguir:

$$PFD_{avg} = \lambda_{du} * (TI/2)$$

Figura 22 - Arquitetura 1oo1 para a SIF001

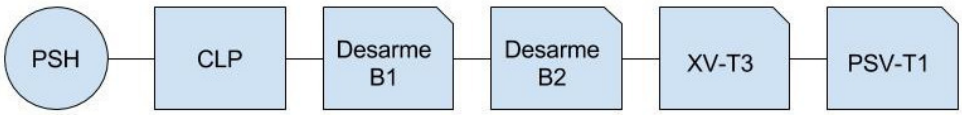


Figura 23 - Cálculo para o PFD_{avg} da SIF001

SIF 001	RRF alvo	90				
	Sensor Pressão	CLP	Circuito B1	Circuito B2	XVT3	PSVT1
Taxa de Falha	5.55E-3	1.00E-3	1.70E-3	1.70E-3	2.51E-2	5.21E-2
PFDavg individual	6.94E-4	1.25E-4	2.13E-4	2.13E-4	3.13E-3	6.52E-3
TI [anos]	0.25					
PFDavg da SIF	1.09E-2	RRF	91.82			

Primeiramente, calcula-se o PFD_{avg} para cada grupo de componente da SIF. O PFD_{avg} total da SIF é obtido pelo somatório dos valores individuais. O RRF é obtido pelo inverso do PFD_{avg}.

A princípio, o valor de Intervalo entre Testes (IT) foi utilizado como parâmetro livre e variado entre valores considerados minimamente praticáveis considerando o perfil de utilização da UEEM. Com um intervalo de 0,25 anos, ou seja, 4 meses, a SIF consegue alcançar a RRF com esta estrutura.

Em um segundo exemplo, analisa-se a SIF004. Pelos cálculos, mostrados na Figura 24, com a arquitetura 1oo1 e o IT de 0,25, não foi possível alcançar o RRF especificado. Optou-se por não reduzir o IT e adicionar uma redundância no sensor de nível. A escolha foi devido ao peso de contribuição da taxa de falha do sensor e ao

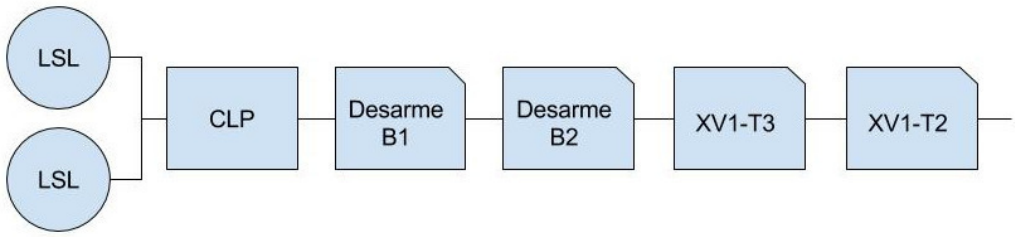
preço menor se comparado aos outros componentes. Ou seja, do ponto de vista de projeto, seria economicamente mais atrativo adquirir dois sensores, além do fato que a contribuição para a diminuição da PFD_{avg} total seria maior. E, como não há uma preocupação com o MTTFS, optou-se pelo esquema de votação de 1oo2, como pode ser visto na Figura 25. A fórmula é mostrada abaixo:

$$PFD_{avg} = ((\lambda_{du})^2 * (TI)^2) \,/\, 3$$

Figura 24 - Cálculo para o PFD_{avg} da SIF004

SIF 004	RRF alvo	96				
Arq	Sensor Nivel	CLP	Circuito B1	Circuito B2	XVT3	XVT2
Failure Rate	5.03E-2	1.00E-3	1.70E-3	1.70E-3	2.51E-2	2.51E-2
PFDavg individual	6.29E-3	1.25E-4	2.13E-4	2.13E-4	3.13E-3	3.13E-3
TI	0.25					
PFDavg da SIF	1.31E-2	RRF	76.34			
Arq	[2x] Sensor Nivel	CLP	Circuito B1	Circuito B2	XVT3	XVT2
Failure Rate	5.03E-2	1.00E-3	1.70E-3	1.70E-3	2.51E-2	2.51E-2
PFDavg individual	5.27E-5	1.25E-4	2.13E-4	2.13E-4	3.13E-3	3.13E-3
TI	0.25					
PFDavg da SIF	6.87E-3	RRF	145.64			

Figura 25 - Arquitetura de votação 1oo2 para os sensores da SIF004



Em casos em que o MTTFS é um parâmetro que deve ser considerado, deve-se utilizar diferentes esquemas de votação e manter o compromisso o PFD_{avg}, como comentado anteriormente.

De forma semelhante, foram realizados cálculos para as demais SIFs. Observou-se que utilizar um TI de 0,25 permitia que nenhuma arquitetura precisasse de redundâncias de válvulas portanto, optou-se por atribuir esse intervalo de testes

como padrão. A memória de cálculo completa para os PFD_{avg} das SIFs e suas arquiteturas finais se encontram no documento de Projeto de SIS.

Vale lembrar novamente que as equações utilizadas baseiam-se em algumas suposições e são simplificações. Existem softwares comerciais capazes de realizar os cálculos com um grau de aprofundamento maior porém dependem de um levantamento de dados muito mais detalhado. Outro fator a ser observado é que os valores foram retirados de um banco de dados que observa processos similares em ambiente industrial, perfil este diferente do encontrado na UEEM. Para resultados mais aproximados, deve-se utilizar os dados de histórico da planta como parâmetros dos cálculos.

4.6. Projeto Detalhado

4.6.1. Descrição geral dos componentes

A partir da escolha da arquitetura, levantou-se a quantidade de componentes do SIS. Deve-se observar que a SIF007 (“Pressão Menor em T3”) deve ser uma IPL com relação à SIF002 (“Nível Maior” em T1). Desse modo, cada uma deve possuir o seu próprio sistema de desarme das bombas.

4.6.2. Instrumentos de Medição

Seguindo a norma N-2595, sugere-se que os iniciadores do SIS possuam a mesma faixa de operação e incertezas compatíveis que os utilizados no processo. Portanto, a especificação dos instrumentos para o SIS é baseada nos já existentes no processo.

4.6.3. Elementos finais

Devido à localização das válvulas do SIS, as características de vazão, pressão, estanqueidade acabam sendo similares às do processo. Portanto, opta-se por utilizar as mesmas especificações do projeto original [1].

Outro parâmetro a ser definido é o tempo de resposta. A API 14C recomenda que o SIS deva ser capaz de levar o processo ao seu estado seguro em menos de 45 segundos [2]. Este templo inclui a detecção, o processamento da lógica e a completa

atuação dos elementos finais. A ação do SIS da UEEM recebe uma resposta praticamente direta do processo portanto o tempo de resposta das SIFs será basicamente composto pelos tempos de resposta de cada componente. Como sensores e CLPs possuem respostas rápidas, a dinâmica das válvulas acaba sendo o parâmetro mais significativo.

Anteriormente, já foi mencionado que o tempo de resposta das válvulas não pode ser muito pequeno pois pode causar o efeito de *water hammer* porém não há nenhuma outra referência para a escolha deste tempo. Em algumas fontes, engenheiros da parte de segurança utilizam, na prática, uma regra que estima uma relação entre tempo de fechamento e tamanho da válvula. Esta relação é de 1 ou 1,5 segundos por polegada para o fechamento de válvulas de ESD [6]. Não tendo acesso a nenhuma outra fonte, optou-se por utilizar esta regra prática como base.

4.6.4. Valores de *trip*

Definidos os tempos de resposta das válvulas, pode-se identificar o valor limite, em termos de unidades do parâmetro de desvio, onde a SIF ainda consegue responder antes do processo alcançar o cenário perigoso. Para isso, é preciso conhecer ou estimar a dinâmica do processo nos respectivos cenários. Não foi possível realizar ensaios e não se encontrou dados suficientes para modelar o processo portanto realizou-se um estudo teórico para obter uma aproximação da dinâmica da planta nos cenários de pior caso em que as SIFs precisam agir.

A dinâmica da pressão em T1 mostrou-se complexa e necessitaria de um aprofundamento maior no estudo da termodinâmica ou de ensaios na planta. Como o objetivo deste projeto não é a modelagem do processo e como seria perigoso realizar testes nos limites de segurança do tanque, optou-se por não levantar o tempo de resposta para essa SIF.

A vazão de entrada em T1 considera a maior vazão especificada em projeto que é de 15 m^3/h [1]. Para o cenário de Nível Alto, o pior caso seria quando não há fluxo de saída de T1. A SIF deve ser ativada com no mínimo 1,5 segundos (sem considerar o tempo de atraso de transporte) para que o nível não alcance o limite superior. Isto representa um valor de 1% da altura limite máxima.

A vazão de entrada em T2 foi baseada no tempo médio de permanência do líquido em T1 [1] e o ponto de operação para este caso é o mesmo do projeto original.

O nível do tanque T2 em operação normal é de aproximadamente 95%, representando uma distância de apenas 5 centímetros até a tampa do tanque. Devido à pequena margem, optou-se por especificar o valor de *trip* em 98% da altura de T2. Isto também implica que o sensor de nível deverá possuir uma precisão na ordem de, no mínimo, centímetros.

A vazão de saída de T2 considera a dinâmica de esvaziamento de tanque por gravidade. Considerou-se como limite inferior a altura em que a interface de água-óleo alcança a saída de água do tanque T2. Considerando o ponto de operação de 60% de nível de interface, isto implica que a altura da superfície do óleo se encontraria em 75% da altura máxima de T2 e este é especificado como valor de *trip* para a SIF004.

Não incluindo vazamentos, há dois cenários para o esvaziamento de T4 e T5. O primeiro seria por esquecimento da válvula manual para o fosso aberta e o segundo seria pela vazão de saída forçada pela bomba. Considerando o processo já em operação, ou seja, com T4 e T5 parcialmente preenchidos, a vazão média causada pelas bombas se mostrou maior que a vazão pela gravidade. Portanto, o tempo de esvaziamento dos tanques consideram o pior caso com a vazão de saída em 10 m^3/h [5].

Com base nos dados apresentados no capítulo sobre a UEEM, pode-se inferir que T4 trabalha com aproximadamente 14% de nível para escoamentos envolvendo água e óleo. No entanto, deve-se notar que, uma vez preenchido, o volume de líquido do tanque T2 não retorna aos tanques de armazenamento. Portanto, o pior caso para T4 seria com T2 cheio (devido alguma utilização anterior) e um novo ensaio com escoamento com apenas água ou água-ar. Numa estimativa com o ponto de operação de nível em T1 para 50%, o tanque T4 teria apenas 4% de nível de água. O ponto de *trip* escolhido foi de 1,5% da altura máxima. Deste modo, tenta-se fugir de *trips* espúrios devido à agitação da água mas também tenta-se manter o compromisso com a precisão do sensor de nível.

Os cálculos para o esvaziamento de T5 seguiram o mesmo raciocínio porém apresenta uma margem um pouco maior devido ao ponto de operação projetado para T2. Para tentar manter uma semelhança, especifica-se o mesmo ponto de *trip* que T4.

4.6.5. Alarmes

Definidos os valores de *trip*, também é possível prever uma lista de alarmes do SIS. Além dos alarmes para cada ocorrência de demanda, também sugere-se a implementação de um para avisar sobre a ativação da função automática do SSC de proteção contra nível alto em T1.

Para o caso de utilização de sensores contínuos, diferentes de chaves *on-off*, a N-2595 permite a comparação entre os sensores do processo e do SIS para identificação de desvios de leitura. Para o SIS da UEEM, é possível fazer essa comparação na medição de nível em T1 e em T2. Por esse motivo, são previstos alarmes de desvio para estas duas variáveis.

Outro tipo de alarme previsto em norma é o de pré-*trip*. Estes são especificados sempre que houver tempo suficiente para ação corretiva pelo operador. De acordo com [4], o estudo mostrou que um operador numa sala de controle consegue responder a múltiplos alarmes simultâneos em média em 25 segundos. Considerando o perfil de usuário da UEEM, optou-se por especificar 30 segundos como resposta média do operador. Os processos que possuem uma dinâmica que permitem os alarmes de pré-*trip* são os de nível alto em T1 e de nível baixo em T2.

4.6.6. Demais Requisitos

A N-2595 detalha que não podem ser utilizado protocolos digitais para a comunicação dos iniciadores e elementos finais do SIS. As implementações devem ser realizadas no padrão 4 a 20 mA.

Outros requisitos também são descritos detalhadamente na norma. Foi criado um documento de projeto de SIS com a intenção de ser utilizado como base para a aquisição de equipamentos, contratação de serviços e instalação do SIS.

4.7. Plano de Manutenção

O propósito do plano de manutenção é alertar futuros usuários do laboratório sobre os impactos que o perfil de utilização da UEEM e a modificação dos parâmetros do SIS causam no desempenho da segurança.

