JEFERSON AFONSO LOPES DE SOUZA

ARQUITETURA DE CONTROLE PARA SEGURANÇA DE SISTEMAS CRÍTICOS COMPLEXOS COM POSSIBILIDADE DE INTERAÇÃO ENTRE FALHAS CRÍTICAS

SÃO PAULO

2022

JEFERSON AFONSO LOPES DE SOUZA

ARQUITETURA DE CONTROLE PARA SEGURANÇA DE SISTEMAS CRÍTICOS COMPLEXOS COM POSSIBILIDADE DE INTERAÇÃO ENTRE FALHAS CRÍTICAS

Versão Corrigida

(Versão original encontra-se na unidade que aloja
o programa de Pós-graduação)

Tese apresentada à Escola Politécnica da Universidade de São Paulo para obtenção do título de Doutor em Ciências.

Área de Concentração: Engenharia de Controle e Automação Mecânica.

Orientador: Prof. Dr. Diolino José dos Santos Filho

SÃO PAULO

2022

Este exemplar foi revisado e alterado em relação à versão original sob responsabilidade única do autor e com a anuência de seu orientador.

São Paulo, 30 de dezembro de 2022.

_____	_____
Jeferson Afonso Lopes de Souza	Prof. Dr. Diolino José dos Santos Filho
Autor	Orientador

Catalogação na publicação
Serviço de Biblioteca e Documentação
Escola Politécnica da Universidade de São Paulo

Souza, Jeferson Afonso Lopes de

Arquitetura de controle para segurança de sistemas críticos complexos com possibilidade de interação entre falhas críticas / J.A.L. Souza; orientador: Prod. Dr. Diolino José dos Santos Filho. Versão corrigida, São Paulo, 2022, 169p.

Tese (Doutorado) – Escola Politécnica da Universidade de São Paulo Departamento de Engenharia Mecatrônica e de Sistemas Mecânicos.

1. Indústrias de Processos 2. Sistemas de controle de segurança 3. Arquitetura de controle de segurança 4. Interação entre falhas críticas I. Universidade de São Paulo. Escola Politécnica. Departamento de

Nome: Souza, Jeferson Afonso Lopes de

Título: Arquitetura de controle para segurança de sistemas críticos complexos com possibilidade de interação entre falhas críticas

Tese apresentada à Escola Politécnica da Universidade de São Paulo para obtenção do título de Doutor em Ciências.

Aprovado em: 01/11/2022

Banca Examinadora

Prof. Dr. Diolino José dos Santos Filho

Instituição: Escola Politécnica da USP, PMR

Julgamento: Aprovado

Prof. Dr. Newton Maruyama

Instituição: Escola Politécnica da USP, PMR

Julgamento: Aprovado

Prof. Dr. Marcelo Ramos Martins

Instituição: Escola Politécnica da USP, PNV

Julgamento: Aprovado

Prof. Dr. Francisco Yastami Nakamoto

Instituição: Instituto Federal de Educação, campus São Paulo

Julgamento: Aprovado

Prof. Dr. Robson Marinho da Silva

Instituição: Universidade do Estado da Bahia – UNEB

Julgamento: Aprovado

DEDICATÓRIA

Aos meus pais Daltro e Adelfina

Aos meus irmãos Denise, Fábio e Rafael

À Carina

AGRADECIMENTOS

Este trabalho não é resultado do trabalho isolado de um pesquisador ao longo de sua vida acadêmica, mas a soma das contribuições de diversas pessoas que, de diferentes formas e amplitudes, me inspiraram, me motivaram e me deram forças para que este trabalho fosse edificado a cada dia de pesquisa.

Desta forma, não poderia deixar de agradecer aos meus pais Daltro e Adelfina, a meus irmãos Denise, Fábio e Rafael, além de meus sobrinhos, e sobretudo a meus queridos avós e tios.

Agradeço também à minha companheira Carina, que sempre ficou ao meu lado, mesmo nas situações difíceis, e que sempre me incentivou a seguir com trabalho como forma de contornar tais situações.

De forma particular, agradeço ao meu orientador, Prof. Dr. Diolino José dos Santos Filho, por me fazer entender a postura e o método de trabalho que um pesquisador deve ter quando se depara com problemas cada vez mais complexos. Talvez este foi o maior aprendizado que tive neste período, cujo resultado é representado neste trabalho.

Agradeço também ao Prof. Dr. Paulo Eigi Miyagi por suas contribuições, e aos colegas do grupo de pesquisas do PMR-LSA, em especial ao Reinaldo Squillante Jr, André Cesar Cavalheiro, Marcosiris Pessoa, Caio Fattori, Osvaldo Asato, Edinei Legaspe, Rodrigo Ferrarezzi, e de todos com que pude conviver neste período.

Agradeço à Escola Politécnica da Universidade de São Paulo, e aos Docentes do Departamento de Engenharia Mecatrônica e de Sistemas Mecânicos.

Às secretárias Marisa e Regianne do PPGEM e ao secretário Cássio do PMR.

RESUMO

SOUZA, Jeferson A.L. **Arquitetura de controle para segurança de sistemas críticos complexos com possibilidade de interação entre falhas críticas.** 2022. 169p. Tese (Doutorado em Ciências) – Escola Politécnica, Universidade de São Paulo, São Paulo, 2022.

O avanço constante da automação nas indústrias de processos, fundamental para o atendimento de requisitos tais como custos, qualidade, tempos de entrega, flexibilidade na produção e tecnologia empregada, em um cenário de legislações restritivas quanto a aspectos de segurança e sustentabilidade, entre outros fatores, sendo fortemente influenciada pelo avanço da tecnologia e dos recursos computacionais, resulta em Sistemas Produtivos (SP) caracterizados por elevada complexidade em seus sistemas de controle. Dentre tais processos produtivos há a classe dos sistemas críticos, caracterizados por elevados riscos ao seu funcionamento. Nesse sentido, a ocorrência de determinada classe de falhas pode resultar em cenários com potenciais danos à população, ao meio ambiente e às próprias instalações. O conceito de múltiplas barreiras implementadas por meio de sistemas de controle de segurança permite com que tais sistemas produtivos possam operar sob nível aceitável de riscos. No entanto, arquiteturas até então utilizadas para sistemas de controle de segurança apresentam limitações diante da crescente realidade da complexidade. O trabalho propõe uma nova arquitetura de controle modular e distribuída, operando de forma colaborativa entre níveis hierárquicos como solução à complexidade dos algoritmos de segurança até então concebidos. Como consequência da modularização, verificou-se a possibilidade da abordagem de aspectos de interação entre falhas críticas, além de uma nova classificação de barreiras de segurança, em que recursos humano-operacionais passam a operar de forma colaborativa com os algoritmos de controle de segurança dos módulos.

Palavras-chave: Sistemas produtivos críticos. Sistema de controle de segurança. Arquitetura de sistema de controle de segurança. Barreiras de segurança. Interação entre falhas críticas.

ABSTRACT

SOUZA, Jeferson A.L. **Control architecture for security of complex critical systems with possibility of interaction between critical faults.** 2022. 160p. Tese (Doutorado em Ciências) – Escola Politécnica, Universidade de São Paulo, São Paulo, 2022.

The constant advancement of automation in the process industries, essential for meeting requirements such as costs, quality, delivery times, flexibility in production and technology used, in a scenario of restrictive legislation regarding safety and sustainability aspects, among other factors, being strongly influenced by the advancement of technology and computational resources, results in Production Systems (SP) characterized by high complexity in their control systems. Among such production processes there is the class of critical systems, characterized by high risks to their operation. In this sense, the occurrence of a certain class of faults can lead to scenarios with potential damage to the population, the environment and the facilities themselves. The concept of multiple barriers implemented through security control systems allows such production systems to operate under an acceptable level of risk. However, traditional architectures for security control systems have limitations in view of the growing reality of complexity. The work proposes a new modular and distributed control architecture, operating collaboratively between hierarchical levels as a solution to the complexity of the safety algorithms conceived so far. As a consequence of modularization, it was verified the possibility of approaching aspects of interaction between critical faults, in addition to a new classification of safety barriers, in which human-operational resources start to operate in a collaborative way with the safety control algorithms of its modules.

Keywords: Critical production systems. Safety control system. Safety control system architecture. Security barriers. Interaction between critical faults.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS, ACRÔNIMOS E SIGLAS

AAE	Análise de Árvore de Eventos
ANSI	*American National Standards Institute*
BP	Barreira de Prevenção
BM	Barreitra de Mitigação
CBRIG	Controlador de Brigadas
CP	Controlador de Prevenção
CM	Controlador da Mitigação
E/E/EP	Elétricos, eletrônicos e eletrônicos-programáveis
ET	Evento Topo
FMEA	*Failure Modes and Effect Analysis*
FMECA	*Failure Modes and Effects Consequences Analysis*
FRR	Fator de redução de risco
FTA	*Fault Tree Analysis*
HAZOP	*Hazard and Operability*
IEC	*International Electrotechnical Commission*
ISA	*The instrumentation, Systems and Automation Society*
ISO	*International Organization for Standardization*
MCBP	Módulo de Controle de Barreiras de Prevenção
MCM	Módulo de Controle da Mitigação
MCBRIG	Módulo de Controle das Brigadas
PES	Controlador Programável de Segurança
PFD	Probabilidade de Falha em demanda
PHA	*Preliminar Hazard Analysis*
RdP	Rede de Petri
SCBP	Sistema de Controle Básico de Processo
SCS	Supervisório do Controle de Segurança
SED	Sistemas a Eventos Discretos

SIF	*Safety Instrumented Function*
SIL	*Safety Integrated Level*
SIS	Sistemas Instrumentados de Segurança
SP	Sistemas Produtivos
SVC	Sistemas a variáveis contínuas
WI	*What-If*

LISTA DE SÍMBOLOS

P	conjunto finito de lugares
T	conjunto finito de transições
F	conjunto finito de arcos orientados
W	conjunto de pesos dos arcos orientados
M_0	conjunto de marcas iniciais nos lugares
M	conjunto de marcas nos lugares
(N, M)	rede de Petri marcada
R(N,M)	conjunto de marcas alcançáveis na rede de Petri N a partir da marcação M

SUMÁRIO

1. INTRODUÇÃO

Desde o início do século XXI verifica-se uma crescente implementação da automação nas indústrias de processos, fundamental para o atendimento de requisitos tais como custos, qualidade, tempos de entrega, flexibilidade na produção e tecnologia empregada, entre outros fatores, sendo fortemente influenciada pelo avanço da tecnologia e dos recursos computacionais, resultando em Sistemas Produtivos (SP) caracterizados por elevada complexidade de seus sistemas de controle (SANTOS FILHO, 2000; CHEN e DAI, 2004; WU, XI e ZHUO, 2008) para a execução de processos complexos (FERREIRA, RIBEIRO, *et al.*, 2014; SAMPAIO, 2011), que não poderiam ser exequíveis por meio de métodos convencionais de produção (KAMTEKAR, 2009; MAZZOLINI, BRUSAFERRI e CARPANZANO, 2011).

A complexidade desses sistemas de controle é consequência de seu comportamento dinâmico. Algumas explicações pertinentes que justificam a complexidade é que são sistemas abertos que interagem com o ambiente. A dinâmica natural das interações entre os elementos que a compõem e a característica de sistemas abertos, conduzem os sistemas complexos à não linearidade (CAMERON e LARSEN-FREEMAN, 2007). Outro fator inerente à complexidade de tais sistemas é a questão de alocação dinâmica de recursos de acordo com as funcionalidades exigidas para execução dos processos que devem ser executados em um determinado SP. O reducionismo causado pelo uso de métodos determinísticos para uma alocação estática dos recursos necessários pode comprometer a eficácia, eficiência e até segurança destes SP (SANTOS FILHO, 2000), uma vez que a complexidade, inerente das múltiplas interações, resulta na impossibilidade do determinismo. A alocação dinâmica dos recursos é uma solução para a complexidade, do que resulta na necessidade de sistemas de controle com semântica distintas.

Além da complexidade, há uma classe de sistemas produtivos que são classificados como críticos, em que riscos elevados são inerentes ao seu funcionamento. Nesse sentido, sistemas críticos são caracterizados pela probabilidade de ocorrência de uma determinada classe de falhas, em que sua ocorrência pode resultar em efeitos que podem levar a um cenário catastrófico. Tais falhas são classificadas como falhas críticas (ABNT NBR 5462, 1994; IEC: 61508 PARTE IV, 2010). A ocorrência destas

falhas pode resultar em acidentes com perdas humanas, danos ao meio ambiente e perdas financeiras significativas, envolvendo custos de equipamentos e propriedades (KNIGHT, 2002). Exemplos de sistemas críticos e, portanto, com probabilidade de ocorrência de falhas críticas, são os sistemas de transportes de massa, aviação, usinas nucleares, indústrias químicas e petroquímicas, etc (KNIGHT, 2002).

As indústrias de processos, notadamente complexas, inseridas na classe de sistemas críticos, são o foco deste trabalho. A possível ocorrência de falhas críticas durante a dinâmica de funcionamento dos processos que ocorrem nesses sistemas possui estrita relação com os seguintes fatores: (***i***) o fator humano; (***ii***) a possibilidade de ocorrência de falha nos dispositivos e (***iii***) a natureza computacional dos algoritmos de controle lógico e sequencial. De acordo com Yoe (2012), a ocorrência de falhas pode estar associada a falhas de projeto, falhas de equipamentos, erros operacionais humanos e a falhas nos softwares de controle de processo.

O “fator humano” inserido no projeto, instalação, operação, manutenção e gestão de sistemas deve ser considerado como um dos fatores que causam complexidade nos sistemas críticos. Sob o ponto de vista de segurança, Cacciabue (2004), discute que durante o projeto de plantas industriais, assim como, durante os processos de avaliação de segurança dessas plantas, é impossível conceber uma planta industrial que seja “totalmente livre de erros humanos”. Ainda de acordo com alguns estudos, o erro humano tem um papel fundamental na ocorrência de acidentes em sistemas críticos, tais como na aviação, sistemas ferroviários ou instalações nucleares (REASON, 1997).

A possibilidade de ocorrência de “falha nos dispositivos” (ex: sensores e atuadores), segundo Rouvroye e Van Den Bliek (2002), está associada à probabilidade de não executar sua função sob demanda, comprometendo a segurança destes processos.

Finalmente, a “natureza computacional dos algoritmos de controle lógico e sequencial envolvendo paralelismo e assincronismo de eventos” evoluiu em sua complexidade, de modo que seu grau de comprometimento com o equipamento, com a integridade física dos operadores, e com o meio ambiente no qual os SPs estão inseridos seja extremamente elevada (MAZZOLINI, BRUSAFERRI e CARPANZANO, 2011).

Desta forma, para garantir um nível de segurança adequado em um sistema crítico, medidas apropriadas devem ser implementadas para explorar tanto a potencialidade

das habilidades humanas, como o potencial de automação para a prevenção ou possível degeneração, e para a mitigação das consequências de falhas críticas que não puderam ser evitadas (CACCIABUE, 2004).

Dentre as medidas para diminuir a probabilidade de ocorrência de um evento crítico estão as camadas ou barreiras sucessivas de proteção. Estas têm como objetivo reduzir a probabilidade de ocorrência de eventos de perigo - portanto minimizar a probabilidade de ocorrência da falha crítica - para uma condição de risco aceitável para o funcionamento da planta / processo. Dentre tais camadas ou barreiras, destacam-se as barreiras de prevenção e mitigação de falhas críticas. A prevenção tem como objetivo diminuir a probabilidade de ocorrência de um determinado acontecimento indesejável, enquanto que na mitigação, os esforços são realizados no sentido de diminuir ou mitigar as consequências desse mesmo acontecimento (CARVALHO, 2011).

Nesse sentido, o termo “salvaguardas” data do início dos anos 1960, com o modelo de energia proposto por Gibson (1961), em que são propostas barreiras para a interrupção do fluxo de hidrocarbonetos em casos de vazamentos em instalações químicas. A nomenclatura do modelo reside no fato da enorme quantidade de energia contida nos fluidos, e das consequências catastróficas para casos de acidentes.

Já o conceito de “barreira de segurança” data de 1973 (HADDON, 1990). Barreiras de segurança físicas, constituídas de materiais anti-chamas, são exploradas em diversos trabalhos (JOHNSON, 1980; SVENSON, 1991; WAHLSTROM, B. e GUNSELL, L., 1998; NEOGY, P., HANSON, A., *et al.*, 1996; DOE, 1997; HALE, 2003). Holland (1997) define “barreira de segurança” como uma barreira de proteção física, com a função de “impedir o fluxo”, e deve ser capaz de prevenir um cenário que antecede uma consequência indesejável (CCPS, 2003). Johnson (1980) define “barreiras de segurança” como medidas físicas e organizacionais para prevenir um alvo de possíveis ameaças. Em Wahlstrom & Gunsell (1998) são explorados os conceitos de barreiras técnicas, implementadas por sistemas de jateamento de água. Em Svenson (1991) é proposto o conceito de barreira técnica por sensoriamento de gás. O conceito de “barreira técnica” é mencionado em Kjellén (2000), que menciona válvulas de segurança de pressão. Em De Dianous & Fievez (2006) a barreira de prevenção consiste em um sistema automático de emergência de purga com ações de

emergência da equipe de brigadistas. Em praticamente em todos os trabalhos são mencionados os aspectos humanos de barreiras, principalmente em relação à necessidade de adequado treinamento diante de situações de elevado risco (NEOGY, P., HANSON, A., *et al.*, 1996; DOE, 1997; WAHLSTROM, B. e GUNSELL, L., 1998).

De forma contemporânea, normas de segurança para a indústria de processos foram regulamentadas para o estabelecimento dos requisitos mínimos para a segurança dos processos. Técnicas de análises de riscos foram desenvolvidas e normatizadas para a identificação dos potenciais riscos das instalações. Modelos probabilísticos de causa / efeito foram implementados em *softwares*, o que permite uma melhor avaliação do risco da planta / processo.

Sklet (2006) define o conceito de barreiras de segurança como “meios físicos e/ou não físicos planejados para prevenir, controlar, ou mitigar eventos indesejados ou acidentes”. A caracterização de barreiras é feita com base no conceito de *detecção, diagnóstico e tratamento*. Desta forma, Sklet (2006) classifica as barreiras de segurança em (i) *barreiras comportamentais,* nas quais o processo de detecção, diagnóstico e tratamento é totalmente performada por humanos; (ii) *barreiras sócio-técnicas*, em que há uma interface homem-máquina, na qual o processo de detecção e diagnóstico é feito pelo homem e a ação de tratamento é realizada por um dispositivo mecânico / elétrico / eletrônico ou constituído de um de um sistema de controle e (iii) *barreiras de hardware*, em que os três processos, de detecção, diagnóstico e tratamento de falhas são implementados por elementos de *hardware* ou por sistemas de controle.

Diante do modelo de cenários de acidentes proposto por Reason (1997), Sklet (2006) propõe o conceito de defesa em profundidade, que é a proposta de múltiplas linhas de defesa e um sistema de barreiras de segurança (comportamentais, sócio-técnicas e *hardware*) ao longo do cenário de acidente.

Hollnagel (2007) define três abordagens para o requisito de segurança de sistemas: (i) o princípio da eliminação dos riscos; (ii) o princípio da substituição dos riscos e (iii) Prevenção e proteção (mitigação).

O princípio da eliminação dos riscos é uma tarefa que requer que todos os riscos de um processo devem ser identificados e removidos. Diante da complexidade inerente

dos sistemas produtivos, este princípio tem mostrado pouco sucesso. (HOLLNAGEL, 2007).

Por outro lado, o alcance da segurança por meio do princípio da substituição tem sido a solução mais frequente (HOLLNAGEL, 2007). O caso mais notado que vem sendo usado no princípio da substituição é quando o "desempenho humano" é substituído pela tecnologia, especialmente pela automação. A justificativa é que a automação é altamente confiável, pois ela é o resultado de um processo de *design* formal, e adicionalmente ela é baseada em componentes com taxas de falhas conhecidas. Por outro lado, o ser humano é mais vulnerável a falhas e inseguro. Tendo por base relatórios de investigação, observa-se que vários acidentes são provocados por "erros humanos" (HOLLNAGEL, 2007).

Com relação à abordagem de prevenção e proteção, Hollnagel (2007) argumenta que prevenir é melhor que proteger, ou seja, a melhor forma de assegurar um estado de segurança de um sistema crítico é por meio da prevenção que um evento indesejado ocorra ou proteção contra as consequências provocadas pelo evento indesejado. Diante da impossibilidade da eliminação dos riscos, Hollnagel (2007) propõe um modelo conceitual de segurança que integra as abordagens de prevenção de falhas e mitigação (proteção) de falhas.

Considerando o princípio da substituição (HOLLNAGEL, 2007) do elemento humano pela automação, e das classificações das barreiras técnicas, implementadas por elementos de *hardware*, e considerando a complexidade e criticidade dos sistemas produtivos, a detecção e a tomada de decisão humana para a implementação de barreiras de segurança, embora necessárias, não são mais suficientes para a manutenção de estado seguro de uma planta / processo.

Nesse sentido, o conceito de Sistemas Instrumentados de Segurança (SIS), de acordo com especialistas, é uma solução tecnológica para a implementação de sistemas de controle relacionados à segurança funcional na indústria de processos. Um SIS[1] implementa uma ou mais camadas de redução de riscos por meio de sistemas eletrônicos programáveis, sensores e atuadores independentes do Sistema de

[1] O conceito de SIS será apresentado com mais detalhes na seção 2.5.