A primeira observação é com relação ao intervalo de tempo que a planta fica parada. Como mencionado no capítulo 3, isto faz com que a probabilidade de falha de dispositivos de campo aumentem significativamente. Este comportamento pode ser

observado experimentalmente ou através de bancos de dados. Para um mesmo tipo de válvula, por exemplo, as taxas de falhas em válvulas de SIS são no mínimo 3 vezes maiores. Portanto, uma sugestão é considerar instrumentos e dispositivos do processo como se tivessem o mesmo comportamento dormente do SIS.

Uma outra sugestão é que seja realizada uma bateria de testes para verificar a integridade de todos os componentes, tanto do SIS quanto do processo, antes de cada novo período de utilização.

No plano de manutenção, sugere-se fortemente o início de monitoramento de falhas dos componentes da UEEM. A curto prazo, este dados podem não ser significativos porém é de grande importante iniciar a cultura de coleta de relatórios de testes e de falhas para o gerenciamento de riscos da planta.

5. RESULTADOS

Neste trabalho, algumas análises foram realizadas para identificação, verificação e apoio à decisão de projeto e são mostradas na Tabela 7. Além disso, foram gerados 4 relatórios principais: um para o HAZOP, um para o LOPA, um para o Projeto do SIS e um para o Plano de Manutenção. Cada um destes itens é comentado a seguir.

Tabela 7 - Análises e respectivos resultados

Análise	**Resultados**
HAZOP	Identificação de 8 desvios perigosos na UEEM
LOPA	Levantamento de 6 SIFs principais e 1 auxiliar e respectivos valores alvo de SIL
Verificação de SIL (via equações simplificadas de Markov)	Especificação de 3 SIFs com arquitetura 1oo1 e 4 SIFs com 1oo2
Dinâmica do processo	Tempos de resposta para as SIF e valores de *trip*

A análise de riscos HAZOP resultou em um relatório com o levantamento de cenários de potencial perigo e a identificação de suas causas e consequências. Foram reconhecidos 7 tipos diferentes de falhas em 39 pontos distintos, que podem gerar 8 tipos de desvios indesejáveis ou perigosos. Além disso, foram documentadas sugestões para o melhoramento da segurança da planta em diferentes níveis de camadas de proteção e podem ser conferidos no Apêndice A. O relatório final contém a descrição da metodologia e considerações realizadas que explicam o contexto sob o qual foi realizado o HAZOP. Estas informações são bastante importantes pois permitem sincronizar trabalhos realizados em épocas e por pessoas diferentes.

Através do LOPA foi possível classificar os cenários de risco através de categorias de severidade, estimar sua frequência de ocorrência e identificar diferentes camadas de proteção. A tabela gerada nesta etapa pode ser conferida no Apêndice B. Esta é uma maneira de quantificar o risco associado ao processo e compará-lo com uma métrica de risco aceitável para apoiar decisões de engenharia. Sem quantificação do risco, não seria encontrado um valor de RRF e o levantamento do SIL teria de ser baseado apenas na experiência do engenheiro projetista.

Também foi criado um relatório final para o LOPA. É com base nesses resultados que se identifica a necessidade da implementação de uma SIF e obtém-se seu respectivo valor alvo de SIL. A metodologia e considerações também foram registradas para permitir a reutilização e auditoria de seus dados.

Além de projetar a SIF, foi realizada a análise de verificação de SIL. Nos casos onde se observou que a arquitetura dos instrumentos não era suficiente, especificou-se uma redundância em algum dos componentes. A memória de cálculo para todas as SIFs pode ser verificada pelo Apêndice C.

Foram conduzidos estudos teóricos do processo em seu ponto de operação e próximo aos limites de segurança. Seus resultados foram utilizados para estimar o tempo necessário para o desvio alcançar a consequência indesejável. Dessa forma, pôde-se especificar os valores de *trip* e também adiantar uma estimativa da precisão necessária dos sensores utilizados em cada SIF.

A especificação das SIFs é composta por uma extensa lista de parâmetros. Requisitos funcionais, de integridade, alarmes, entre outros, foram levantados e documentados em folhas de SIF, que podem ser conferidos integralmente no Apêndice D. Este formato de documentação facilita sua utilização, uma vez que não é direta a visualização das SIFs através de diagramas como o P&ID, que é mostrado na Figura 26. Um resumo de cada SIF com seus principais resultados é mostrado na Tabela 8. A tabela de alarmes do SIS com valores de *trip* e tempos de segurança estimados é mostrada no Apêndice E. O relatório de projeto de SIS contém todas as folhas de SIFs, assim como a descrição de demais requisitos e serve de base para a aquisição de componentes e para a instalação e operação do SIS.

Um resultado interessante foi a ausência de SIFs para os casos de esvaziamento e pressão baixa em T1. Isto foi possível porque ambas não foram identificadas como causas diretas de consequências indesejáveis. Esta ausência é vantajosa pois permite a troca de líquido e a despressurização em T1 sem a necessidade de um *bypass* durante a inicialização e o desligamento do sistema.

A ausência de SIFs para transbordamento dos tanques T4 e T5 são justificadas porque o sistema foi projetado para ser auto suficiente e pelo fato das SIFs de esvaziamento e transbordamento de T2 conseguirem evitar os casos em que e água e óleo acumulem em um mesmo tanque.

Figura 26 - P&ID do SIS

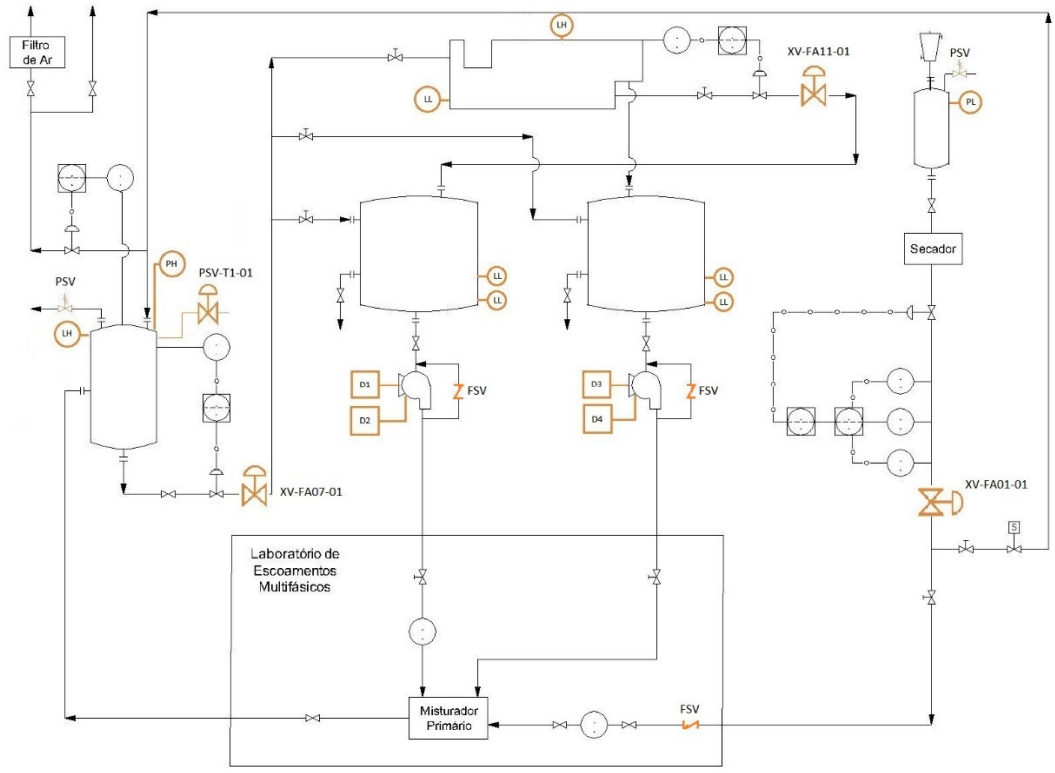


Tabela 8 – Resumo das SIF

SIF	Desvio	SIL	IT (ano)	Redundância	IPLs
001	Pressão alta em T1	1	0,25	---	PSV
002	Nível alto em T1	1	0,50	---	Função Automática
003	Nível alto em T2	2	0,25	1oo2 Sensor	---
004	Nível baixo em T2	1	0,25	1oo2 Sensor	---
005	Nível baixo em T4	3	0,25	1oo2 Sensor	---
006	Nível baixo em T5	3	0,25	1oo2 Sensor	---
007	Pressão baixa em T3	1	0,25	---	---

O plano de manutenção contém considerações e recomendações de operação do SIS e da planta devido ao seu perfil de utilização. Estas informações são importantes do ponto de vista de orientar ou impedir possíveis mudanças no SIS por futuros operadores ou projetistas.

6. CONSIDERAÇÕES FINAIS E PERSPECTIVAS

Através deste trabalho, foi possível realizar a especificação de um SIS para a UEEM seguindo as primeiras etapas do ciclo de projeto de segurança. Isto incluiu a aplicação do HAZOP, do LOPA, das normas da Petrobrás e de práticas recomendadas de projeto para a indústria de petróleo e gás que resultou em documentos detalhados de análises e especificação. Esta documentação é bastante importante, não apenas do ponto de vista de organização, mas também de orientação e de segurança pois pretende-se, assim, minimizar os riscos de acidentes também devido à falta de informação. Portanto, pode-se dizer que os objetivos iniciais foram alcançados com sucesso.

Observou-se que esta é uma tarefa que exige grande esforço e o envolvimento de todas as partes ligadas à planta ou ao processo. Pensando amplamente, não é surpresa encontrar resistência por parte de empresas e indústrias devido à necessidade de alto investimento financeiro, de tempo e de recursos humanos em um sistema predominantemente dormente. O engenheiro deve estar preparado para argumentar e convencer a direção de uma empresa, por exemplo, da importância dos sistemas de segurança. Nesse sentido, a análise e avaliação de riscos da planta se mostram ferramentas poderosas para a discussão.

Sem a utilização de uma ferramenta metódica, a identificação de riscos associados à planta torna-se muito influenciável ao subjetivismo e empirismo. Utilizar o HAZOP e o LOPA permite explorar uma vasta quantidade de cenários e tentar minimizar possíveis erros de especificação, além de sistematizar e alinhar a análise de risco à práticas utilizadas na indústria. Pode-se citar como outra vantagem que a mesma análise se mantém válida enquanto a planta manter as mesmas características. Dependendo da experiência do grupo responsável pelo estudo, pequenas modificações podem ser analisadas pontualmente e anexadas ao estudo original.

Por outro lado, se é exigido tamanho esforço para a execução de um projeto de SIS, pode-se entender que garantir a segurança não é uma tarefa tão simples ou óbvia quanto pode parecer. Tanto as demais camadas de proteção quanto o comprometimento das pessoas envolvidas em todo o ciclo de segurança são de igual importância. O SIS é considerado a última barreira de prevenção e, na prática, deve-se tentar evitar de todo modo que uma demanda real ocorra.

Além do risco inerente da planta, o perfil de utilização da UEEM aumenta a possibilidade de cenários indesejáveis. Por esse motivo, é importante criar e manter uma cultura de segurança da planta. Sugere-se investir em procedimentos e outras camadas de proteção, além de manter o SIS como uma camada independente e, na medida do possível, imutável.

Como sugestão para trabalhos futuros, cita-se a aplicação das etapas seguintes do ciclo de segurança previsto na norma N-2595. Isto inclui a implementação, testes e validação do SIS, além da criação de um plano de gerenciamento de segurança da UEEM. Poderia ser incluído também uma etapa para a verificação de reutilização de instrumentos do SIS antigo.

Durante o projeto, observou-se a ausência do detalhamento de uma metodologia para determinação dos estados seguros e de ações para levar o processo até eles. Uma estratégia levantada empiricamente durante a especificação poderia esconder uma situação de desvio não contemplada, por exemplo. De forma análoga, seria interessante uma metodologia para determinação de procedimentos de *bypass* e para rearme de SIFs.

Também propõe-se a análise da possibilidade de implementação de algumas das recomendações apresentadas no HAZOP para aumentar o grau de segurança da UEEM.

REFERÊNCIAS

[1] ALMEIDA, C. M. *Projeto de uma Unidade para Pesquisa de Medição e Controle de Escoamento Multifásico*. 2009. Relatório de Estágio – Universidade Federal de Santa Catarina, Florianópolis, 2009.

[2] AMERICAN PRETROLEUM INSTITUTE. API RP 14C: Recommended Practice for Design, Installation, and Testing of Basic Surface Safety Systems for Offshore Production Platforms. 7 ed. 2001.

[3] BOFF, G. S. *Projeto de Intertravamento da Unidade de Pesquisa de Medição e Controle de Escoamento Multifásico*. 2011. Relatório de Estagio – Universidade Federal de Santa Catarina, Florianópolis, 2011.

[4] BUDDARAJU, D. *Performance of Control Room Operators in Alarm Management*. 2011. Tese – Louisiana State University and Agricultural and Mechanical College, 2011.

[5] DIAS, M. A. *Automação de uma Unidade de Experimentação de Escoamento Multifásico utilizando tecnologia Foundation Fieldbus*. 2015. Dissertação – Universidade Federal de Santa Catarina, Florianópolis, 2015.

[6] Emergency Shutdown Valve Closure Time? Disponível em: http://www.theiet.org/forums/forum/messageview.cfm?catid=205&threadid=102823. Acesso em: 10 de julho 2017.

[7] GRUHN, P.; CHEDDIE, H. L. Safety Instrumented Systems: Design, Analysis, and Justification. 2 ed. EUA: ISA, 2006.

[8] HEALTH & SAFETY EXECUTIVE. Proposal for requirements for low complexity safety related systems. Reino Unido: HSE, 2002

[9] ISA. TR84.00.02-2002 – Part 2. Safety Instrumented Functions (SIF) –Safety Integrity Level (SIL) Evaluation Techniques Part 2: Determining the SIL of a SIF via Simplified Equations. EUA: ISA, 2002.

[10] OREDA. Offshore Reliability Data Handbook. 4 ed. OREDA, 2002.

[11] PETROBRÁS. DR-ENGP-I-1.3 – R.3: Diretrizes de Engenharia de Produção E&P. Filosofia de Segurança. 2013.

[12] PETROBRÁS. N-2595: Critérios de Projeto, Operação e Manutenção de Sistemas Instrumentados de Segurança em Unidades Industriais. 2015.

APÊNDICE A – RELATÓRIO HAZOP

i. Tabelas HAZOP

	HAZOP - ESTUDO DE PERIGOS E OPERABILIDADE			Data:	05/2017
Unidade:	LEEM	Processo:	UEEM	Página:	1 de 3
Nó:	T1		Documento (com revisão):		1
Desvio	Causas	Consequências	(D) Detecção (S) Salvaguarda	Recomendações Observações	Cenário
PRESSÃO MAIOR	Válvula de controle de pressão falha CLOSED	Danos aos instrumentos; ruptura tubulação; ruptura e explosão do tanque	(D) SSC indicador de pressão (S) PSV	#R001; #R002; #R003; #R004	FF detecta Device Failure em T1; FF troca controle para Manual; sem possibilidade de aliviar pressão; pressão excede o limite;
	Falha sensor de pressão		(S) PSV	#R001; #R002; #R003; #R004	FF detecta Instrument Failure em T1; FF troca controle para Manual; válvula na última posição válida; pressão sobe com a diferença de entrada/saída de fluido
	Controle em malha aberta		(D) SSC indicador de pressão (S) PSV	#R005;	Erro operacional; controle deixado no modo Manual; pressão aumenta com a diferença de entrada/saída de fluido;
	Obstrução da tubulação de controle de saída de ar		(D) SSC indicador de pressão (S) PSV	#R001; #R002; #R003; #R004	Controle automatico funcionando mas pressão não responde; sem possibilidade de aliviar pressão;
	Válvula manual de entrada do filtro de ar CLOSED		(D) SSC indicador de pressão (S) PSV	#R001; #R002; #R003; #R004	Erro operacional; controle automático funciona mas pressão não responde; sem possibilidade de aliviar pressão;
	Válvula manual de saída direta de ar CLOSED		(D) SSC indicador de pressão (S) PSV	#R001; #R002; #R003; #R004	Erro operacional; controle automático funciona mas pressão não responde; sem possibilidade de aliviar pressão;
PRESSÂO MENOR	Válvula de controle de pressão falha OPEN	Para pressão muito baixa, há acúmulo de liquido; pode ocorrer refluxo	(D) SSC indicador de pressão	#R001; #R002; #R003	FF detecta Device Failure; FF troca controle pressão para Manual; sem possibilidade de aumentar pressão;
	Falha sensor de pressão			#R001; #R002; #R003	FF detecta Instrument Failure; FF troca controle para Manual; válvula na última posição válida; pressão diminui com a diferença de entrada/saída de fluido
	Falha do C1		(D) SSC indicador de pressão	#R001; #R002; #R003; #R012	Pressão diminui com a diferença de entrada/saída de fluido;
TEMPERATURA MAIOR	Mudança de temperatura do fluido	N/R			
TEMPERATURA MENOR	Mudança de temperatura do fluido	N/R			
FLUXO MAIOR	Cenário de PRESSÃO MAIOR	N/R			
FLUXO MENOR	Falha de C1	N/R			

	HAZOP - ESTUDO DE PERIGOS E OPERABILIDADE			Data:	05/2017
Unidade:	LEEM	Processo:	UEEM	Página:	2 de 3
Nó:	T1		Documento (com revisão):		1
Desvio	Causas	Consequências	(D) Detecção (S) Salvaguarda	Recomendações Observações	Cenário
FLUXO NULO SAIDA	Obstrução da tubulação de saída de fluido	Aumento sem controle do nivel			SSC funciona mas Nivel não responde ao controle;
	Válvula manual de bypass fechada			#R008	Falha Operacional; SSC funciona mas Nivel não responde ao controle
	Válvula de entrada de T2 falha CLOSED			#R001; #R002	Seleção de escoamento Água-Óleo ou Água-Óleo-Ar; válvula falha fechada; único caminho de saída
	Válvula de saída para T4 falha CLOSED			#R001; #R002	Seleção de escoamento Água; válvula falha fechada; único caminho de saída
	Válvula de saída T5 falha CLOSED			#R001; #R002	Seleção de escoamento Óleo; válvula falha fechada; único caminho de saída
FLUXO REVERSO	Queda de energia	Refluxo do fluido que estiver na altura da entrada do tanque		#R006	Válvulas entram em Fault-State; pressão dentro do tanque gera refluxo do fluido que estiver na altura da tubulação de entrada (ar ou líquido)
CONTAMINAÇÃO	N/A				
NIVEL MAIOR	Falha da válvula de controle CLOSED	Tanque overfill	(D) SSC indicador de nivel; (S) Função Automática (S) SIS	#O001; #R003	FF detecta Device Failure; FF muda controle Nivel para Manual; sem possibilidade de diminuir nivel
	Falha sensor de nivel		(D/S) Sensor redundante de nivel; (S) Função Automática; (S) SIS	#O001; #R003	FF detecta Instrument Failure; FF muda controle nivel para Manual; aumento de nivel depende de entrada/saída de fluido
	Cenários de FLUXO NULO na saída		(D) SSC indicador de nivel; (S) Função Automática; (S) SIS	#R003	Sem fluxo de saída, há acumulo de fluido; sem possibilidade de diminuir nivel
	Cenários de PRESSÃO MENOR		(D) SSC indicador de nivel; (S) Função Automática; (S) SIS		Sem pressão para enviar fluido para T2; sem possibilidade de diminuir nivel
NIVEL MENOR	Falha da válvula de controle OPEN	T1 esvazia	(D) SSC indicador de nivel; (S) SIS	#O002	FF detect Device Failure; FF muda controle para modo Manual;
	Falha do sensor de nivel em HIGH		(S) SIS	#O002	FF detect Device Failure; FF muda controle Nivel para Manual; nivel diminui com a diferença de entrada/saída

	HAZOP - ESTUDO DE PERIGOS E OPERABILIDADE			Data:	05/2017
Unidade:	LEEM	Processo:	UEEM	Página:	3 de 3
Nó:	T1		Documento (com revisão):		1
Desvio	Causas	Consequências	(D) Detecção (S) Salvaguarda	Recomendações Observações	Cenário
NIVEL DE INTERFACE MAIOR	N/A				
NIVEL DE INTERFACE MENOR	N/A				
COMUNICAÇÃO NULA	Queda da rede FF	Instrumentos e elementos finais mantém última configuração válida	(D) FF alarme (S) FF hot backup	#R007; #R011	FF faz switch para Mestre backup
	Queda da rede HSE			#O003; #R011	Sem comunicação com o sistema supervisório; instrumentos e elementos finais entram em Fault-State
	Falha do SSC/IHM			#R002	Falha no software ou IHM; sem comunicação, instrumentos e elementos finais entram em Fault-State
ALIMENTAÇÃO INSTRUMENTAÇÃO NULA	Falha do sistema de ar comprimido para instrumentação	Sistema inteiro em malha aberta	(D) SSC	#O004; #R001	Elementos finais entram em Fault-State; FF detecta Device Failure; controles mudam para Manual
ALIMENTAÇÃO ENERGIA NULA	Queda de energia			#R002; #R010	Elementos finais entram em modo de segurança
N/A: Não Aplicável; N/R: Não Relevante; N/P: Não Possível					

	HAZOP - ESTUDO DE PERIGOS E OPERABILIDADE			Data:	05/2017
Unidade:	LEEM	Processo:	UEEM	Página:	1 de 2
Nó:	T2		Documento (com revisão):		1
Desvio	Causas	Consequências	Detecção (D) Salvaguardas (S)	Recomendações Observações	Cenário
PRESSÃO MAIOR	NIVEL MAIOR; tanque *overfill*	Danos aos equipamentos	N/P		Nível sobe pressionando tampa superior do tanque; Líquido transborda
PRESSÃO MENOR	N/A				
TEMPERATURA MAIOR	temperatura do fluido	N/R		#O004	
TEMPERATURA MENOR	temperatura do fluido	N/R		#O004	
FLUXO MAIOR	Rotação das bombas acima do especificado	T4 e T5 recebem os líquidos misturados	(D) SSC indicador de fluxo da linha de água; (D) N/P para linha de óleo	#R002	Com 100% de rotação de cada bomba, água e óleo não se separam em T2; dinâmica moderada
FLUXO MENOR	N/R				
FLUXO NULO ENTRADA	Falha do SSC de pressão ou nivel de T1	N/R	N/P	#R001; #R002	Fluido não consegue chegar à T2; desvios em T1
	Tubulação de entrada obstruída	N/R			Fluido não consegue chegar à T2; desvios em T1
	Válvula de seleção na entrada de T2 falha CLOSED	N/R		#R001; #R002	Seleção de operação Água-Óleo
FLUXO REVERSO	N/R				
CONTAMINACAO	Tampa do tanque T2 aberta	Partículas externas podem vir a obsruir ou danificar a tubulação		#R013	Erro Operacional
NIVEL MAIOR	Obstrução de saída de óleo		(S) SIS	#R001; #R002; #R003	Acumulo da camada de óleo; óleo transborda
NIVEL MENOR	Erro na malha de controle de nivel de interface	Contaminação do tanque T4 por óleo		#R001; #R002; #R003	Tanque esvazia; camada de óleo alcança a saída de água
NIVEL DE INTERFACE MAIOR	Válvula de controle falha CLOSED	Queda do controle automatico de nivel de interface; contaminação do tanque T5 por água;	SSC indicador de nivel de interface	#R001; #R002;	FF detecta Bad: Device Failure; controle passa para modo Manual; fuga da faixa de operação do sensor de nivel de interface; emulsão alcança a saída de óleo; contaminação do tanque T5; sem possibilidade de controlar nivel de interface
	Sensor de nivel de interface falha LOW			#R001; #R002;	FF detecta Bad: Instrument Failure; controle passa para modo Manual; nivel de interface em malha aberta
	Válvula de seleção na saída de T2 falha CLOSED			#R001; #R002;	SSC funciona mas nivel não responde; sem possibilidade de controlar nivel de interface
	Obstrução da saída de água				Sem possibilidade de controlar nivel de interface

	HAZOP - ESTUDO DE PERIGOS E OPERABILIDADE			Data:	05/2017
Unidade:	LEEM	Processo:	UEEM	Página:	2 de 2
Nó:	T2		Documento (com revisão):		1
Desvio	Causas	Consequências	Detecção (D) Salvaguardas (S)	Recomendações Observações	Cenário
NIVEL DE INTERFACE MENOR	Válvula de controle falha OPEN	Passagem de óleo para T4	SSC indicador de nivel de interface	#R001; #R002;	FF detecta Bad: Device Failure; controle passa para modo Manual; fuga da faixa de operação do controle de nivel de interface; camada de emulsão alcança a saída de água; contaminação do tanque T4
	Sensor de nivel de interface falha HIGH			#R001; #R002;	FF detecta Bad: Device Failure; controle passa para modo Manual; nivel de interface em malha aberta
	Válvula de seleção (saída) falha OPEN			#R001; #R002;	FF detecta Bad: Device Failure
COMUNICAÇÃO NULA	Queda da rede FF	Instrumentos e elementos finais mantém última configuração válida	(D) FF alarme (S) FF hot backup	#R007; #R011	FF faz switch para Mestre backup
	Queda da rede HSE			#O003; #R011	Sem comunicação com o sistema supervisório; instrumentos e elementos finais entram em Fault-State
	Falha do SSC/IHM			#R001; #R002;	Falha no software ou IHM; sem comunicação, instrumentos e elementos finais entram em Fault-State
ALIMENTAÇÃO INSTRUMENTAÇÃO NULA	Falha do sistema de ar comprimido para instrumentação	Sistema inteiro em malha aberta	(D) SSC	#O004; #R001	Elementos finais entram em Fault-State; FF detecta Device Failure; controles mudam para Manual
ALIMENTAÇÃO ENERGIA NULA	Queda de energia			#R002; #R010	Elementos finais entram em modo de segurança
N/A: Não Aplicável; N/R: Não Relevante; N/P Não Possível					