Controle Básico do Processo – SCBP. Normas tais como a IEC 61508 (IEC: 61508, 2010) e a IEC 61511 (IEC: 61511, 2003), entre outras, provem diretrizes para diferentes atividades relacionadas ao ciclo de vida de projeto de SIS, tais como *design*, instalação, operação, manutenção, testes, entre outros (FANG e ZONGZHI WU, 2008; LUNDTEIGEN e RAUSAND, 2009; FERRAREZI, SANTOS FO, *et al.*, 2014a).

Squillante (2011) utiliza o conceito de SIS para a prevenção de falhas críticas na indústria de processos. As falhas críticas são identificadas por meio de estudo Hazop e os modelos para o diagnóstico e tratamento das falhas críticas são obtidos por meio de redes Bayesianas. Não foram considerados, no entanto, aspectos de sequenciamento entre falhas.

Markowski & Kotynia (2011) apresentam o conceito de SIS para a prevenção dos possíveis caminhos críticos para a falha crítica “vazamento de hexano” e ações de mitigação. A lógica *fuzzy* foi utilizada para a determinação das ações de controle de detecção e atuação em cenários de riscos avaliados pela técnica Hazop. Foi considerado apenas uma falha crítica para o processo.

Souza (2014) propõe um método para o desenvolvimento de SIS para a prevenção e mitigação de falhas críticas por meio da lógica *fuzzy*, com o objetivo de ações antecipativas às ocorrências dos eventos topo. No entanto, não foram considerados aspectos de sequenciamento e interação entre as falhas críticas.

Em Ferrarezi e Santos Filho (2014), é proposto um ambiente unificado para a modelagem e posterior verificação por meio da técnica *model-checking* para os códigos de controle de prevenção e mitigação de SIS. O ambiente realiza a verificação formal dos modelos bem como suas possíveis interações, que não poderiam ser identificadas em abordagem não unificada.

Pfeiffer e Urbas (2015) propõem cinco arquiteturas diferentes de SIS para validação quanto a falhas randômicas de *hardware*. As arquiteturas foram validadas, resultando em arquiteturas redundantes robustas quanto à falha de componentes. No entanto, não apresentam as arquiteturas de *hardware* para as funcionalidades de prevenção e mitigação de falhas críticas.

Já Souza (2016) apresenta a modelagem de SIS por meio das redes de Petri coloridas, em que múltiplas falhas críticas são consideradas em uma planta / processo, e os respectivos eventos inicializadores, representados por *multisets* são

utilizados para as respectivas barreiras de prevenção. Não são considerados aspectos de interação entre falhas.

Squillante (2017) propõe uma nova classificação para barreiras de segurança, em que propõe o conceito de barreiras de segurança reativas, em que barreiras de prevenção e mitigação são implementadas por meio do conceito de SIS, em que a diagnosticabilidade e filtragem de eventos espúrios é realizada no Sistema Supervisório de Controle de Segurança do Processo – SCSP.

Souza (2017) apresenta o modelo qualitativo de SIS que considera a interação entre eventos topo, em que a ocorrência de um evento topo pode desencadear a ocorrência dos demais eventos topo. Deve-se, portanto, alocar as respectivas prevenções sobre os demais eventos topo. Os algoritmos de controle não são apresentados de forma modular, dificultando a verificação e validação dos modelos, dependendo da complexidade do sistema crítico.

Trabalhos recentes vêm sendo publicados para a avaliação de riscos e frequências de ocorrências, com a avaliação de disponibilidade e efetividade de barreiras de segurança em estruturas de árvores de falhas, com foco na indústria de óleo e gás, apresentando soluções de engenharia a exemplos de instalações, porém, sem apresentar um método de implementação (BUCELLI, M., LANDUCCI, G., *et al.*, 2018; TSUNEMI, KIHARA, *et al.*, 2019; SOBRAL, J. e SOARES, G., 2019; MISURI, LANDUCCI e COZZANI, 2020; DING, KHAN, *et al.*, 2020; ZHU, QI e JIANG, 2020; MISURI, LANDUCCI e COZZANI, 2021a); MISURI, LANDUCCI e COZZANI, 2021b); PARK, KIM, *et al.*, 2021; OVIDI, ZHANG, *et al.*, 2021; DIMAIO, SCAPINELLO, *et al.*, 2021; HOSSEINNIA DAVATGAR, PALTRINIERI e BUBBICO, 2021; SUN, WANG, *et al.*, 2021).

Sobral, J. e Soares, G. (2019) apresentam um método para avaliação da adequação das barreiras de segurança em cenários de perigos, porém, sem apresentar métodos formais para a modelagem do algoritmo de controle de barreiras técnicas.

(SQUILLANTE, R., DIAS, J., *et al.*, 2021) propõem o conceito de barreiras de segurança reativas, em que barreiras de prevenção e mitigação são implementadas por meio do conceito de SIS, em que a diagnosticabilidade e filtragem de eventos espúrios é realizada no sistema supervisório de controle de segurança do processo – SCSP. Não apresenta, porém, um método que contemple múltiplos eventos topo e o

gerenciamento entre tipos distintos de barreiras. Outra limitação é a abordagem determinística dos modelos dos algoritmos de controle para uma estrutura de árvore de falhas obtida por aprendizagem Bayesiana.

Barreiras técnicas, implementadas por meio de SIS, embora tenha sua eficácia reconhecidas, provavelmente fará parte de um sistema de barreiras, de tal modo com que aspectos de interação devam ser considerados. Yuan, S. *et al.* (2022) apresentam o conceito de gerenciamento de barreiras, porém sem apresentar um método para tal.

Nesse contexto, surge uma questão: como implementar um sistema de controle de segurança para a prevenção e mitigação de falhas críticas em plantas / processos em que sejam identificados múltiplos eventos topo, que apresente aspectos de interação e a necessidade do gerenciamento do conjunto de barreiras sem aplicar processos reducionistas que comprometam o tratamento da complexidade destes sistemas ?

1.1 OBJETIVO

O objetivo deste trabalho é propor uma metodologia para o projeto de sistemas de controle de segurança para as indústrias de processos, que sejam capazes de suportar a ocorrência de múltiplos eventos críticos ou falhas críticas de tal forma que sejam tratados os aspectos de possíveis interações entre falhas, tendo como diretrizes máximas os seguintes conceitos preconizados nas normas correlatas:

- O conceito de segurança funcional de acordo com a norma IEC 61511 (IEC, 2003);
- O conceito de cenários críticos conforme as normas HSE (HSE, 2006a) e N-2782 (N-2782, 2015);
- Fases do ciclo de vida útil de acordo com a norma N-2782 (N-2782, 2015);
- Imposições legais das normas ABNT 14.726 (ABNT NBR 14276, 2006) e ABNT (ABNT NBR 15219, 2019).

A metodologia está embasada em dois contextos fundamentais:

I. Proposta de uma arquitetura de controle modular, distribuída e integrada para a prevenção e mitigação de falhas críticas;
II. Proposta de uma sistemática para a síntese dos sistemas de controle de cada módulo e suas integrações.

Neste contexto, de forma específica, são consideradas as seguintes metas a serem atingidas:

I. Pertinente à arquitetura de controle:
    a. Síntese de uma estrutura de controle distribuída e modular para a prevenção e mitigação de múltiplos eventos críticos ou falhas críticas, em consonância com as normas IEC 61508 (IEC, 2010) e IEC 61511 (IEC, 2003);
    b. Integração dos módulos de controle distribuído de prevenção e mitigação com o módulo de interface para atendimento legal das normas NBR 14.726 (ABNT NBR 14276, 2006) e NBR 15.219 (ABNT NBR 15219, 2019).
    c. Definição de um módulo supervisório de segurança do processo que gerencie os módulos de controle distribuídos de prevenção e mitigação, aderente ao princípio da diagnosticabilidade segura;
        i. Definição, no módulo supervisório, de módulos de controle para o gerenciamento do conjunto global de barreiras de segurança, aderente ao princípio de defesa em profundidade.

II. Pertinente à sistemática*:*
    a. Identificação dos elementos críticos de uma planta – processo - em função da fase em que se encontrar de seu ciclo de vida útil (N-2782, 2015) e identificação dos cenários críticos para ocorrência de cada evento crítico topo (HSE, 2006a);
    b. Identificação das funções instrumentadas de segurança de prevenção e mitigação de falhas críticas por meio de estudo *HAZOP* (IEC 61882, 2001);

c. Síntese dos algoritmos de segurança de prevenção e mitigação das falhas críticas baseada em procedimentos de modelagem formal da teoria de controle de SEDs;
d. Modularização dos algoritmos de prevenção e mitigação de acordo com os cenários críticos identificados;
e. Síntese dos algoritmos dos módulos do sistema de controle supervisório baseada em procedimentos de modelagem formal da teoria de controle de SEDs;
f. Integração entre algoritmos dos módulos de controle de prevenção e mitigação e entre os módulos do controle supervisório de segurança.

Por sua vez, a metodologia proposta será aplicada a um exemplo de indústria de processos e a análise dos resultados permitirá a sua verificação.

1.2 MÉTODO DE PESQUISA

O método de pesquisa aplicado ao presente baseia-se no desenvolvimento das seguintes questões:

A. Definição e descrição do problema;
B. Formulação das Hipóteses;
C. Definição do tipo de pesquisa;
D. Definição do método de investigação;
E. Ciclo de vida do projeto de pesquisa.

A seguir são apresentados os detalhamentos destas questões.

A. Definição e descrição do problema – são abordados sistemas produtivos complexos e críticos, em que a ocorrência de uma determinada classe de falhas pode resultar em perdas de vidas humanas, danos ao meio ambiente e

perdas financeiras significativas com propriedades e equipamentos (KNIGHT, 2002).

B. Formulação das hipóteses - faz parte de nosso estudo falhas cujos efeitos possam ser mensurados, isto é, dispõe-se de dispositivos que possam detectar a ocorrência de uma falha, seja por falha de equipamento / dispositivo ou detecção da falha por meio da variação dos parâmetros de um processo. Quanto ao comportamento dinâmico dos sistemas a serem abordados ressalta-se que:
    - Ao associarmos um estado binário, pode-se caracterizar a dinâmica do sistema a uma sucessão de eventos, com transições instantâneas entre os estados, de maneira independente do tempo, caracterizando-o, portanto, como um Sistema a Eventos Discretos – SED (MIYAGI, 1996);
    - O uso da abordagem de controle de Sistemas a Eventos Discretos (SEDs) é adequado à modelagem e análise de questões relacionadas a sistemas de segurança (BAKOLAS e SALEH, 2011);
    - A consideração de princípios de observabilidade e rastreabilidade de falhas durante a evolução de falhas, para que seja possível convergir para um conceito de diagnosticabilidade segura;
    - A consideração de aspectos de interações entre falhas, falhas conjuntas ou ainda sequenciamentos de falhas, ou ainda relações de causalidade entre falhas.

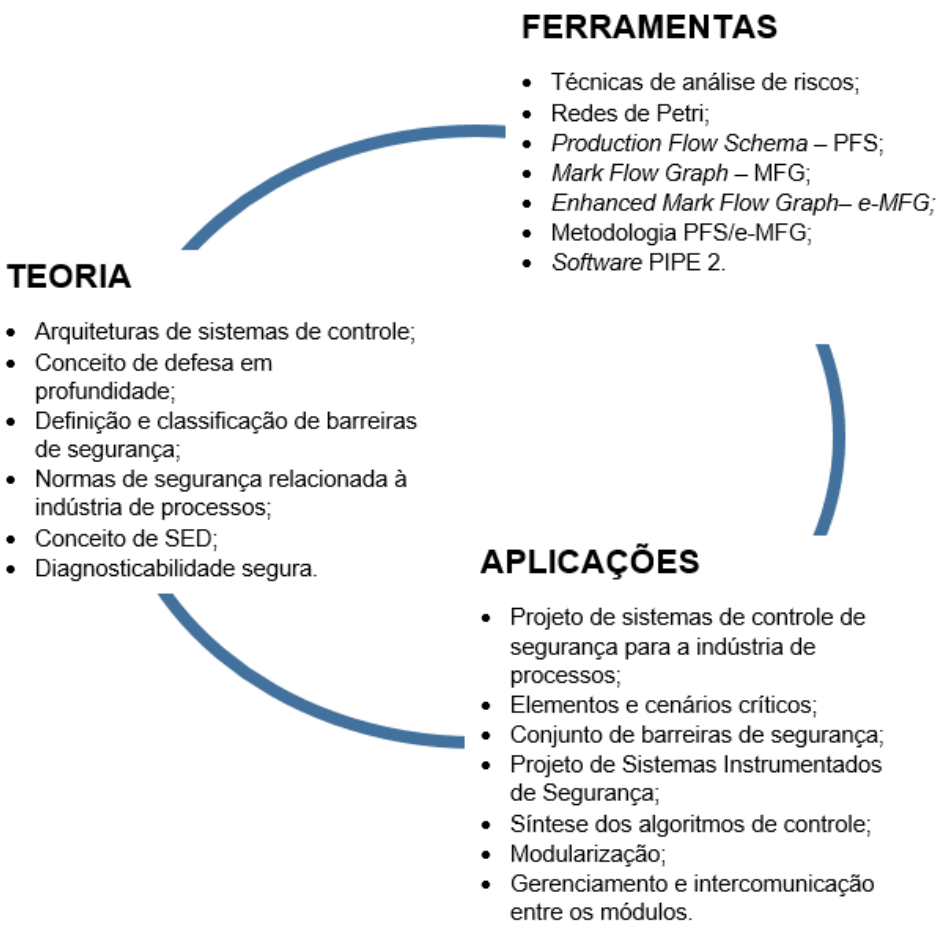
C. Definição do tipo de pesquisa - esta pesquisa é do tipo teórico-experimental (SEVERINO, 2007); ou seja, de uma pesquisa aplicada, que baseia-se em um levantamento teórico de assuntos relacionados ao tema, o levantamento de soluções para as carências apresentadas, e a proposta de procedimentos e de modelos matemáticos formais, além da aplicação da proposta em casos de uso reais para a avaliação dos resultados obtidos e das respectivas conclusões a respeito de sua eficácia. As fontes de dados utilizadas para o desenvolvimento da pesquisa têm como base uma exaustiva revisão bibliográfica. Em relação aos objetivos do trabalho, a pesquisa será descritiva, de modo que procurou-se delinear o problema por meio da descrição detalhada de seus elementos estruturais e de suas relações de forma com que se

tornasse possível a aplicação de técnicas para a solução do problema e propor uma metodologia para a aplicação em um caso real.

D. O método de investigação utilizado neste trabalho foi o dedutivo, por meio de uma visão sistêmica a partir da representação de modelos constituídos de uma estrutura e de um comportamento. O processo de revisão bibliográfica utilizado para o desenvolvimento do trabalho constitui-se em pesquisas em bancos de dados de produção científica internacional, tais como o *Web of Science, Scopus, Research Gate, Elsevier, Google Scholar* e *Dedalus – USP.* Outras fontes de pesquisa foram as normas internacionais e os livros acadêmicos relacionados ao tema, além de anais de congressos de tema correlato. O processo de investigação foi realizado por meio de busca nas bases de dados citadas por meio de “palavras chave” e a leitura dos *Abstracts* / Sumários dos resultados obtidos. Caso o artigo / livro tivesse de fato uma estreita relação com o projeto de pesquisa, era feita uma investigação mais detalhada.

E. O ciclo de vida do projeto de pesquisa aplicado é o proposto por Jensen (1992); onde são abordados de forma cíclica e repetitiva, os aspectos associados às teorias, ferramentas e aplicações envolvidas. Considerando o escopo do presente trabalho, a Figura 1 sintetiza as referências do presente trabalho em termos do ciclo de vida proposto para o desenvolvimento de um projeto de pesquisa.

Figura 1 - Ciclo de desenvolvimento de pesquisa realizado



Fonte: Adaptado de (JENSEN, 1992)

1.3 ORGANIZAÇÃO DO TEXTO

Após a apresentação dos aspectos introdutórios o capítulo 2 apresenta a revisão da literatura pertinente ao desenvolvimento do trabalho, iniciando com o conceito de defesa em profundidade e estratégias para a implementação deste conceito para o projeto de sistemas de controle de segurança. Uma ampla revisão do conceito de barreiras de segurança é apresentada, com a definição, classificação das barreiras e um conjunto de regras para a implementação de um diagrama de barreiras de segurança. As principais técnicas de análises de riscos, referenciadas por normas,

são apresentadas tanto para a definição dos elementos críticos e dos cenários críticos de uma planta / processo, quanto para a definição das funções instrumentadas de prevenção e mitigação de cada barreira de segurança. Normas de segurança à indústria de processos servem como referência ao desenvolvimento do trabalho.

O capítulo 3 apresenta a metodologia para o desenvolvimento de um sistema de controle de segurança para a indústria de processos, com a proposta de uma arquitetura de controle modular, distribuída e integrada a um sistema supervisório de segurança, para o gerenciamento da prevenção e mitigação de múltiplas falhas críticas – considerando-se a possível interação entre elas - em uma planta / processo. Definida a arquitetura de controle, o capítulo apresenta um *framework* para a síntese dos algoritmos de controle de cada módulo e para a intercomunicação entre os módulos.

O capítulo 4 apresenta a aplicação da metodologia proposta a um exemplo de indústria de processos para a discussão e avaliação dos resultados.

No capítulo 5 são apresentadas as conclusões e contribuições do trabalho e as sugestões de continuidade da temática abordada por meio de trabalhos futuros.

O Anexo A apresenta um método para a definição dos cenários críticos de uma planta / processo. O Anexo B as ferramentas formais para a modelagem de processos a eventos discretos. O Apêndice A apresenta um exemplo em E-MFG para a confirmação de ocorrência de falha, considerando critérios de votação de sensores.

2. REVISÃO DA LITERATURA

Considerando-se o método de pesquisa proposto, este capítulo apresenta os fundamentos teóricos, as ferramentas e as técnicas para o desenvolvimento de uma metodologia para projetos de sistemas de controle de segurança para a indústria de processos. Nesse sentido, o sequenciamento dos itens do capítulo apresenta, na medida do possível, a evolução concatenada dos conceitos de forma a facilitar a compreensão da metodologia proposta.

A seção 2.1 apresenta as principais técnicas de avaliação de riscos, referenciadas por normas, para a definição dos elementos críticos e dos cenários críticos para a ocorrência de um evento topo. Na seção 2.2 trata das normas de segurança pertinentes à indústria de processos, fundamentais para referenciar a metodologia proposta. A seção 2.3 apresenta o conceito de defesa em profundidade, em que as múltiplas linhas de defesa são implementadas pelo conceito de barreiras de segurança de diferentes naturezas. A seção 2.4 apresenta o conceito de Sistemas Instrumentados de Segurança – SIS, fundamental para o projeto das barreiras de segurança técnicas reativas. O capítulo se encerra na seção 2.5, em que é apresentado o conceito de diagnosticabilidade segura, que fornece subsídios para o projeto do conceito de SIS, implementado nas barreiras reativas. Como subsídio ao desenvolvimento e síntese dos algoritmos de controle, o Anexo B contém os fundamentos da teoria de sistemas a eventos discretos – SED, as ferramentas de modelagem de SED utilizadas para o desenvolvimento do trabalho: o *mark flow graph* (MFG) e o *enhanced mark flow graph* (E-MFG) com arcos comunicadores, o *production flow schema* (PFS), e a metodologia PFS / E-MFG.

2.1 TÉCNICAS DE AVALIAÇÃO DE RISCOS

Para a identificação dos elementos críticos de uma planta / processo, foram desenvolvidas diversas técnicas de avaliação de riscos, referenciadas por normas, e reunidas na (ABNT ISO/IEC 31010, 2012), em que foram compiladas quarenta e duas técnicas diferentes para identificar, compreender a avaliar os diferentes riscos de

processos. Dentre as técnicas relacionadas, são identificadas as técnicas constantes nas normas de segurança relacionadas à indústria de processos (seção 2.2), foco do presente trabalho.

De acordo com Modarres, Kaminskiy e Krivtsov (2009), nenhuma técnica de análise de risco, aplicada de forma isolada, é capaz de realizar um estudo de risco completo. Cada técnica possui sua particularidade e contribuição, de forma com que a avaliação dos cenários de risco de uma instalação (e suas consequências) é obtido por meio de um conjunto de técnicas. Nas subseções subsequentes são apresentadas as principais técnicas referenciadas nas normas de segurança para a indústria de processos.

2.1.1 *What-If* – WI

Esta técnica examina ordenadamente as respostas do sistema frente às falhas de equipamentos, erros humanos e condições anormais do processo. Para o desenvolvimento desta técnica, se faz necessário a constituição de uma equipe com conhecimentos específicos sobre o processo a ser analisado e sua operação. Esta equipe procura responder a questões do tipo: “O que...se... ?” (MODARRES, 2006).

Segundo Silva Carneiro (2011) e Freitas (2008), *What if* (O que aconteceria se...?) é uma técnica de identificação de falhas e análise de riscos que consiste em detectar tais falhas por meio de questionamentos livres ou sistemáticos.

Exemplo: “O que ocorreria se a válvula de alívio não abrisse na pressão especificada?”.

Estas questões são elaboradas na tentativa de identificar os riscos potenciais presentes no processo. Como depende da experiência e do conhecimento do grupo de análise, esta técnica normalmente é utilizada como complemento ou parte auxiliar de outras técnicas.

2.1.2 Análise de Modos de Falha e seus Efeitos – FMEA

A FMEA, definido na (IEC 60812, 2006) e (ABNT NBR 5462, 1994) como Análise dos Modos de Falha e seus Efeitos *(**F**ailure **M**odes and **E**ffects **A**nalysis)*, envolve um estudo detalhado e sistemático das possíveis falhas de componentes ou de sistemas mecânicos. Os modos de falha de cada componente são identificados e os efeitos destas falhas no sistema são avaliados, sendo propostas medidas de eliminação, mitigação e controle das causas e consequências destas falhas (ROUSH, 2000; MODARRES, KAMINSKIY e KRIVTSOV, 2009; RAUSAND, 2011).