	HAZOP - ESTUDO DE PERIGOS E OPERABILIDADE			Data:	05/2017
Unidade:	LEEM	Processo:	UEEM	Página:	1 de 1
Nó:	T3		Documento (com revisão):		1
Desvio	Causas	Consequências	Detecção (D) Salvaguardas (S)	Recomendações Observações	Cenário
PRESSÃO MAIOR	Falha do sistema do compressor	ruptura, vazamento de óleo; explosão; danos à tubulação	(D) Indicador local de pressão (S) PSV	#R014	
PRESSÃO MENOR	Falha do compressor C1	PRESSÃO MENOR em T1	SSC indicador de pressão em T3	#R012; #R001; #R002	Queda de pressão em T1
	Compressor desligado			#R012	Erro Operacional; sem pressão em T1
TEMPERATURA MAIOR	falha do relé de segurança do compressor	superaquecimento do compressor; explosão		#R014	
TEMPERATURA MENOR	temperatura ambiente	N/R			
FLUXO MAIOR	N/A				
FLUXO MENOR	N/A				
FLUXO NULO	Falha da válvula CLOSED em T3	PRESSÃO MENOR em T1	SSC indicador de fluxo em T3	#R015	Sem possibilidade de controlar pressão
	Válvula solenóide de seleção do tipo de escoamento falha CLOSED			#R001	Queda na pressão em T1; sem possibilidade de controlar pressão
FLUXO REVERSO	PRESSÃO MENOR da linha de ar comprimido	Entrada de fluido pela tubulação de ar (LCA)	(S) Valvula de retenção	#R006	Pressão baixa da linha de ar permitindo o refluxo de líquido a partir do misturador primário (LCA)
	Tanque "*overfill*"	Entrada de fluido pela tubulação de ar	(S) Valvula de retenção	#R006	Tanque *overfill*; passagem de líquido para a tubulação de ar
CONTAMINAÇÃO	Partículas externas	Falha do compressor; explosão		#R014	Entrada de partículas externas no compressor
NIVEL MAIOR	N/A				
NIVEL MENOR	N/A				
NIVEL DE INTERFACE MAIOR	N/A				
NIVEL DE INTERFACE MENOR	N/A				
N/A: Não Aplicável; N/R: Não Relevante; N/P: Não Possível					

	HAZOP - ESTUDO DE PERIGOS E OPERABILIDADE			Data:	05/2017
Unidade:	LEEM	Processo:	UEEM	Página:	1 de 2
Nó:	T4		Documento (com revisão):		1
Desvio	Causas	Consequências	Detecção (D) Salvaguardas (S)	Recomendações Observações	Cenário
PRESSÃO MAIOR	Fluxo nulao na saída de T4	Danos à bomba, fissura em dutos	(S) circuito fechado de recirculação		Aumento da pressão da linha de água
PRESSÃO MENOR	N/R				
TEMPERATURA MAIOR	temperatura da água	N/R			
TEMPERATURA MENOR	temperatura da água	N/R			
FLUXO MAIOR	N/A				
FLUXO MENOR					Considerar casos de FLUXO NULO
FLUXO NULO ENTRADA	Falha do sistema de controle de interface em T2	NIVEL MENOR em T2			Falha em T2; fluxo de água interrompido
	Válvula de seleção do tipo de escoamento da saída de T2 falha CLOSED				Tanque T4 esvazia, danos à bomba
	Válvula de seleção do tipo de escoamento da entrada de T4 falha CLOSED				Tanque T4 esvazia, danos à bomba
	Obstrução da tubulação de saida de água de T2				Desvios em T2; Tanque T4 esvazia, danos à bomba
	Obstrução da tubulação de entrada de T4				Desvios em T1; Tanque T4 esvazia; danos à bomba
FLUXO NULO SAÍDA	Válvula de seleção do tipo de escoamento da saída de T4 falha CLOSED	N/R	(S) Circuito de recirculação de água	#R001; #R003	Com fluxo nos dutos interrompido, a água começa a passar pelo circuito de recirculação
	Mal configuração da válvula manual da saída de T4			#R008	Erro Operacional; válvula de bypass fechada; bomba não consegue puxar água do tanque; bomba trabalha com água no circuito de recirculação
	Falha da bomba B1				Sistema operando temporiamente como escoamento sem água
	Obstrução da tubulação de saída				Sistema operando temporiamente como escoamento sem água
FLUXO REVERSO	Refluxo do LCA			#R016	
CONTAMINAÇÃO	Falha do controle de interface de T2	Passagem de óleo para T4		#R001; #R003	Óleo entra pela tubulação de água
	Tampa do tanque T4 aberta	Partículas externas podem vir a obstruir ou a danificar a tubulação		#R013	Erro operacional
	Válvula de seleção do tipo de escoamento na saída de T5 falha OPEN	Passagem de óleo para T4			Óleo dos dutos se mistura com água cirulando no sistema
	Válvula de seleção do tipo de escoamento na entrada de T4 falha OPEN	Passagem de óleo para T4			Modo Operação: Óleo ou Ar-Óleo-Água;

	HAZOP - ESTUDO DE PERIGOS E OPERABILIDADE			Data:	05/2017
Unidade:	LEEM	Processo:	UEEM	Página:	2 de 2
Nó:	T4		Documento (com revisão):		1
Desvio	Causas	Consequências	Detecção (D) Salvaguardas (S)	Recomendações Observações	Cenário
NÍVEL MAIOR	CONTAMINAÇÃO por óleo em T4	T4 transborda (água)	(S) SistSeg		Óleo entra no circuito de água elevando o volume total da porção de água do sistemam
NIVEL MENOR	Fluxo nulo de entrada	danos à B1	(S) SistSeg	#R002	T4 esvazia; B1 trabalha em vazio
	Preenchimento do tanque abaixo da capacidade segura		(S) SistSeg	#R017	Erro Operacional; T4 esvazia; B1 trabalha em vazio
	Válvula manual de escape para o fosso OPEN		(S) SistSeg	#R008	Erro Operacional; T4 esvazia; B1 trabalha em vazio
NIVEL DE INTERFACE MAIOR		N/R			
NIVEL DE INTERFACE MENOR		N/R			
N/A: Não Aplicável; N/R: Não Relevante; N/P: Não Possível					

	HAZOP - ESTUDO DE PERIGOS E OPERABILIDADE			Data:	05/2017
Unidade:	LEEM	Processo:	UEEM	Página:	1 de 1
Nó:	T5		Documento (com revisão):		1
Desvio	Causas	Consequências	Detecção (D) Salvaguardas (S)	Recomendações Observações	Cenário
PRESSÃO MAIOR	N/R		(S) Circuito fechado de recirculação		
PRESSÃO MENOR	N/R				
TEMPERATURA MAIOR	Temperatura do óleo	N/R			
TEMPERATURA MENOR	Temperatura do óleo	N/R			
FLUXO MAIOR	N/A				
FLUXO MENOR					Considerar casos de FLUXO NULO
FLUXO NULO ENTRADA	Válvula de seleção do tipo de escoamento da entrada de T5 falha CLOSED	NIVEL MENOR em T5			T5 esvazia; danos à bomba
	Obstrução da tubulação de entrada				T5 esvazia; danos à bomba
FLUXO NULO SAÍDA	Válvula de seleção do tipo de escoamento da saída de T5 falha CLOSED	N/R	(S) Circuito fechado de recirculação	#R001; #R003	Com fluxo nos dutos interrompido, o óleo começa a passar pelo circuito de recirculação
	Mal configuração da válvula manual da saída de T5	N/R		#R008	Erro Operacional; válvula de bypass fechada; bomba não consegue puxar óleo do tanque; bomba trabalha com óleo no circuito de recirculação
	Falha da bomba B2	N/R			Sistema operando temporariamente como escoamento sem óleo
	Obstrução da tubulação de saída de T5	N/R			Sistema operando temporariamente como escoamento sem óleo
FLUXO REVERSO	Refluxo do LCA			#R018	
CONTAMINAÇÃO	Falha SSC em T2	Entrada de água em T5		#R001; #R003	Interface de água invade tubulação de óleo
	Tampa do tanque T5 aberta	Partículas externas podem vir a obstruir ou danificar a tubulação		#R013	Erro Operacional
	Válvula de seleção do tipo de escoamento falha OPEN	Entrada de água em T5			FF detecta Bad: Device Failure; válvula de seleção da saída T4 aberto (misturando no LCA) e/ou retorno T1 aberto (misturando em T5)
NÍVEL MAIOR	CONTAMINAÇÃO por água em T5	T5 transborda (óleo)	(S) SIS		Água entra no circuito de óleo elevando o volume total da porção de óleo do sistema
NIVEL MENOR	Fluxo nulo de entrada	danos à B2	(S) SIS	#R002	T5 esvazia; B2 trabalha em vazio
	Preenchimento do tanque abaixo da capacidade segura	danos à B2	(S) SIS	#R017	Erro Operacional; T5 esvazia; B2 trabalha em vazio
	Válvula manual de escape para fosso OPEN	danos à B2	(S) SIS	#R008	Erro Operacional; T5 esvazia; B2 trabalha em vazio
NIVEL DE INTERFACE MAIOR		N/R			
NIVEL DE INTERFACE MENOR		N/R			
N/A: Não Aplicável; N/R: Não Relevante; N/P: Não Possível					

	HAZOP - ESTUDO DE PERIGOS E OPERABILIDADE			Data:	05/2017
Unidade:	LEEM	Processo:	UEEM	Página:	1 de 1
Nó:	LCA - Sala de medições		Documento (com revisão):		1
Desvio	Causas	Consequências	Detecção (D) Salvaguardas (S)	Recomendações Observações	Cenário
PRESSÃO MAIOR	Falha Operacional: válvula manual de saída fechada	Vazamentos/danos à tubulação, fluido entra em contato com operador e instrumentos, danos a instrumentos, perda de fluido		#R019	Válvulas manuais fechadas, fluxo de fluido sem passagem, pressão interna à tubulação aumenta
	Falha Operacional: válvula manual de entrada fechada			#R008	
	Casos de Fluxo Maior				
PRESSÃO MENOR	N/R				
TEMPERATURA MAIOR	N/R				
TEMPERATURA MENOR	N/R				
FLUXO MAIOR	N/R				
FLUXO MENOR	N/R				
FLUXO NULO	N/R				
FLUXO REVERSO	Fluxo reverso de T1	Invasão dos dutos de alimentação por fluidos diferentes, aumento na pressão interna dos dutos invadidos, danos aos instrumentos	(S) Válvula direcional na linha de ar	#R006	Ocorrência de fluxo reverso proveniente de T1, fluido retorna podendo invadir os dutos individuais antes do misturador, aumento da pressão interna
CONTAMINAÇÃO	N/R				
NIVEL MAIOR	N/A				
NIVEL MENOR	N/A				
NIVEL DE INTERFACE MAIOR	N/A				
NIVEL DE INTERFACE MENOR	N/A				
N/A: Não Aplicável; N/R: Não Relevante; N/P: Não Possível					

ii. Recomendações

#R001: Projetar alarme de falha. Falhas detectadas por diagnóstico de instrumentos inteligentes ou pela rede de campo devem ser apresentadas ao usuário através da IHM

#R002: Desenvolver sistema de alarmes para a casa de utilidades. O operador deve ser capaz de reconhecer o acontecimento e identificar o tipo de desvio mesmo estando na casa de utilidades e longe do IHM.

#R003: Avaliar projeto de SIF. Levar processo a um estado seguro caso haja desvios perigosos

#R004: Ajustar PSV para um valor limite maior de modo a aproveitar melhor a faixa de operação do tanque de pressão (e permitir utilização do ponto de operação especificado em projeto)

#R005: Dar prioridade para a visualização do modo de operação do controle. O operador deve ser capaz de visualizar rapidamente o estado do modo de operação (automático ou manual) das malhas de controle.

#R006: Instalar válvulas de retenção nas linhas de ar comprimido (FA02) e de saída do tanque T1 (FA07) para evitar o refluxo

#R007: Gerar alarmes devido a erros na rede de campo. Como instrumentos estão programados para manter a última configuração válida, erros podem passar despercebidos. Se possível, gerar registro de falhas de rede automaticamente.

#R008: Monitorar posição das válvulas manuais. Instalar cadeados de proteção ou instrumentar válvulas manuais para monitoramento

#R009: Utilizar função automática para limitar a vazão total fornecida em conjunto pelas duas bombas. Proteger acesso contra modificações sem autorização.

#R010: Utilizar redundância dos cabeamento de energia do sistema

#R011: Utilizar redundância dos cabeamento de rede

#R012: Instrumentar sistema do compressor de ar (compressor C1 e tanque T3) para monitoramento

#R013: Utilizar procedimentos e/ou proteções físicas para evitar entrada de partículas estranhas ao sistema que possam danificar instrumentos ou prejudicar a operação da planta.

#R014: Garantir manutenção em dia do compressor.

#R015: Implementar malha de controle em T3.

#R016: Investigar a necessidade de instalar uma válvula de retenção na linha de água para proteger contra possíveis refluxos provindos da sala de medições

#R017: Criar procedimentos para inicialização correta do sistema (quantidade de água e óleo necessários, pontos de operação, etc.)

#R018: Investigar a necessidade de instalar uma válvula de retenção na linha de óleo para proteger contra possíveis refluxos provindos da sala de medições

#R019: Realizar estudos de técnicas de monitoramento e detecção de vazamentos em tubulações. Verificar API RP 1130 ou TRFL.

iii. Observações

#O001: Função automática implementada no SSC presente. Quando nível é detectado com 80% da altura máxima, há a redução da rotação das bombas para 10%.

#O002: Proteção contra nível baixo em T1 incompatível com modo de escoamento do tipo Ar quando T1 estiver sem líquido.

#O003: Garantir configuração correta dos dispositivos de campo (procedimentos, máscaras de programação, etc.). Cuidado especial para o modo de falha para alarmes, queda de comunicação, queda de ar de instrumentação, queda de energia de alimentação.

#O004: O sensor de densidade DT302 possui compensação de temperatura.

iv. Outras recomendações

Garantir que todos os dispositivos estejam devidamente configurados, principalmente seus modos de falha devido à perda de alimentação elétrica, comunicação e alimentação pneumática para instrumentação.

APÊNDICE B – TABELA LOPA

#	ID	Descrição			Severidade Maxima	Frequência Tolerável	Frequencia do cenário	IPL	PFD da IPL	Frequência da Consequência	RRF	SIL
001		Falha CLOSED da válvula de controle de pressão	tanque T3 continua a enviar ar comprimido, pressão interna em T1 aumenta além da capacidade máxima, danos aos instrumentos em T1	explosão do tanque T1, danos estruturais ao laboratório, danos a outros equipamentos do laboratório, fatalidades	V	1.0E-5	.04555	PSV	0.01	0.0004555	46	SIL 1
002					V	1.0E-5	.04555	PSV	0.01	0.0004555	46	SIL 1
003		Falha sensor de pressão em T1			V	1.0E-5	.00555	PSV	0.01	0.0000555	6	a
004					V	1.0E-5	.00555	PSV	0.01	0.0000555	6	a
005		Obstrução dos dutos de saída de ar do controle de pressão			V	1.0E-5		PSV	0.01			
006				fissuras nos dutos/equipamentos despressurizam T1	V	1.0E-5		PSV	0.01			
007		Falha operacional: válvula manual de saída de ar fechada			V	1.0E-5		PSV	0.01			
008					V	1.0E-5		PSV	0.01			
009		Falha operacional : válvula da linha do filtro de ar fechada			V	1.0E-5		PSV	0.01			
010					V	1.0E-5		PSV	0.01			
011		Falha operacional: controle pressão de T1 em malha aberta	pressão interna em T1 aumenta de acordo com variação de entrada/saída de fluido até ultrapassar a capacidade máxima, danos aos instrumentos em T1	explosão do tanque T1, danos estruturais ao laboratório, danos a outros equipamentos do laboratório, fatalidades	V	1.0E-5		PSV	0.01			
012				fissuras nos dutos/equipamentos despressurizam T1	V	1.0E-5		PSV	0.01			
013		Falha CLOSED da válvula de controle de nivel	fluido acumula em T1,nivel alcança capacidade máxima, invasão do duto de ar por liquido, aumento da pressão interna nas linhas, danos aos instrumentos em T1, vazamento por fissuras em conexões/equipamentos, inundação do laboratório, danos a outros equipamentos do laboratório		III	1.0E-3	.0763			0.0762996	76	SIL 1
014		Obstrução do duto de saída de fluido em T1			III	1.0E-3						
015		Falha operacional: válvula manual da linha de saída de fluido fechada			III	1.0E-3		Função Automática de Nivel	0.1			
016		Modo Água-Óleo ou Água-Óleo-Ar, válvula de seleção para T2 falha CLOSED			III	1.0E-3	.04275	Função Automática de Nivel	0.1	0.0042749	4	a
017		Modo Água, válvula de seleção para T4 falha CLOSED			III	1.0E-3	.04275	Função Automática de Nivel	0.1	0.0042749	4	a
018		Modo Óleo, válvula de seleção para T5 falha CLOSED			III	1.0E-3	.04275	Função Automática de Nivel	0.1	0.0042749	4	a
019		Pressão insuficiente em T1			III	1.0E-3	.15778	Função Automática de Nivel	0.1	0.0157779	16	SIL 1
020			IPL mitigadora não impede o refluxo		III	1.0E-3	.15778		0.01	0.0015778	2	a
021			IPL mitigadora impede o refluxo		III	1.0E-3	.15778	Função Automática de Nivel; Válvula de retenção	0.099	0.0156201	16	SIL 1
022		Falha operacional: controle de nivel em T1 em malha aberta	nivel em T1 aumenta de acordo com variação de entrada/saída de fluido, alcançada capacidade máxima, invasão do duto de ar por liquido, aumento da pressão interna nas linhas, danos aos instrumentos em T1, vazamento por fissuras em conexões/equipamentos, inundação do laboratório, danos a outros equipamentos do laboratório		III	1.0E-3		Função Automática de Nivel	0.1			
023		Falha sensor de nivel em T1			III	1.0E-3	.02036			0.0203590	20	SIL 1
024		Falha OPEN da válvula de controle de pressão em T1	pressão interna em T1 atinge o mínimo, fluido não consegue ser enviado e acumula em T1				.05966			0.0596556		
025		Modo Água-Ar, Óleo-Ar ou Água-Óleo-Ar: Seleção do tipo de escoamento, válvula de saída de ar em T3 falha CLOSED					.04275			0.0427488		
026		Modo Água ou Óleo: Seleção do tipo de escoamento, válvula de saída de ar em T3 falha CLOSED					.04275			0.0427488		
027		Modo Água ou Óleo: Falha Operacional: válvula manual de saída de ar fechada										
028		Modo Água-Ar, Óleo-Ar ou Água-Óleo-Ar: Falha operacional: válvulas manuais da linha de ar fechadas										
029		Falha do sensor de pressão em T1	pressão interna cai de acordo com variações de entrada/saída de fluido até atingir o mínimo, fluido não consegue ser enviado e acumula em T1				.00555			0.0055546		
030		Falha no compressor de Ar	falha da IPL mitigadora				.26683		0.0265	0.0070710		
031			SIF 008 funciona como IPL mitigadora				.26683	SIF008	0.9735	0.2597586		

032	Falha operacional: rotações das bombas acima do especificado	separação de óleo e água não ocorre completamente, passagem de emulsação (água e óleo) para o tanque T4, contaminação do tanque de armazenamento de água T4		II	1.0E-2							
033	Falha CLOSED da válvula de controle de nível de interface em T2		mistura acumula em T2, passagem de emulsão (água e óleo) para o tanque T5, contaminação do tanque de armazenamento de óleo T5	II	1.0E-2	.0763			0.0762996		8	a
034	Falha do sensor de nível de interface em T2			II	1.0E-2	.0378			0.0378009		4	a
035	Modo Água-Óleo ou Água-Óleo-Ar, válvula de seleção na saída de T2 falha CLOSED			II	1.0E-2	.04275			0.0427488		4	a
036	Obstrução da saída de água de T2			II	1.0E-2							
037	Modo Água ou Água-Ar, Óleo, Óleo-Ar: válvula seleção de operação na entrada de T2 falha OPEN	água aumenta o nível do tanque T2, controle tenta corrigir mas válvula de saída de seleção de operação CLOSED		II	1.0E-2	.04275			0.0427488		4	a
038	Obstrução da saída de óleo de T2, nivel aumenta em T2, óleo transborda			III	1.0E-3	.09408			0.0940824		94	SIL 1
039	Falha OPEN da válvula de controle de nível de interface em T2	tanque começa a esvaziar, camada de emulsão alcança a saída de água	contaminação do tanque T4 e transbordamento	III	1.0E-3	.09592			0.0959220		96	SIL 1
040	Falha do sensor de nível de interface em T2	tanque esvazia de acordo com a relação vazão entrada/saída		III	1.0E-3	.0378			0.0378009		38	SIL 1
041	Acumulo de líquido em T2	desvios em T2	tanque T4 esvazia, danos à bomba	IV	1.0E-4	.29368			0.2936805		2937	SIL 3
042	Aucumulo de líquido em T1	fluxo nulo para T4, desvio de nível em T1		IV	1.0E-4	.12577			0.1257722		1258	SIL 3
043	Falha operacional: preenchimento do tanque T4 abaixo do mínimo especificado em projeto			IV	1.0E-4							
044	Falha operacional: válvula manual de escape para fosso aberta			IV	1.0E-4							
045	Acumulo de líquido em T2	desvios em T2	tanque T5 esvazia, danos à bomba	IV	1.0E-4	.29368			0.2936805		2937	SIL 3
046	Aucumulo de líquido em T1	fluxo nulo para T5, desvio de nível em T1		IV	1.0E-4							
047	Falha operacional: preenchimento do tanque T5 abaixo do mínimo especificado em projeto			IV	1.0E-4							
048	Falha operacional: válvula manual de escape para fosso aberta			IV	1.0E-4							
049	Falha operacional: válvula manual de saída da sala de medições fechada, pressão na linha aumenta, vazamento pelas conexões, fissura dos dutos, inundação da sala			IV	1.0E-4							
050	Modo Água ou Água-Ar: válvula seleção de operação na entrada de T5 falha OPEN	passagem de água para T5	contaminação do tanque T5	II	1.0E-2	.04275			0.0427488		4	a
051	Modo Água-Óleo-Ar: válvula seleção de operação na entrada de T5 falha OPEN	passagem de mistura para T5	contaminação e transbordamento de T5	II	1.0E-2	.04275			0.0427488		4	a
052	Modo Óleo ou Óleo-Ar: válvula seleção de operação na entrada de T4 falha OPEN	passagem de óleo para T4	contaminação do tanque T4	II	1.0E-2	.04275			0.0427488		4	a
053	Modo Água-Óleo-Ar: válvula seleção de operação na entrada de T4 falha OPEN	passagem de mistura para T4	contaminação e transbordamento de T4	II	1.0E-2	.04275			0.0427488		4	a

IPLs Mitigadoras	PFD
SIF de pressão baixa em T3	2.65E-02
SIF de pressão baixa em T1	1.65E-02

APÊNDICE C – MEMÓRIA DE CÁLCULO – VERIFICAÇÃO DE SIL

SIF 001	RRF alvo	90				
	Sensor Pressão	CLP	Circuito B1	Circuito B2	XVT3	PSVT1
Taxa de Falha	5.55E-3	1.00E-3	1.70E-3	1.70E-3	2.51E-2	5.21E-2
PFDavg individual	6.94E-4	1.25E-4	2.13E-4	2.13E-4	3.13E-3	6.52E-3
TI [anos]	0.25					
PFDavg da SIF	1.09E-2	RRF	91.82			

SIF 002	RRF alvo	76			
	Sensor Nível	CLP	Circuito B1	Circuito B2	XVT3
Taxa de Falha	2.04E-2	1.00E-3	1.70E-3	1.70E-3	2.51E-2
PFD individual	5.09E-3	2.50E-4	4.25E-4	4.25E-4	6.26E-3
TI [anos]	0.5				
PFDavg da SIF	1.25E-2	RRF	80.30		

SIF 003	RRF alvo	94				
	Sensor Nível	CLP	Circuito B1	Circuito B2	XVT3	XVT1
Taxa de Falhas	5.03E-2	1.00E-3	1.70E-3	1.70E-3	2.51E-2	2.51E-2
PFD individual	6.29E-3	1.25E-4	2.13E-4	2.13E-4	3.13E-3	3.13E-3
TI [anos]	0.25					
PFDavg	1.31E-2	RRF	76.34			
	[2x] Sensor Nível	CLP	Circuito B1	Circuito B2	XVT3	XVT1
Taxa de Falhas	5.03E-2	1.00E-3	1.70E-3	1.70E-3	2.51E-2	2.51E-2
PFD individual	5.27E-5	1.25E-4	2.13E-4	2.13E-4	3.13E-3	3.13E-3
TI [anos]	0.25					
PFDavg	6.87E-3	RRF	145.64			

SIF 004	RRF alvo	96				
Arq	Sensor Nivel	CLP	Circuito B1	Circuito B2	XVT3	XVT2
Failure Rate	5.03E-2	1.00E-3	1.70E-3	1.70E-3	2.51E-2	2.51E-2
PFDavg individual	6.29E-3	1.25E-4	2.13E-4	2.13E-4	3.13E-3	3.13E-3
TI	0.25					
PFDavg da SIF	1.31E-2	RRF	76.34			
Arq	[2x] Sensor Nivel	CLP	Circuito B1	Circuito B2	XVT3	XVT2
Failure Rate	5.03E-2	1.00E-3	1.70E-3	1.70E-3	2.51E-2	2.51E-2
PFDavg individual	5.27E-5	1.25E-4	2.13E-4	2.13E-4	3.13E-3	3.13E-3
TI	0.25					
PFDavg da SIF	6.87E-3	RRF	145.64			