Desta forma, podemos elencar quais componentes críticos do sistema, ou seja, quais elementos que, sob falha, podem causar as consequências mais sérias ao sistema.

A análise completa consiste em identificar o modo e o tipo da falha, os agentes promotores e inibidores, a fase do ciclo de vida do componente ou o sistema em que a falha ocorreu e a fase geradora, ou seja, quando os agentes promotores foram introduzidos.

Deve-se refletir sobre cinco questões a respeito do sistema como base para uma correta elaboração do FMEA:

- ✓ Como cada componente do sistema pode falhar?
- ✓ Qual ou quais são seus modo(s) de falha?
- ✓ Quais os efeitos desta(s) falhas(s) sobre o sistema?
- ✓ Quão críticos são estes efeitos?
- ✓ Como detectar a falha?
- ✓ Quais as medidas contra estas falhas (evitar, prevenir a ocorrência, minimizar seus efeitos)?

Um exemplo de FMEA é apresentado por meio da Tabela 1.

Tabela 1 - Exemplo de tabela FMEA .

FORMULÁRIO FMEA																	
Produto/ Processo:						Área envolvida:							Data Elaboração:				
Fornecedor:						Aplicação:							Data Revisão:				
ITEM	NOME DO COMPONENTE OU PROCESSO	FUNÇÃO DO COMPONENTE OU PROCESSO	FALHAS POSSÍVEIS			ATUAL					AÇÃO CORRETIVA		RESULTADO				
			MODO	EFEITO(S)	CAUSA(S)	CONTROLES ATUAIS	ÍNDICES				RECOMENDAÇÕES	TOMADA	ÍNDICES REVISTOS				RESPONSÁVEL
							O	G	D	R			O	G	D	R	

Probabilidade de Ocorrência	Gravidade	Probabilidade de Detecção	Risco
muito remota.....1		muito alta.....1	
muito pequena.....2	apenas perceptível.....1	alta.....2	baixo.....2
pequena.....3	pouco importante.....2 e 3	moderada.....3	moderado.....3
moderada.....4,5,6	moderadamente grave.....4 a 6	pequena.....4,5,6	alto.....4,5,6
alta.....7,8	grave.....7 e 8	muito pequena.....7,8	
muito alta.....9,10	extremamente grave.....9 e 10	remota.....9,10	

Fonte: adaptado de (IEC 60812, 2006)

Este método é muito útil na fase de planejamento de prevenção de riscos, pois o conhecimento dos prováveis modos de falhas que podem ocorrer permite ao analista eliminá-los ou minimizá-los e evitar as consequências que deles podem advir. As grandes vantagens são a sua sistematização e o caráter metódico de análise dos vários subsistemas e respectivos estados de funcionamento. (SILVA CARNEIRO, 2011).

Uma limitação da FMEA é que este estudo é centrado no componente, por isso possui limitações quando vários modos de falha ocorrem de forma simultânea.

Esta técnica pode incluir o nível de gravidade das consequências e as probabilidades de ocorrência, sendo denominada, neste caso, de FMECA (IEC 60812, 2006) Análise de criticidade, modos e efeitos de falhas.

2.1.3 Estudo de Operabilidade e Riscos – Hazop

O estudo de operabilidade e riscos, ou *HAZOP (**HAZ**ard and **OP**erability studies)* definido na IEC 61882 (IEC 61882, 2001) foi desenvolvido para o exame eficiente e detalhado das variáveis de um processo, possuindo uma forte semelhança com o FMEA. É um processo de análise de perigos, utilizado mundialmente para estudar não só os perigos de um sistema, mas também os seus problemas de operacionalidade; explorando os efeitos de quaisquer desvios de um projeto (ARNALDOS, DUNJÓ, *et al.*, 2009). Por meio do Hazop identificam-se os caminhos nos quais os equipamentos de processos podem falhar ou ser inadequadamente operados. É desenvolvida por uma equipe multidisciplinar, sendo guiada pela aplicação de palavras específicas – palavras guia – a cada variável do processo. Desta forma, geram-se os desvios dos padrões operacionais, os quais são analisados em relação às suas causas e consequências.

Dependendo do grau de severidade da consequência, possíveis tratamentos podem ser sugeridos. Para a aplicação da análise é importante utilizar diagramas de fluxo do processo (de acordo com a norma ISA S5.1 (ISA S-5.1-1984, 2009) baseado nos seguintes passos:

- ✓ Dividir o sistema em partes, e descrever o comportamento esperado de cada parte;
- ✓ Selecionar um parâmetro do processo;
- ✓ Aplicar as palavras guias ao parâmetro e identificar eventuais desvios;
- ✓ Determinar possíveis causas e consequências do desvio;
- ✓ Identificar sensores e atuadores para a identificação e tratamento do desvio.

A Tabela 2 ilustra a estrutura funcional do Hazop.

Tabela 2 – Exemplo de documentação de HAZOP–IEC 61882, (IEC 61882, 2001).

Elemento	Evento Crítico / Desvio	Causa(s)	Consequência(s)	Ação	Equipamentos	Sensores	Atuadores
Válvulas de alívio RV-1,2 e 3	Falha no fechamento das válvulas	a) Desgaste mecânico b) Falha no atuador das válvulas	Excesso de alimentação de refinado no tanque de blowdown	a) Instalar sensores de posição (aberta / fechada) nas válvulas b) Diagnosticar e sinalizar falha de posição fechada das válvulas	a) SIS b) IHM	a) Chaves fim de curso de válvula aberta b) Chaves fim de curso de válvula fechada	não se aplica
Sensor 1 de nível alto de refinado	Falha do sensor 1	a) Falha do sensor 1 b) Erro na calibração c) Falha na alimentação do sensor 1	Falha de alarme de nível	a) Diagnosticar e sinalizar falha do sensor 1 b) Diagnosticar e sinalizar erro de calibração do sensor 1 c) Diagnosticar e sinalizar falha na alimentação do sensor 1	a) SIS b) IHM	não se aplica	não se aplica

Fonte: Exemplo de HAZOP. Extraído de (SQUILLANTE JR, 2017)

2.1.4 Análise de Árvore de Falhas – FTA

A Análise de Árvore de Falhas (FTA) é uma metodologia de raciocínio dedutivo que parte de um evento ou uma falha específica do sistema, denominada evento topo, e busca determinar as relações lógicas entre falhas de componentes e erros humanos que podem ser associados à ocorrência do evento topo (VILLEMEUR, 1992; ROUSH, 2000; MODARRES, KAMINSKIY e KRIVTSOV, 2009).

Descrita na IEC 61025 (IEC 61025, 2008), a análise é realizada através da construção de árvore lógica, partindo do evento topo para as falhas básicas. Utilizada para quantificar a frequência ou a probabilidade de falha do sistema, através da quantificação da probabilidade de falha de cada um dos componentes do sistema. Relações lógicas (+, *) (ou / e) indicam qualitativamente a relação causal entre cada ocorrência, até a geração do evento topo, que, em geral, é perda de uma funcionalidade, que pode envolver não somente componentes e/ou sistemas inteiros, mas também a execução de procedimentos operacionais.

Os eventos básicos da árvore de falhas podem ser eventos de falhas de componentes, sistemas ou uma falha do operador ao executar uma tarefa ou atividade.

De posse das probabilidades de ocorrência da falha, obtidos por dados estatísticos de bancos de dados pode ser quantificada a probabilidade de ocorrência do efeito topo (falha) por álgebra booleana.

Com base nos resultados obtidos, melhorias de projeto podem ser realizadas, como por exemplo alterações ou inserções de componentes ou subsistemas (como por exemplo paralelismos), com o objetivo do aumento da confiabilidade do sistema para níveis desejados, principalmente para os elementos críticos do sistema, que por sua vez podem ser identificados através do estudo do FMEA.

Um estudo qualitativo também pode ser realizado, não envolvendo os valores de probabilidades de ocorrência, somente o relacionamento lógico.

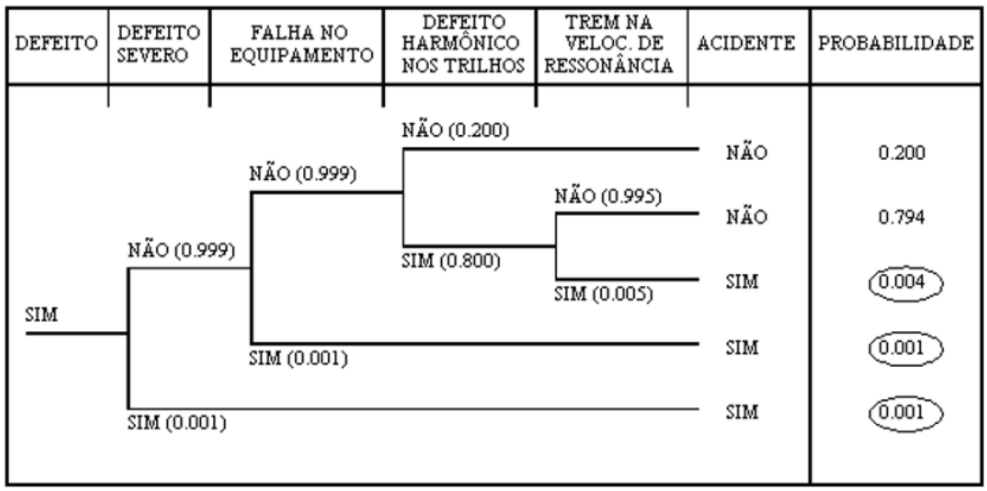
A vantagem da FTA sobre o FMEA é que o FTA é uma técnica que considera a combinação dos modos de falhas dos diversos componentes / subsistemas na ocorrência da falha, enquanto o FMEA, via de regra, é focada em um componente / subsistema.

2.1.5 Análise de Árvore de Eventos – AAE

Definida na norma (IEC 62502, 2010), parte-se de um evento resultante de uma falha específica de um equipamento ou erro humano, denominado evento iniciador, para determinar um ou mais estados subsequentes de falhas possíveis (VILLEMEUR, 1992; MODARRES, KAMINSKIY e KRIVTSOV, 2009; RAUSAND, 2011).

Desta forma, a AAE considera a ação a ser tomada pelo operador ou a resposta do processo para o evento inicial. Assim como na FTA, o estudo é realizado através de uma árvore, partindo-se do evento iniciador e as ações de sucesso ou insucesso, podendo estar associadas à probabilidades, com o objetivo de se mitigar os efeitos de ocorrência do evento iniciador. Para o contexto do presente trabalho, o de mitigar os efeitos da ocorrência do evento topo ou falha crítica. Um diagrama esquemático de uma árvore de eventos é representado na Figura 2.