SIF 005	RRF alvo	2937	
	Sensor Nível	CLP	Circuito B1
Taxa de Falha	8.55E-2	1.00E-3	1.70E-3
PFD individual	1.07E-2	1.25E-4	2.13E-4
TI [anos]	0.25		
PFDavg da SIF	1.10E-2	RRF	90.71
	Sensor Nível	CLP	Circuito B1
Taxa de Falha	8.55E-2	1.00E-3	1.70E-3
PFD individual	1.52E-4	1.25E-4	2.13E-4
TI [anos]	0.25		
PFDavg da SIF	4.90E-4	RRF	2,041.70
			ALARP

SIF 006	RRF alvo	2937	
	Sensor Nível	CLP	Circuito B2
Taxa de Falha	8.55E-2	1.00E-3	1.70E-3
PFD individual	1.07E-2	1.25E-4	2.13E-4
TI [anos]	0.25		
PFDavg da SIF	1.10E-2	RRF	90.71
	Sensor Nível	CLP	Circuito B2
Taxa de Falha	8.55E-2	1.00E-3	1.70E-3
PFD individual	1.52E-4	1.25E-4	2.13E-4
TI [anos]	0.25		
PFDavg da SIF	4.90E-4	RRF	2,041.70
			ALARP

SIF 007	RRF alvo	—	
	Sensor Pressão	CLP	Circuito B1	Circuito B2
Failure Rate	4.86E-2	1.00E-3	1.70E-3	1.70E-3
PFD individual	6.08E-3	1.25E-4	2.13E-4	2.13E-4
TI	0.25			
PFDavg	6.63E-3	RRF	150.89	

APÊNDICE D – FOLHAS DE ESPECIFICAÇÃO DE SIF

UEEM	Folha de Dados	Nº 1	Rev. 1
		Folha 1	de 2
	Especificação SIF-UEEM001		

INFORMAÇÕES GERAIS

Tag:	SIF-UEEM001	**Relatório de Análise de Riscos:**	LOPA: 001 a 012; HAZOP: Nó T1
Descrição da SIF [LOPA]:	Pressão alta em tanque de pressão T1 bloqueia fluxo de entrada de ar comprimido e de entrada de fluidos. Tanque T1 é despressurizado.		
Causas da Demanda [HAZOP]:	Falha na malha de controle de pressão em T1, obstrução de dutos da malha de controle de pressão, falha operacional (válvulas manuais fechadas, controle em modo Manual)		
Consequências da Falha na Demanda [HAZOP]:	Aumento da pressão interna do tanque de pressão T1 com possibilidade de ruptura de equipamentos e/ou explosão, seguido de ferimentos graves/fatalidades, danos estruturais ao laboratório, contaminação do solo ao redor do laboratório		
Consequências do Trip Espúrio [HAZOP/LOPA]:	Interrupção do ensaio. Tanque despressuriza, fazendo-se necessário novo startup da malha de controle de pressão de T1. Fluidos permanecem dentro do tanque.		

REQUISITOS DE PROCESSO E DA ANÁLISE DE RISCO	**Tempo de Segurança de Processo:**		**Tempo de Resposta:** 1,5 s	**Tempo de Retardo:**	
	Intervalo entre Testes Periódicos:	0,25 ano	**MTTR:**		
	RRF Requerido:	90	**SIL Requerido:** SIL 1	**MTTFS Aceitável:**	
RESULTADOS	**RRF Obtido:**	92	**SIL Obtido:** SIL 1	**MTTFS Obtido:**	

INICIADORES

Tag	Descrição dos Iniciadores	Modo de Atuação	Detecção	Valor da Trip
PSH-T1-01	Transmissor de pressão no tanque de pressão T1	Energiza para trip (20 mA)	HH	60 psi (4,2 bar)

ELEMENTOS FINAIS

Tag	Descrição dos Elementos Finais	Modo de Atuação	Estado Seguro
PSV-T1-01	Válvula de alívio para despressurizar T1	Desenergiza para trip (4 mA)	Válvula aberta
XV-FA01-01	Válvula de bloqueio da linha FA01 (ar comprimido)	Desenergiza para trip (4 mA)	Válvula fechada
Desarme B1	Circuito de shutdown da bomba B1	Desenergiza para trip (4 mA)	Circuito aberto
Desarme B2	Circuito de shutdown da bomba B2	Desenergiza para trip (4 mA)	Circuito aberto

EXEC

Tag:	CLP-SIS	**Descrição do Executor da Lógica:**	CLP de Segurança
Módulos de Entrada:		**Módulos de Saída:**	

TRIP MANUAL

Tag	Descrição do Trip Manual	Tipo	Localização

DESCRIÇÃO FUNCIONAL

Descrição da Lógica:

Caso iniciador indicar HH deve-se fechar a válvula de bloqueio de saída de ar comprimido e desligar bombas. Em seguida, despressurizar tanque T1 abrindo válvula de alívio de pressão. Estado dos elementos finais é mantido até que o rearme da SIF seja acionado.

Ações Secundárias:

Caso ainda operante, interromper controle automático da malha de pressão em T1. Demais subsistemas estabilizam com o tempo se respectivos controles continuarem no modo automático.

Descrição do Estado Seguro a ser Atingido ou Mantido:

T1 despressurizado, sem fluxo de entrada de ar comprimido (evitar aumento de pressão)
Sem fluxo de entrada de líquido em T1 (evitar aumento desvios de nivel alto e aumento de pressão)
Controle automático de pressão desligado (evitar ações na malha)
Caso o fluxo de saída de T1 esteja desimpedido, o tanque T1 poderá esvaziar (cenário considerado não perigoso)

ALARMES

Alarme Pré-Trip:	Não	**Descrição:**		**Ponto de Ajuste:**
Alarme Trip:	Sim	**Descrição:**	Alarme para operador via IHM. Alarme na casa de utilidades	
Alarme Desvio:	Sim	**Descrição:**	Alarme para operador via IHM	**Ponto de Ajuste:** delta 0.55 bar
Diagnóstico de Falha:		**[X] Iniciadores**	**[X] Atuadores** **[X] Cartões E/S** **[X] Outros:** CLP	
Outros Alarmes:				

UEEM	Folha de Dados	Nº 1	Rev. 1
		Folha 2	de 2
	Especificação SIF-UEEM001		

REQUISITOS DE IMPLEMENTAÇÃO

BYPASS

Bypass para Manutenção: Sim	**Descrição:** Bloqueio da linha na qual se encontra a válvula de alívio
Cuidados Adicionais:	
Bypass de Início de Operação: Não	**Descrição**
Cuidados Adicionais:	

Procedimento para Rearme: *

Verificar se bombas estão desligadas; Verificar se o controle de pressão e de nível T1 se encontram em modo manual; Manter fechada a válvula de saída de líquido via controle manual do SSC; Se o compressor estiver ligado, manter aberta a válvula de controle de pressão via controle manual do SSC; Rearmar a SIF;
Válvula de alívio de pressão deve fechar e válvulas de bloqueio da saída de T1 e de saída de ar devem abrir. Válvulas de seleção são acionadas de acordo com o tipo de escoamento antes de ocorrer o trip;
Realizar o startup da malha de pressão em T1; Realizar o startup da malha de nível em T1

Ação na Detecção de Falha:	**[X] Trip**	**[ ] Operação em modo degradado**	**Tempo Máx. de Operação em Modo Degradado:**

Descrição do Modo Degradado:

OUTRAS IPLS NECESSÁRIAS	Camadas de Proteção Independentes	RRF
	Válvula de alívio 87 psi (6 bar). Aprox. 90% PMTA	100

Notas e Observações

*Os procedimentos para Rearme são uma sugestão originada a partir do ponto de vista de análise de risco. Necessário verificação e validação.

UEEM	Folha de Dados	Nº 1	Rev. 1
		Folha 1	de 2
	Especificação SIF-UEEM002		

INFORMAÇÕES GERAIS

Tag: SIF-UEEM002	**Relatório de Análise de Riscos:** LOPA: 013 a 023; HAZOP: Nó T1
Descrição da SIF [LOPA]:	Nível alto no tanque de pressão T1 bloqueia entrada de líquido e de ar comprimido.
Causas da Demanda [HAZOP]:	Falha na malha de controle de nível em T1, falha operacional (controle em malha aberta, válvulas manuais fechadas), falha nas válvulas de seleção de modo de operação (fluxo nulo na saída de T1), falha na malha de pressão em T1 ou falha no sistema de ar comprimido (despressurização do tanque).
Consequências da Falha na Demanda [HAZOP]:	Transbordamento do tanque T1, danos a instrumentos em T1, aumento da pressão nos dutos com possibilidade de ruptura, inundação do laboratório, danos a equipamentos próximos a T1, contaminação do solo ao redor do laboratório
Consequências do Trip Espúrio [HAZOP/LOPA]:	Interrupção do ensaio

REQUISITOS DE PROCESSO E DA ANÁLISE DE RISCO	**Tempo de Segurança de Processo:**		**Tempo de Resposta:**	3,5 s	**Tempo de Retardo:**
	Intervalo entre Testes Periódicos:	0,5 ano	**MTTR:**		
	RRF Requerido:	76	**SIL Requerido:**	SIL 1	**MTTFS Aceitável:**
RESULTADOS	**RRF Obtido:**	80	**SIL Obtido:**	SIL 1	**MTTFS Obtido:**

INICIADORES

Tag	Descrição dos Iniciadores	Modo de Atuação	Detecção	Valor da Trip
LSH-MBJ01-01	Transmissor de nível no tanque de pressão T1	Energiza para trip (20 mA)	HH	90% Nivel Max.

ELEMENTOS FINAIS

Tag	Descrição dos Elementos Finais	Modo de Atuação	Estado Seguro
XV-FA01-01	Válvula de bloqueio da linha FA01 (ar comprimido)	Desenergiza para trip (4 mA)	Válvula fechada
Desarme B1	Circuito de shutdown da bomba B1	Desenergiza para trip (4 mA)	Circuito aberto
Desarme B2	Circuito de shutdown da bomba B2	Desenergiza para trip (4 mA)	Circuito aberto

EXEC

Tag: CLP-SIS	**Descrição do Executor da Lógica:**	CLP de Segurança	
Módulos de Entrada:		**Módulos de Saída:**	

TRIP MANUAL

Tag	Descrição do Trip Manual	Tipo	Localização

DESCRIÇÃO FUNCIONAL

Descrição da Lógica:

Caso iniciador indicar HH deve-se desligar bombas para impedir fluxo de entrada de líquidos em T1. Impedir fluxo de ar comprimido para evitar que haja fluxo forçado dos líquidos presentes no duto.
Estado dos elementos finais é mantido até que o rearme da SIF seja acionado.

Ações Secundárias:

Caso ainda operante, interromper controle automático da malha de nivel e de pressão em T1. Demais subsistemas estabilizam com o tempo se respectivos controles continuarem no modo automático.

Descrição do Estado Seguro a ser Atingido ou Mantido:

Sem fluxo de entrada de líquido (impedir agravamento do desvio de nível alto)
Sem fluxo de ar comprimido (impedir fluxo forçado de líquidos)
Controle automático de nível e de pressão em T1 desligados (evitar ações na malha)

ALARMES

Alarme Pré-Trip:	Sim	**Descrição:**	Alarme para operador	**Ponto de Ajuste:**	82% Nivel Max.
Alarme Trip:	Sim	**Descrição:**	Alarme para operador; Sistema de alarme na casa de utilidades		
Alarme Desvio:	Sim	**Descrição:**	Alarme para operador	**Ponto de Ajuste:**	delta 4% Hmax
Diagnóstico de Falha:		**[X] Iniciadores**	**[X] Atuadores** **[X] Cartões E/S**	**[X] Outros:**	CLP
Outros Alarmes:					

UEEM	Folha de Dados	Nº 1	Rev. 1
		Folha 2	de 2
	Especificação SIF-UEEM002		

REQUISITOS DE IMPLEMENTAÇÃO

BYPASS

Bypass para Manutenção:	Não	**Descrição:**
Cuidados Adicionais:	Manutenção realizada apenas com o sistema desligado	
Bypass de Início de Operação:	Não	**Descrição**
Cuidados Adicionais:		

Procedimento para Rearme: *

Verificar se bombas se encontram desligadas; Manter fechada a válvula de saída de líquido via controle manual do SSC; Se o compressor estiver ligado, manter aberta a válvula de controle de pressão via controle manual do SSC; Rearmar SIF;
Válvula de bloqueio da saída de T1 e de ar comprimido devem abrir automaticamente. Válvulas de seleção devem abrir de acordo com o tipo de escoamento selecionado antes de ocorrer o trip;
Realizar o startup da malha de pressão; Realizar o startup da malha de nível

Ação na Detecção de Falha:	**[X] Trip**	**[ ] Operação em modo degradado**	**Tempo Máx. de Operação em Modo Degradado:**

Descrição do Modo Degradado:

OUTRAS IPLS NECESSÁRIAS	Camadas de Proteção Independentes	RRF
	Função automática SSC: caso nível alcance 80% do máximo, rotação das bombas são levadas a 10%	10

Notas e Observações

Presença de sensor redundante de nível. Switch acontece automaticamente (configurado via blocos funcionais da rede)

*Os procedimentos para Rearme são uma sugestão originada a partir do ponto de vista de análise de risco. Necessário verificação e validação.

UEEM	Folha de Dados	Nº 1	Rev. 1
		Folha 1	de 2
	Especificação SIF-UEEM003		

INFORMAÇÕES GERAIS

Tag:	SIF-UEEM003	**Relatório de Análise de Riscos:**	LOPA: 038; HAZOP: Nó T2
Descrição da SIF [LOPA]:	Nível alto em T2 bloqueia fluxo de saída de líquido de T1. Fluxo de ar comprimido é interrompido para evitar desvios em T1		
Causas da Demanda [HAZOP]:	Obstrução do duto de saída de óleo		
Consequências da Falha na Demanda [HAZOP]:	Transbordamento do tanque T2, vazamento de óleo, possibilidade de fissuras em T2.		
Consequências do Trip Espúrio [HAZOP/LOPA]:	Interrupção do ensaio		

REQUISITOS DE PROCESSO E DA ANÁLISE DE RISCO						
	Tempo de Segurança de Processo:	*14 s	**Tempo de Resposta:**	4,5 s	**Tempo de Retardo:**	
	Intervalo entre Testes Periódicos:	0,25 ano	**MTTR:**			
	RRF Requerido:	94	**SIL Requerido:**	SIL 1	**MTTFS Aceitável:**	
RESULTADOS	**RRF Obtido:**	146	**SIL Obtido:**	SIL 2	**MTTFS Obtido:**	

INICIADORES

Tag	Descrição dos Iniciadores	Modo de Atuação	Detecção	Valor da Trip
LSH-T2-01	Transmissor de nível no separador T2	Energiza para trip (20 mA)	HH	98%

ELEMENTOS FINAIS

Tag	Descrição dos Elementos Finais	Modo de Atuação	Estado Seguro
XV-FA07-01	Válvula de bloqueio da linha FA07 (saída de T1)	Desenergiza para trip (4 mA)	Válvula fechada
XV-FA01-01	Válvula de bloqueio da linha FA01 (ar comprimido)	Desenergiza para trip (4 mA)	Circuito aberto
Desarme B1	Circuito de shutdown da bomba B1	Desenergiza para trip (4 mA)	Circuito aberto
Desarme B2	Circuito de shutdown da bomba B2	Desenergiza para trip (4 mA)	Circuito aberto

EXEC

Tag:	CLP-SIS	**Descrição do Executor da Lógica:**	CLP de Segurança
Módulos de Entrada:		**Módulos de Saída:**	

TRIP MANUAL

Tag	Descrição do Trip Manual	Tipo	Localização

DESCRIÇÃO FUNCIONAL

Descrição da Lógica:

Caso iniciador indicar HH deve-se fechar válvula de bloqueio da saída de T1
Desligar bombas e fechar válvula de saída de ar comprimido para evitar desvios de nível em T1

Ações Secundárias:

Caso ainda operante, interromper controle automático da malha de nível e de pressão em T1.

Descrição do Estado Seguro a ser Atingido ou Mantido:

T1 isolado (interromper fluxo para T2 e evitar desvios em T1)
Controle automático de nível de interface em T2 ligado (evitar esvaziamento de T2)
Controle automático de nível e de pressão em T1 desligado (evitar ações na malha)

ALARMES

Alarme Pré-Trip:	Não	**Descrição:**		**Ponto de Ajuste:**	
Alarme Trip:	Sim	**Descrição:**			
Alarme Desvio:	Não	**Descrição:**			**Ponto de Ajuste:**
Diagnóstico de Falha:		**[X] Iniciadores**	**[X] Atuadores**	**[X] Cartões E/S**	**[X] Outros:** CLP
Outros Alarmes:					

UEEM	Folha de Dados	Nº 1	Rev. 1
		Folha 2	de 2
	Especificação SIF-UEEM003		

REQUISITOS DE IMPLEMENTAÇÃO

BYPASS

Bypass para Manutenção:	Não	**Descrição:**
Cuidados Adicionais:		Manutenção realizada apenas com o sistema desligado
Bypass de Início de Operação:	Não	**Descrição**
Cuidados Adicionais:		

Procedimento para Rearme: **

Verificar se bombas se encontram desligadas; Verificar se o controle de nível de interface em T2, de nível e de pressão em T1 se encontram em modo manual; Manter fechadas as válvulas de controle de saída de T2 e de T1; Se o compressor estiver ligado, manter aberta a válvula de controle de pressão em T1; Rearmar a SIF;
Válvulas de seleção devem abrir de acordo com o tipo de escoamento selecionado antes de ocorrer o trip;
Realizar o startup da malha de controle de nível de interface em T2; Realizar o startup da malha de pressão em T1; Realizar o startup da malha de controle de nível em T1;

Ação na Detecção de Falha:	**[X] Trip**	**[ ] Operação em modo degradado**	**Tempo Máx. de Operação em Modo Degradado:**

Descrição do Modo Degradado:

OUTRAS IPLS NECESSÁRIAS	**Camadas de Proteção Independentes**	**RRF**

Notas e Observações

*Tempo de segurança estimado. Utilizar apenas como estimativa inicial

**Os procedimentos para Rearme são uma sugestão originada a partir do ponto de vista de análise de risco. Necessário verificação e validação.

UEEM	Folha de Dados	Nº 1	Rev. 1
		Folha 1	de 2
	Especificação SIF-UEEM004		

INFORMAÇÕES GERAIS

Tag:	SIF-UEEM004	**Relatório de Análise de Riscos:**	LOPA: 039 e 040; HAZOP: Nó T2
Descrição da SIF [LOPA]:	Nível baixo em T2 bloqueia o fluxo de saída em T2 e de saída em T1. Para evitar desvios de nível em T1, interromper fluxo de ar comprimido e de entrada de líquidos em T1		
Causas da Demanda [HAZOP]:	Falha na malha de controle de nível de interface em T2		
Consequências da Falha na Demanda [HAZOP]:	Todo conteúdo de T2 passa para o tanque de armazenamento T4. Contaminação de T4. Possibilidade de transbordamento de T4		
Consequências do Trip Espúrio [HAZOP/LOPA]:	Interrupção do ensaio		

REQUISITOS DE PROCESSO E DA ANÁLISE DE RISCO					
	Tempo de Segurança de Processo:	8 s	**Tempo de Resposta:** 4,5 s	**Tempo de Retardo:**	
	Intervalo entre Testes Periódicos:	0,25 ano	**MTTR:**		
	RRF Requerido:	96	**SIL Requerido:**	SIL 1	**MTTFS Aceitável:**
RESULTADOS	**RRF Obtido:**	100	**SIL Obtido:**	SIL 1	**MTTFS Obtido:**

INICIADORES

Tag	Descrição dos Iniciadores	Modo de Atuação	Detecção	Valor da Trip
LSL-T2-01	Transmissor de nível no separador T2	Desenergiza para trip (4 mA)	LL	76% Nivel máx

ELEMENTOS FINAIS

Tag	Descrição dos Elementos Finais	Modo de Atuação	Estado Seguro
XV-FA11-01	Válvula de bloqueio da linha FA11 (saída do separador T2)	Desenergiza para trip (4 mA)	Válvula fechada
XV-FA01-01	Válvula de bloqueio da linha FA01 (ar comprimido)	Desenergiza para trip (4 mA)	Válvula fechada
Desarme B1	Circuito de shutdown da bomba B1	Desenergiza para trip (4 mA)	Circuito aberto
Desarme B2	Circuito de shutdown da bomba B2	Desenergiza para trip (4 mA)	Circuito aberto

EXEC

Tag:	CLP-SIS	**Descrição do Executor da Lógica:**	CLP de Segurança
Módulos de Entrada:		**Módulos de Saída:**	

TRIP MANUAL

Tag	Descrição do Trip Manual	Tipo	Localização

DESCRIÇÃO FUNCIONAL

Descrição da Lógica:

Caso iniciador indicar LL deve-se fechar válvula de bloqueio de saída de água de T2 e válvula de bloqueio da saída de T1 para interromper fluxo de entrada em T2.
Para evitar desvios de nível em T1, desligar bombas e interromper fluxo de ar comprimido

Ações Secundárias:

Caso ainda operante, interromper controle automático da malha de nivel de interface em T2 e da malha de nível e de pressão em T1.
Em caso de vazamento, acionar a ESD-2

Descrição do Estado Seguro a ser Atingido ou Mantido:

T1 isolado (interromper fluxo para T2 e evitar desvios em T1)
Sem fluxo de saída de líquido em T2 (evitar esvaziamento de T2)
Controle automático de nível e de pressão em T1 e de nivel de interface em T2 desligados (evitar ações nas malhas)

ALARMES

Alarme Pré-Trip:	Sim	**Descrição:**	Alarme para operador via IHM	**Ponto de Ajuste:**	**Ponto de Ajuste:** 80% Nível máx
Alarme Trip:	Sim	**Descrição:**	Alarme para operador via IHM. Sistema de alarme na casa de utilidades		
Alarme Desvio:	Não	**Descrição:**			**Ponto de Ajuste:**
Diagnóstico de Falha:		**[X] Iniciadores**	**[X] Atuadores**	**[X] Cartões E/S**	**[X] Outros:** CLP
Outros Alarmes:					

UEEM	Folha de Dados	Nº 1	Rev. 1
		Folha 2	de 2
	Especificação SIF-UEEM004		

REQUISITOS DE IMPLEMENTAÇÃO

BYPASS

Bypass para Manutenção:	Não	**Descrição:**	
Cuidados Adicionais:		Manutenção realizada apenas com o sistema desligado	
Bypass de Início de Operação:	Sim*	**Descrição**	*Apenas quando T2 inicia vazio Recomenda-se que o bypass seja desativado através de funções automáticas
Cuidados Adicionais:			

Procedimento para Rearme: **

Verificar se bombas se encontram desligadas; Verificar se o controle de nivel de interface em T2, de nível e de pressão em T1 se encontram em modo manual; fechar a válvula de saída de T2 e de saída de T1 via respectivo controle manual do SSC; Se o compressor estiver ligado, manter aberta a válvula de controle de pressão em T1;
Rearmar SIF;
Válvulas de seleção devem abrir de acordo com o tipo de escoamento selecionado antes de ocorrer o trip;
Realizar o startup das malhas de controle de pressão e nível em T1; Realizar o startup do controle de nivel de interface em T2;

Ação na Detecção de Falha:	**[X] Trip**	**[ ] Operação em modo degradado**	**Tempo Máx. de Operação em Modo Degradado:**

Descrição do Modo Degradado:

OUTRAS IPLS NECESSÁRIAS	Camadas de Proteção Independentes	RRF

Notas e Observações

**Os procedimentos para Rearme são uma sugestão originada a partir do ponto de vista de análise de risco. Necessário verificação e validação

UEEM	Folha de Dados	Nº 1	Rev. 1
		Folha 1	de 2
	Especificação SIF-UEEM005		

INFORMAÇÕES GERAIS

Tag:	SIF-UEEM005	**Relatório de Análise de Riscos:**	LOPA: 041 a 044; HAZOP: Nó T4
Descrição da SIF [LOPA]:	Nível baixo em tanque de armazenamento T4 bloqueia fluxo de saída de água		
Causas da Demanda [HAZOP]:	Falha nas válvulas de seleção de modo de operação, falha operacional (válvulas manuais abertas, mal preenchimento do tanque de armazenamento), vazamentos.		
Consequências da Falha na Demanda [HAZOP]:	Danos às bombas		
Consequências do Trip Espúrio [HAZOP/LOPA]:	Interrupção do ensaio		

REQUISITOS DE PROCESSO E DA ANÁLISE DE RISCO	**Tempo de Segurança de Processo:**	13 s	**Tempo de Resposta:** 3 s	**Tempo de Retardo:**	
	Intervalo entre Testes Periódicos:	0,25 ano	**MTTR:**		
	RRF Requerido:	2937	**SIL Requerido:**	SIL 3	**MTTFS Aceitável:**
RESULTADOS	**RRF Obtido:**	2042	**SIL Obtido:**	SIL 3	**MTTFS Obtido:**

INICIADORES

Tag	Descrição dos Iniciadores	Modo de Atuação	Detecção	Valor da Trip
LSL-T4-01	Transmissor de nível no tanque de armazenamento T4	Desenergiza para trip (4 mA)	LL	1,5% Nivel Máx

ELEMENTOS FINAIS

Tag	Descrição dos Elementos Finais	Modo de Atuação	Estado Seguro
XV-FA04-01	Válvula de bloqueio da linha FA04 (água)	Desenergiza para trip (4 mA)	Válvula fechada
Desarme B1	Circuito de shutdown da bomba B1	Desenergiza para trip (4 mA)	Circuito aberto