Figura 2 – Exemplo de representação de árvore de eventos



Fonte: (TAKAYAMA, 2008)

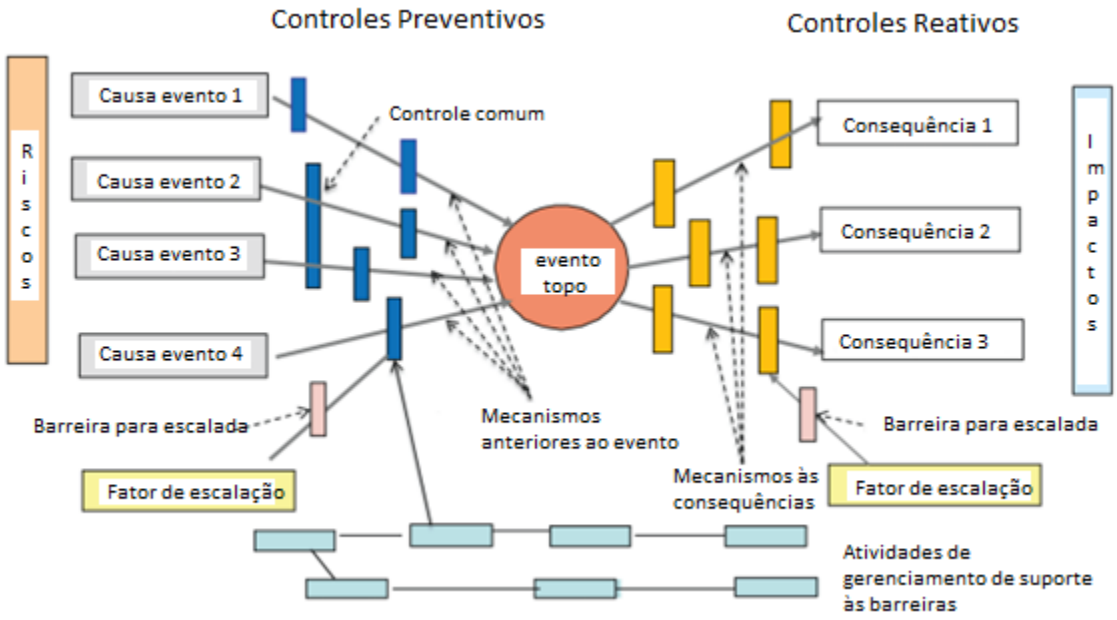
2.1.6 Método *bow-tie*

O *bow-tie,* definido na ABNT ISO/IEC 31010 (2012), é um método de avaliação de risco utilizado para analisar e demonstrar relações causais em cenários de risco, resultando em um diagrama (semelhante a um tipo de gravata masculina, por isso sua denominação) de possíveis cenários de acidentes, a partir da ocorrência de eventuais falhas de uma instalação. A partir destes cenários de falha, o diagrama permite com que sejam inseridas ações para evitar a ocorrência de eventos indesejados.

Historicamente, o *bow-tie* surgiu no início dos anos 1980, Austrália, a partir das análises de cenários de riscos de processos. Após a ocorrência de incidentes catastróficos relacionados à indústria petrolífera, no início dos anos 1990 o método foi utilizado para a identificação dos riscos e de seu gerenciamento (COCKSHOTT, 2005), a partir de um conjunto rígido de regras. Tal procedimento foi rapidamente adotado em outros ramos industriais e econômicos (DIANOUS, V. e FIEVEZ, C, 2006).

A elaboração do *bow-tie* parte do estudo da árvore de falhas (FTA), que irá formar o ramo esquerdo do diagrama, e o evento topo, ao centro. Já o lado direito do diagrama é elaborado por meio do estudo da árvore de eventos (AAE), a partir do evento topo indesejado. A Figura 3 ilustra um típico diagrama *bow-tie*.

Figura 3 - Representação de um diagrama *Bow-Tie*.



Fonte: Adaptado de (ABNT ISO/IEC 31010, 2012)

A estrutura de árvore de falhas, lado esquerdo do *bow-tie* representa os possíveis caminhos críticos e relações causa-efeito, representadas por conectores lógicos elementares até a ocorrência do evento topo. De posse das probabilidades da ocorrência de cada evento, por meio das propriedades de álgebra *booleana* é possível simplificar o modelo representativo da árvore de falhas e calcular a probabilidade de ocorrência do evento topo. No entanto, por tratar-se de sistemas críticos, e considerando-se as múltiplas linhas de defesa preconizadas no conceito de defesa em profundidade, e partindo-se da evidência de que o evento tenha probabilidade não nula de ocorrência, será, portanto, considerado para a prevenção de ocorrência do evento topo.

O lado direito do diagrama, após a ocorrência do evento topo, representa a árvore de eventos, que são todos os possíveis caminhos definidos a partir da ocorrência do evento topo, divididos pelo sucesso / insucesso das medidas de mitigação ao evento topo.

A avaliação de riscos de uma planta / processo pode resultar em vários eventos topo ou falhas críticas, com consequentes respectivos diagramas *bow-tie.*

2.1.6.1Fator de escalação e barreiras do fator de escalação

Como visto, os diagramas de *bow-tie* fornecem uma visão clara dos cenários de falhas e de suas relações causais, permitindo a inserção de medidas reativas para evitar a ocorrência de catástrofes. No entanto, o Psicólogo Cognitivo James T. Reason (REASON, 1997) propôs a metáfora do queijo suíço como modelo de causalidade do acidente.

A hipótese de Reason é de que riscos de uma instalação são impedidos de causar perdas por uma série de ações ou controles, inseridos nas instalações para o gerenciamento dos riscos, a partir dos resultados obtidos pelos diagramas *bow-tie.*

No entanto, Reason afirma tais controles nunca são 100% efetivos. Cada ação ou controle possui deficiências involuntáriase/ou falhas latentes, representanto o “furo” de um queijo suíço. O alinhamento destes “furos” pode representar uma deficiência das medidas pró-ativas e reativas e, na ocorrência de uma falha, pode resultar em um evento catastrófico. De acordo com Reason, as causas comuns das deficiências nos controles geralmente podem estar associadas à políticas organizacionais, tais como cortes de custos para o gerenciamento de manutenção, do que resulta na deterioração da integridade de muitos elementos de *hardware*. A Figura 4 ilustra o modelo proposto por Reason.

Figura 4 - Modelo do queijo suíço representando as falhas de medidas contentivas.

Fonte: Adaptado de (REASON, 1997)

No *bow-tie* tais deficiências são definidas como fatores de escalação (ABNT ISO/IEC 31010, 2012), sendo muito importantes na concepção de projeto das medidas pró-ativas e reativas. De forma geral o fator de escalação está associado ao(s) modos(s) de falha das medidas contentivas.

Deste modo, há uma lacuna na eficácia dos diagramas de *bow-tie*, do que implica em um gerenciamento dos fatores de escalação. Tal medida consiste na implementação das barreiras ao fator de escalação, que são medidas a serem adotadas para minimizar o impacto do fator de escalação das medidas contentivas.

2.2 NORMAS RELACIONADAS À SEGURANÇA EM INDÚSTRIAS DE PROCESSOS

As principais normas aplicadas à segurança em indústrias de processos, que referenciam o desenvolvimento odo presente trabalho são a IEC 61508 (IEC, 2010), a IEC 61511 (IEC, 2003), a *Health and Safety Executive* – HSE (HSE, 2006a), a norma técnica pública Petrobrás N-2782 (N-2782, 2015), e as normas de segurança de brigadas (ABNT NBR 14276, 2006) e dos requisitos do plano de emergência contra incêndio (ABNT NBR 15219, 2019) .

As subseções apresentam os aspectos relevantes das normas para a elaboração do trabalho.

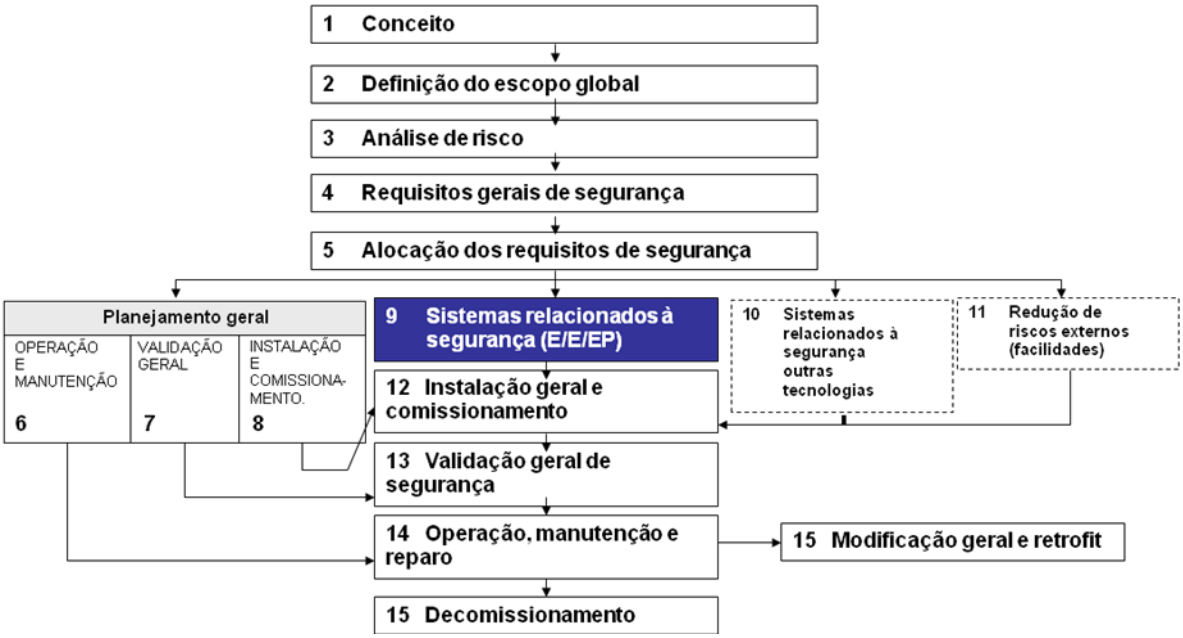
2.2.1 IEC 61508 / IEC 61511

A IEC 61508 é uma norma internacional desenvolvida pela *International Electrotechnical Commission* (IEC) que se aplica a segurança funcional de equipamentos elétricos, eletrônicos e eletrônicos programáveis (E/E/EP). Essa norma é considerada um documento padrão, pois outras normas para diferentes segmentos e aplicações são derivadas desta norma. A IEC 61508 tem dois objetivos:

- ✓ Orientar indústrias no desenvolvimento de normas suplementares que atendam aos requisitos de segurança de suas aplicações;
- ✓ Permitir o desenvolvimento de equipamentos E/E/EP relacionados à segurança, onde normas deste setor de aplicação não existem, sendo aplicada também para a certificação de hardwares e softwares destes equipamentos.

A norma IEC 61508 apresenta um conceito fundamental denominado de ciclo de vida de segurança. O ciclo de vida de segurança é definido como um processo de engenharia que inclui todos os passos necessários para se atingir a segurança funcional exigida. De acordo com a IEC 61508 (IEC 61508 parte IV, 2010), o ciclo de vida de segurança é definido como um conjunto de atividades necessárias envolvidas na implementação de SIFs, ocorrendo durante o período de tempo que começa na fase de concepção e finaliza quando todas as SIFS não são mais utilizadas. A Figura 5 representa o ciclo de vida de segurança, em referência às normas citadas.