EXEC

Tag:	CLP-SIS	**Descrição do Executor da Lógica:**	CLP de Segurança
Módulos de Entrada:		**Módulos de Saída:**	

TRIP MANUAL

Tag	Descrição do Trip Manual	Tipo	Localização

DESCRIÇÃO FUNCIONAL

Descrição da Lógica:

Caso iniciador indicar LL deve-se desligar a bomba B1

Ações Secundárias:

Em caso de vazamento, acionar a ESD-2

Descrição do Estado Seguro a ser Atingido ou Mantido:

Sem fluxo de saída de água em T4 (evitar esvaziamento de T4)
Demais subsistemas conseguem continuar operação ou estabilizam devido ao SSC local

ALARMES

Alarme Pré-Trip:	Não	**Descrição:**		**Ponto de Ajuste:**
Alarme Trip:	Sim	**Descrição:**	Alarme para operador via IHM. Sistema de alarme na casa de utilidades	
Alarme Desvio:	Não	**Descrição:**		**Ponto de Ajuste:**

Diagnóstico de Falha: **[X] Iniciadores** **[X] Atuadores** **[X] Cartões E/S** **[X] Outros:** CLP

Outros Alarmes:

UEEM	Folha de Dados	Nº 1	Rev. 1
		Folha 2	de 2
	Especificação SIF-UEEM005		

REQUISITOS DE IMPLEMENTAÇÃO

BYPASS

Bypass para Manutenção:	Não	**Descrição:**
Cuidados Adicionais:		Manutenção realizada apenas com o sistema desligado
Bypass de Início de Operação:	Não	**Descrição**
Cuidados Adicionais:		

Procedimento para Rearme: **

Verificar se bombas se encontram desligadas; Verificar se todas as malhas de controle se encontram em modo manual; fechar a válvula de saída de T2 e de saída de T1 via respectivo controle manual do SSC; Se o compressor estiver ligado, manter aberta a válvula de controle de pressão em T1; Rearmar SIF;
Válvulas de seleção devem abrir de acordo com o tipo de escoamento selecionado antes de ocorrer o trip;
Realizar o startup dos controle de nivel de interface em T2; Realizar o startup das malhas de controle de pressão e nível em T1;

Ação na Detecção de Falha:	**[X] Trip**	**[ ] Operação em modo degradado**	**Tempo Máx. de Operação em Modo Degradado:**

Descrição do Modo Degradado:

OUTRAS IPLS NECESSÁRIAS

Camadas de Proteção Independentes	RRF

Notas e Observações

*Trip da SIF bem próximo da faixa de operação do processo. Sugere-se monitoração constante

**Os procedimentos para Rearme são uma sugestão originada a partir do ponto de vista de análise de risco. Necessário verificação e validação.

UEEM	Folha de Dados	Nº 1	Rev. 1
		Folha 1	de 2
	Especificação SIF-UEEM006		

INFORMAÇÕES GERAIS

Tag:	SIF-UEEM006	**Relatório de Análise de Riscos:**	LOPA: 045 a 048; HAZOP: Nó T5
Descrição da SIF [LOPA]:	Nível baixo em tanque de armazenamento T5 bloqueia fluxo de saída de óleo.		
Causas da Demanda [HAZOP]:	Falha nas válvulas de seleção de modo de operação, falha operacional (válvulas manuais abertas, mal preenchimento do tanque de armazenamento), vazamentos.		
Consequências da Falha na Demanda [HAZOP]:	Danos às bombas		
Consequências do Trip Espúrio [HAZOP/LOPA]:	Interrupção do ensaio		

REQUISITOS DE PROCESSO E DA ANÁLISE DE RISCO	**Tempo de Segurança de Processo:**	17,5 s	**Tempo de Resposta:**	4,5 s	**Tempo de Retardo:**	
	Intervalo entre Testes Periódicos:	0,5 ano	**MTTR:**			
	RRF Requerido:	2937	**SIL Requerido:**	SIL 3	**MTTFS Aceitável:**	
RESULTADOS	**RRF Obtido:**	2042	**SIL Obtido:**	SIL 3	**MTTFS Obtido:**	

INICIADORES

Tag	Descrição dos Iniciadores	Modo de Atuação	Detecção	Valor da Trip
LSL-T5-01	Transmissor de nível no tanque de armazenamento T5	Desenergiza para trip (4 mA)	LL	2,0 % Nivel Máx

ELEMENTOS FINAIS

Tag	Descrição dos Elementos Finais	Modo de Atuação	Estado Seguro
XV-FA05-08	Válvula de bloqueio da linha FA05 (óleo)	Desenergiza para trip (4 mA)	Válvula fechada
Desarme B2	Circuito de shutdown da bomba B2	Desenergiza para trip (4 mA)	Circuito aberto

EXEC

Tag:	CLP-SIS	**Descrição do Executor da Lógica:**	**CLP de Segurança**
Módulos de Entrada:		**Módulos de Saída:**	

TRIP MANUAL

Tag	Descrição do Trip Manual	Tipo	Localização

DESCRIÇÃO FUNCIONAL

Descrição da Lógica:

Caso iniciador indicar LL deve-se desligar bomba B2 e fechar válvula da linha de saída de óleo

Ações Secundárias:

Em caso de vazamento, acionar a ESD-2

Descrição do Estado Seguro a ser Atingido ou Mantido:

Sem fluxo de saída de óleo em T5 (evitar esvaziamento de T5)
Demais subsistemas conseguem continuar operação ou estabilizam devido ao SSC local

ALARMES

Alarme Pré-Trip:	Não	**Descrição:**		**Ponto de Ajuste:**
Alarme Trip:	Sim	**Descrição:**	Alarme para operador via IHM. Sistema de alarme na casa de utilidades	
Alarme Desvio:	Não	**Descrição:**		**Ponto de Ajuste:**
Diagnóstico de Falha:		**[X] Iniciadores**	**[X] Atuadores** **[X] Cartões E/S** **[X] Outros:** CLP	
Outros Alarmes:				

UEEM	Folha de Dados	Nº 1	Rev. 1
		Folha 2	de 2
	Especificação SIF-UEEM006		

REQUISITOS DE IMPLEMENTAÇÃO

BYPASS

Bypass para Manutenção:	Não	**Descrição:**	
Cuidados Adicionais:		Manutenção realizada apenas com o sistema desligado	
Bypass de Início de Operação:	Não	**Descrição**	
Cuidados Adicionais:			

Procedimento para Rearme: *

Verificar se bombas se encontram desligadas; Verificar se todas as malhas de controle se encontram em modo manual; fechar a válvula de saída de T2 e de saída de T1 via respectivo controle manual do SSC; Se o compressor estiver ligado, manter a válvula de controle de pressão aberta; Rearmar SIF;
Válvulas de seleção devem abrir de acordo com o tipo de escoamento selecionado antes de ocorrer o trip;
Realizar o startup do controle de nivel de interface em T2; Realizar o startup das malhas de controle de pressão e nível em T1;

Ação na Detecção de Falha:	**[X] Trip**	**[ ] Operação em modo degradado**	**Tempo Máx. de Operação em Modo Degradado:**

Descrição do Modo Degradado:

OUTRAS IPLS NECESSÁRIAS	**Camadas de Proteção Independentes**	**RRF**

Notas e Observações

*Os procedimentos para Rearme descritos são uma sugestão originada a partir do ponto de vista de análise de risco. Necessário verificação e validação.

UEEM	Folha de Dados	Nº 1	Rev. 1
		Folha 1	de 2
	Especificação SIF-UEEM007		

INFORMAÇÕES GERAIS

Tag:	SIF-UEEM007	**Relatório de Análise de Riscos:**	LOPA: 045 a 048; HAZOP: Nó T5
Descrição da SIF [LOPA]:	Pressão baixa em tanque do compressor T3 bloqueia fluxo de entrada de líquidos em T1		
Causas da Demanda [HAZOP]:	Falha no compressor de ar		
Consequências da Falha na Demanda [HAZOP]:	Pressão insuficiente em T1		
Consequências do Trip Espúrio [HAZOP/LOPA]:	Interrupção do ensaio		

REQUISITOS DE PROCESSO E DA ANÁLISE DE RISCO

Tempo de Segurança de Processo:		**Tempo de Resposta:**	1,5 s	**Tempo de Retardo:**	
Intervalo entre Testes Periódicos:	0,25 ano	**MTTR:**			
RRF Requerido:	*	**SIL Requerido:**	*	**MTTFS Aceitável:**	
RESULTADOS					
RRF Obtido:	151	**SIL Obtido:**	SIL 1	**MTTFS Obtido:**	

INICIADORES

Tag	Descrição dos Iniciadores	Modo de Atuação	Detecção	Valor da Trip
PSL-T3-01	Transmissor de pressão no tanque de pressão T3 do compressor de ar	Desenergiza para trip (4 mA)	LL	**10 psi (0,7 bar)

ELEMENTOS FINAIS

Tag	Descrição dos Elementos Finais	Modo de Atuação	Estado Seguro
Desarme B1	Circuito de shutdown da bomba B1	Desenergiza para trip (4 mA)	Circuito aberto
Desarme B2	Circuito de shutdown da bomba B2	Desenergiza para trip (4 mA)	Circuito aberto

EXEC

Tag:	CLP-SIS	**Descrição do Executor da Lógica:**	CLP de Segurança
Módulos de Entrada:		**Módulos de Saída:**	

TRIP MANUAL

Tag	Descrição do Trip Manual	Tipo	Localização

DESCRIÇÃO FUNCIONAL

Descrição da Lógica:

Caso iniciador indicar PL deve-se desligar bombas B1 e B2

Ações Secundárias:

Em caso de vazamento, acionar a ESD-2

Descrição do Estado Seguro a ser Atingido ou Mantido:

Sem fluxo de entrada em T1 (evitar desvios de nivel alto em T1)
Demais subsistemas conseguem continuar operação ou estabilizam devido ao SSC local

ALARMES

Alarme Pré-Trip:	Não	**Descrição:**		**Ponto de Ajuste:**
Alarme Trip:	Sim	**Descrição:**	Alarme para operador via IHM. Sistema de alarme na casa de utilidades	
Alarme Desvio:	Não	**Descrição:**		**Ponto de Ajuste:**
Diagnóstico de Falha:		**[X] Iniciadores**	**[X] Atuadores** **[X] Cartões E/S**	**[X] Outros:** CLP
Outros Alarmes:				

UEEM	Folha de Dados	Nº 1	Rev. 1
		Folha 2	de 2
	Especificação SIF-UEEM007		

REQUISITOS DE IMPLEMENTAÇÃO

BYPASS

Bypass para Manutenção:	Não	**Descrição:**	
Cuidados Adicionais:	Manutenção realizada apenas com o sistema desligado		
Bypass de Início de Operação:	Sim**	**Descrição**	**Apenas quando o sistema inicia com o tanque T3 despressurizado
Cuidados Adicionais:			

Procedimento para Rearme: ***

Verificar se compressor se encontra ligado e tanque T3 pressurizado; Fechar manualmente válvula de processo na saída de T3; Rearmar SIF;
Válvulas de seleção devem abrir de acordo com o tipo de escoamento selecionado antes de ocorrer o trip;

Ação na Detecção de Falha:	**[X] Trip**	**[ ] Operação em modo degradado**	**Tempo Máx. de Operação em Modo Degradado:**

Descrição do Modo Degradado:

OUTRAS IPLS NECESSÁRIAS	Camadas de Proteção Independentes	RRF

Notas e Observações

*Esta SIF tem o objetivo de diminuir a ocorrência de cenários de pressão insuficiente em T1 (MBJ01). Portanto, é adotada a menor arquitetura possível e o RRF resultante será utilizado para mitigar os cenários de pressão baixa em T1

**Valor de trip ajustado não contempla perdas nos dutos

***Os procedimentos para Rearme descritos são uma sugestão originada a partir do ponto de vista de análise de risco. Necessário verificação e validação.

APÊNDICE E – TABELA DE ALARMES

ID alarme	Causa	Valor	Tempo de segurança
Trip			
ALM-TR001	Pressão alta em T1	60 psi (4,2 bar)	*12,0 s
ALM-TR002	Nivel alto em T1	90% nível máx	33,5 s
ALM-TR003	Nível alto em T2	98% nível máx	*14,0 s
ALM-TR004	Nível baixo em T2	76% nível máx	8,0 s
ALM-TR005	Nível baixo em T4	2% nível máx	13,0 s
ALM-TR006	Nível baixo em T5	2% nível máx	17,5 s
Pré-trip			
ALM-PT001	Nivel alto em T1	80% nível máx	66,5 s
ALM-PT002	Nível baixo em T2	80% nível máx	38,0 s
Desvio			
ALM-DV001	Desvio de pressão em T1	8 psi (0,55 bar)	
ALM-DV002	Desvio de nivel em T1	4% altura máx	
Função Automática			
ALM-FA001	Nível alto em T1	80% nível max	
* Valor estimado. Utilizar apenas como estimativa inicial			