Figura 5 - Ciclo de vida de segurança de SIS (Adaptado da IEC 61508; 2010).



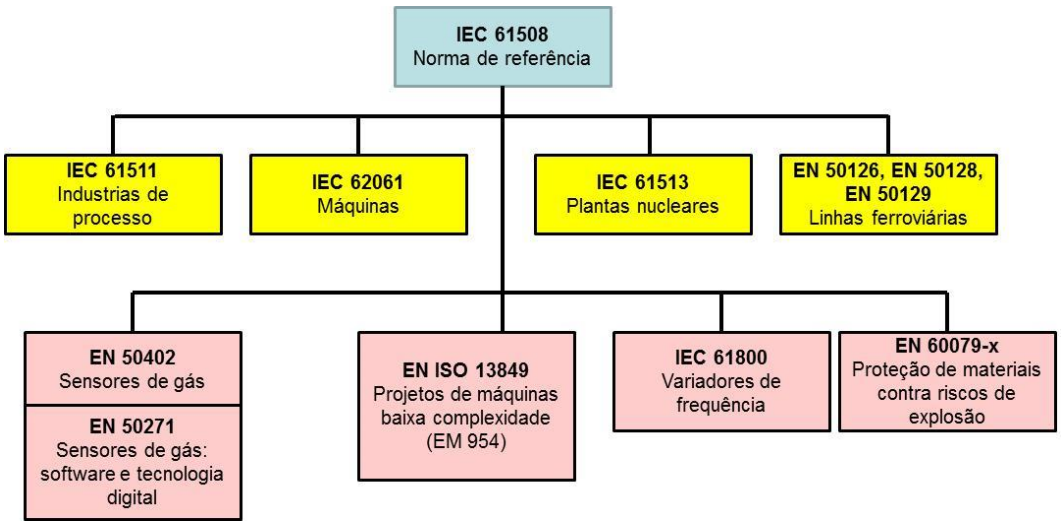
Fonte: Adaptado de (IEC: 61508, 2010)

Para cada fase deste ciclo de vida está relacionada uma ou várias partes da norma IEC 61508, abaixo transcritas:

- IEC 61508-1: requisitos gerais;
- IEC 61508-2: requisitos para sistemas E/E/EP relacionados à segurança;
- IEC 61508-3: requisitos de software;
- IEC 61508-4: definições e abreviações;
- IEC 61508-5: exemplos de métodos de determinação dos níveis de integridade de segurança (*SILs*);
- IEC 61508-6: orientações para aplicação da IEC 61508-2 e IEC 61508-3;
- IEC 61508-7: visualização geral de técnicas e medidas.

A IEC 61511 (IEC, 2003), derivada da IEC 61508 (IEC,2010), é a norma aplicável à indústria de processos, contexto do presente trabalho, conforme a Figura 6.

Figura 6 – Normas derivadas da IEC 61508. Adaptado de IEC 61508 (IEC, 2003)



Fonte: Adaptado de (IEC: 61508, 2010)

A norma IEC 61511 é constituída por três partes: IEC 61511-1 a IEC 61511-3, abaixo descritas:

- IEC 61511-1: estrutura, definições, sistema, requisitos de hardware e software;
- IEC 61511-2: orientações na aplicação da IEC 61151-1;
- IEC 61511-3: orientação para a determinação dos níveis de integridade de segurança (*SILs*) exigidos.

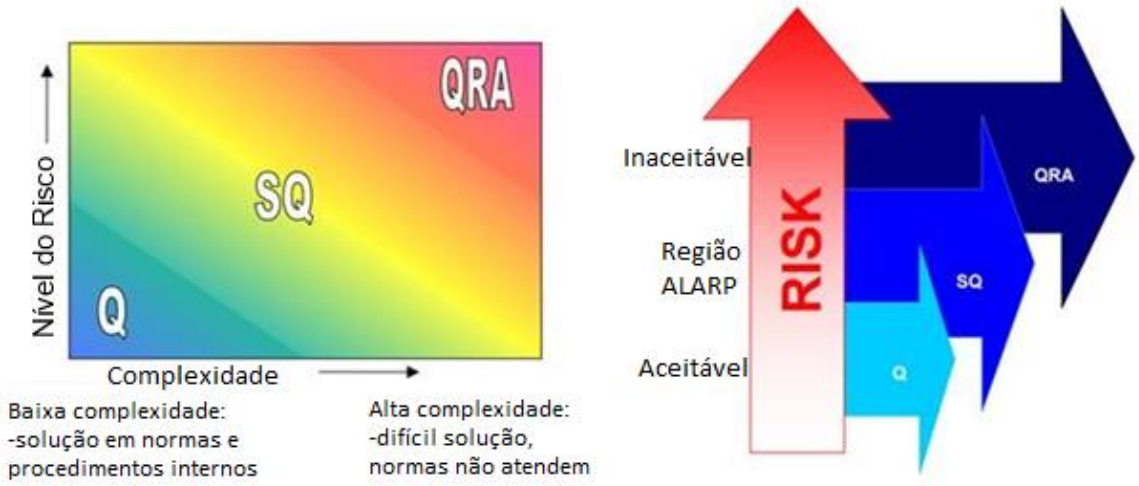
2.2.2 *Health & Safety Executive* - HSE

Para o correto desenvolvimento de um estudo de análise de risco é necessário definir a metodologia e as técnicas apropriadas. Isso deve basear-se no estudo sobre as características e complexidade da instalação e operações desenvolvidas e a atual fase do ciclo de vida da instalação.

De acordo com a HSE – *Health & Safety Executive* (HSE, 2006a), a metodologia de análise de risco de uma instalação deve fornecer as informações suficientes para a correta compreensão e avaliação do risco para que se possa tomar as medidas necessárias para sua redução. A norma prescreve três formas para a avaliação do risco em uma instalação. A norma tem como base a avaliação do risco em função da

complexidade do processo e do nível geral de risco. A Figura 7 ilustra a prescrição resumida da norma.

Figura 7 - Avaliação do risco em função da complexidade, complexidade e nível de risco.



Fonte: Adaptado de (HSE, 2006a)

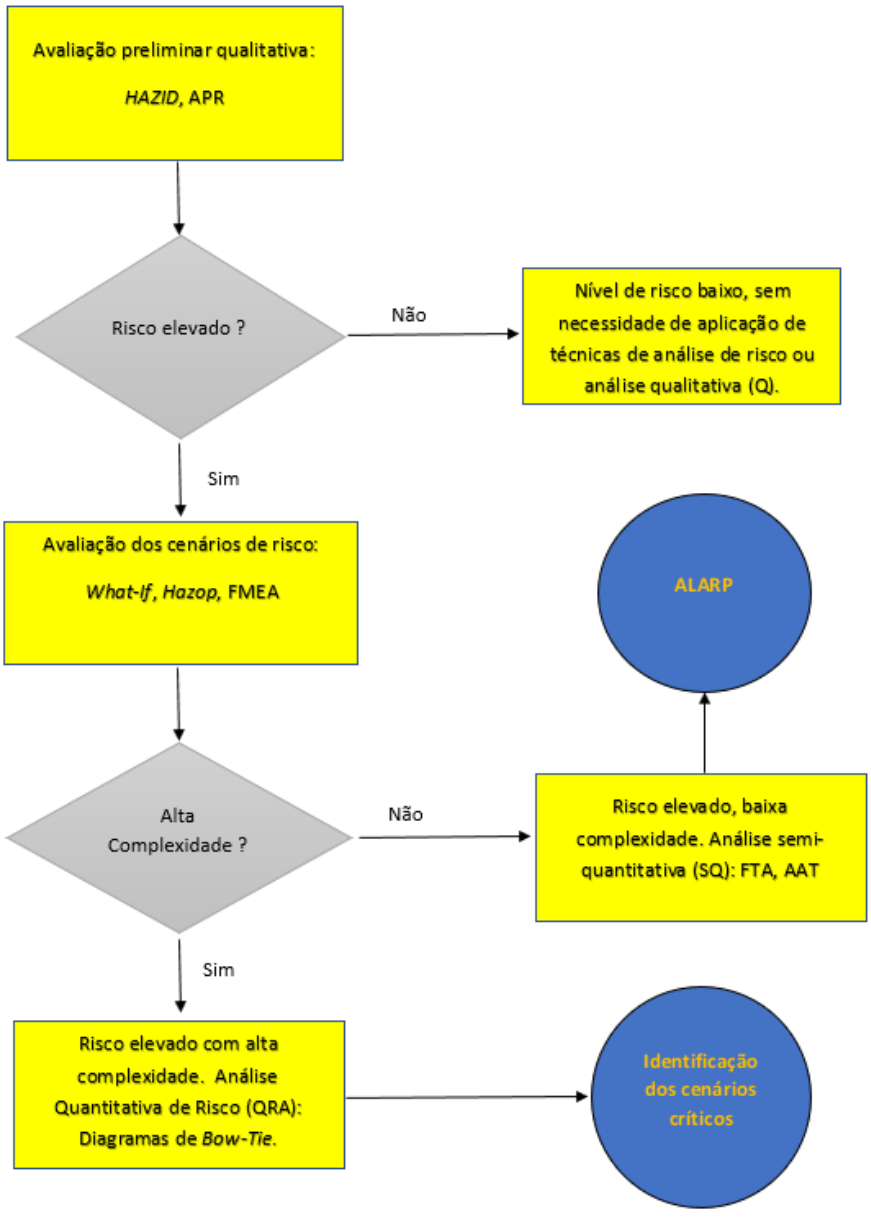
Observa-se que à medida que a magnitude do risco aumenta, o mesmo ocorre com o grau de complexidade na avaliação, que se reflete na abordagem metodológica a ser adotada. As seguintes abordagens podem ser aplicadas (HSE, 2006a):

- Qualitativa (Q): cada frequência e gravidade são determinadas qualitativamente, com base experiência da equipe multidisciplinar envolvida na análise;
- Semi-quantitativa (SQ): cada frequência e gravidade são quantificadas dentro de intervalos numéricos;
- Análise quantitativa de risco (QRA): quando há uma quantificação completa, geralmente é utilizada na determinação da frequência / consequências a grandes eventos acidentais.

O nível de detalhamento é crescente a partir da metodologia qualitativa para a quantitativa, e a escolha da metodologia é obtida a partir da análise preliminar de riscos da instalação e de sua complexidade, além dos efeitos que poderiam surgir em função da ocorrência de falhas críticas.

De forma auxiliar, a norma HSE (HSE, 2006a) orienta o fluxograma representado na Figura 8 para o desenvolvimento do estudo de análise de risco do processo e as técnicas de análise de riscos pertinentes para cada etapa.

Figura 8 - Fluxograma para o desenvolvimento do estudo de análise de risco.



Fonte: Adaptado de (HSE, 2006a)

2.2.3 N2782 – Petrobrás

As Normas Técnicas Petrobrás são elaboradas por Grupos de Trabalho – GT (formados por Técnicos Colaboradores especialistas da Companhia e de suas Subsidiárias), são comentadas pelas Unidades da Companhia e por suas Subsidiárias, são aprovadas pelas Subcomissões Autoras – SC (formadas por técnicos de uma mesma especialidade, representando as Unidades da Companhia e as Subsidiárias) e homologadas pelo Núcleo Executivo (formado pelos representantes das Unidades da Companhia e das Subsidiárias).

Como requisito técnico e aplicabilidade, a Norma é entendida como a mais adequada e que deve ser utilizada estritamente em sua conformidade. Uma eventual resolução de não seguimento ou procedimento que venha a ser adotado em não conformidade com a Norma deve ter fundamentos técnico-gerenciais e deve ser aprovada e registrada pela Unidade da Petrobrás usuária desta norma. É caracterizada por verbos de caráter impositivo (CONTEC).

As Normas Técnicas são estruturadas, de forma geral, em: i) Escopo da aplicação; ii) As Referências Normativas, que são Normas indispensáveis à aplicação da referida Norma; iii) Termos e Definições, em que são apresentados os termos de aplicabilidade da norma e as definições dos termos técnicos utilizados na norma; iv) Condições Gerais, que são as condições gerais de aplicabilidade da Norma e v) Condições específicas, que contém eventuais particularidades da aplicação da Norma.

Dentre as NTPs destacam-se, para o foco do presente trabalho, a Norma N-2782, que referencia os critérios para aplicação de técnicas de avaliação de riscos; ou seja, dependendo da etapa do ciclo de vida da instalação / empreendimento, a N-2782 relaciona a(s) técnica(s) obrigatórias e recomendadas para a avaliação do risco. Tais recomendações são reproduzidas na Tabela 3.

Tabela 3 – Técnicas a serem aplicadas nas diversas fases do ciclo de vida do empreendimento.

Fases do Empreendimento	Técnicas Utilizadas										
	1	2	3	4	5	6	7	8	9	10	11
EVTE	R		O	R							
Projeto Conceitual	R		O	R							
Projeto Básico / Bases Projeto / IBE			O		O	R	R	R	O	R	
Projeto de Detalhamento			O		O	R	R	R	O	R	
Construção e Montagem		R	O	R							
Comissionamento		R	O								
Operação		R	O	R	O	R	R	R	R	R	O
Ampliação/Modificação		R	O	R	O	R	R	R	R	R	
Descomissionamento	R	R	O								

Onde:

O = Técnica Obrigatória;
R = Técnica Recomendada.

Legenda (descrição das técnicas):

1 - Análise Histórica;
2 - Lista de Verificação (“Checklist”);
3 - APR (Análise Preliminar de Riscos);
4 - E se? (What if?);
5 - HAZOP (Estudos de Perigos e Operabilidade);
6 - FMEA/FMECA (Análise de Modos e Efeitos de Falhas);
7 - Análise por Árvore de Falhas;
8 - Análise por Árvore de Eventos;
9 - Análise de Conseqüências;
10 - AQR (Avaliação Quantitativa de Riscos);
11 - Levantamento de Aspectos e Impactos.

Fonte: (N-2782, 2015)

A partir da seleção da(s) técnica(s) de análise de risco, a N-2782 preconiza três categorias de riscos qualitativas: a categoria de risco tolerável (T), a categoria moderada (M) e a categoria Não Tolerável (NT). Para cada categoria de risco, a norma recomenda o nível de controle necessário. Tais categorias e recomendações são apresentadas na Tabela 4.

Tabela 4 – Categorias de Riscos. Extraído de (NTP N-2782 – PETROBRÁS)

Categoria de Risco	Descrição do Nível de Controle Necessário
Tolerável (T)	Não há necessidade de medidas adicionais. A monitoração é necessária para assegurar que os controles sejam mantidos.
Moderado (M)	Controles adicionais devem ser avaliados com o objetivo de obter-se uma redução dos riscos e implementados aqueles considerados praticáveis (conceito "ALARP").
Não Tolerável (NT)	Os controles existentes são insuficientes. Métodos alternativos devem ser considerados para reduzir a probabilidade de ocorrência e, adicionalmente, as conseqüências, de forma a trazer os riscos para regiões de menor magnitude de riscos (níveis "ALARP" ou toleráveis).

Fonte: (N-2782, 2015)

Após o resultado da aplicação da(s) técnica(s) de análise de riscos e da classificação quanto ao risco, a norma prescreve a classificação quanto às possíveis consequências dos eventos de perigo identificados. São consideradas quatro categorias de severidade:

- Desprezível;
- Marginal;
- Crítica;
- Catastrófica.

Cada categoria de severidade por sua vez é associada a um tipo de dano:

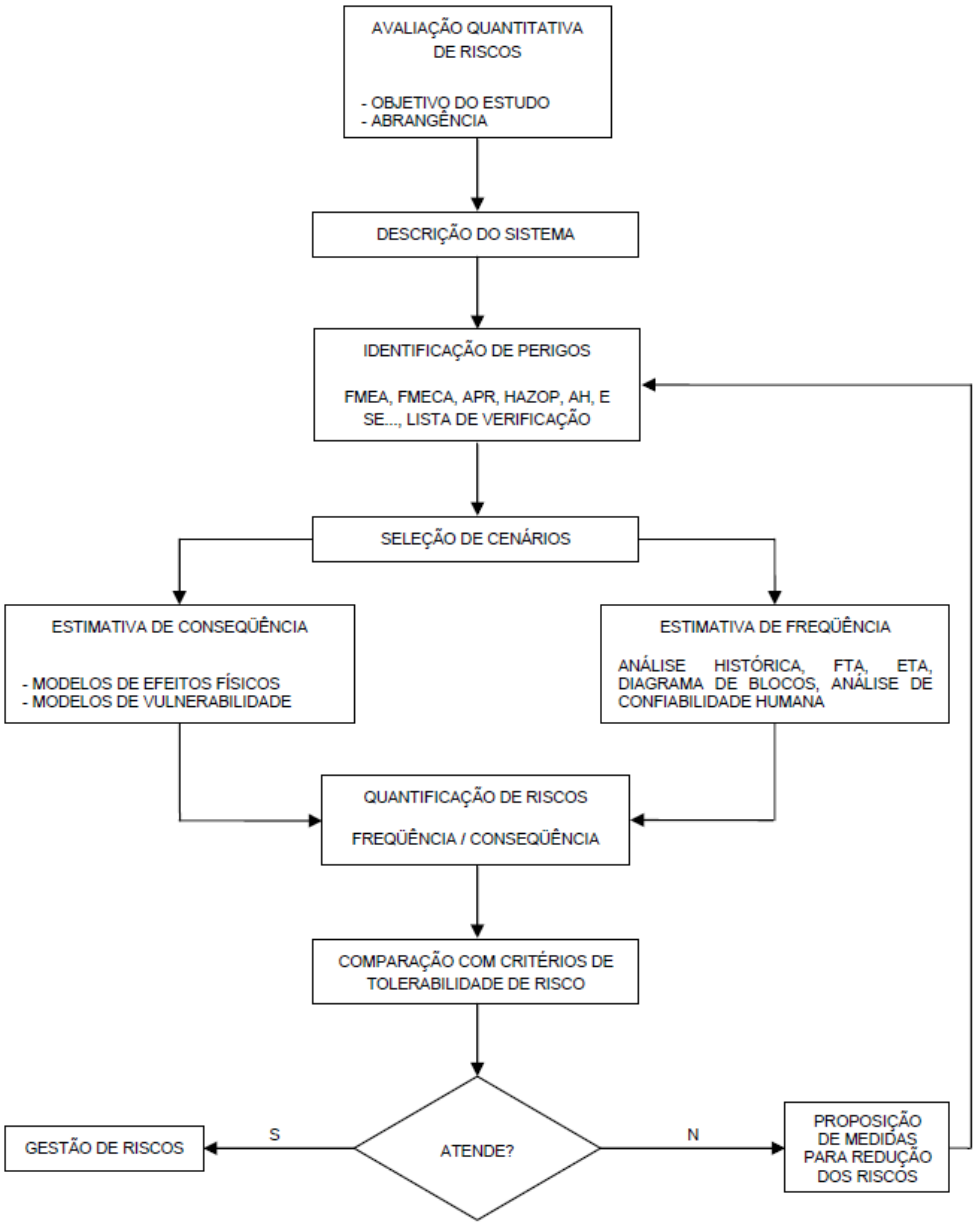
- À segurança pessoal;
- Às instalações;
- Ao meio ambiente;
- À imagem da empresa.

A classificação da consequência de ocorrência e do tipo de dano são comparados com a categoria de frequência da ocorrência:

- Remota: B (em 10^3 a 1 em 10^6 anos);
- Pouco provável: C (1 em 30 a 1 em 10^3anos);
- Provável: D (1 por ano a 1 em 30 anos);
- Frequente E: mais que 1 por ano.

A norma ainda recomenda o uso do fluxograma representado na Figura 9 para a avaliação quantitativa de riscos e seleção dos cenários de riscos em função de sua tolerabilidade.

Figura 9 - Fluxograma para a avaliação quantitativa de riscos.



Fonte: (N-2782, 2015)

Por fim, a norma preconiza que toda análise de risco deve gerar uma documentação na qual fiquem registradas as seguintes informações:

- Os perigos identificados e suas respectivas causas;
- As consequências que podem advir da concretização de cada perigo;
- As medidas de prevenção aplicáveis, de forma a evitar o surgimento de cada causa;
- As medidas de mitigação aplicáveis, de forma a reduzir os efeitos decorrentes da concretização de cada perigo.

2.2.4 Normas de segurança – brigadas

Toda e qualquer instalação, industrial, comercial ou residencial, com exceção das edificações residenciais unifamiliares, devem ter um plano de emergência contra incêndio. (ABNT NBR 15219, 2019).

Nesse sentido, a norma ABNT NBR 15219 (ABNT NBR, 2019) “estabelece os requisitos mínimos para a elaboração, implantação, manutenção e revisão de um plano de emergência contra incêndio, visando proteger a vida e o patrimônio, bem como reduzir as consequências do sinistro e os danos ao meio ambiente”.

A norma apresenta as definições de vernáculos associados ao tema, como por exemplo “bombeiro profissional civil”, “brigada de incêndio”, “grupo de apoio” etc.

Para a implantação do plano de emergência contra incêndio, alguns requisitos devem ser atendidos, como por exemplo a rotina periódica de exercícios simulados.

Considerando o contexto do presente trabalho, destacam-se os exercícios simulados de falhas dos equipamentos e falhas operacionais, e recomenda, por meio de um fluxograma, a sequência dos procedimentos de emergência, incluindo-se a solicitação de apoio externo.

A ABNT NBR 15219 menciona outra norma correlata, que é a ABNT NBR 14276 (ABNT NBR, 2006) fornecendo os subsídios para a definição das equipes de brigadas.

Nesse sentido, a norma “estabelece os requisitos mínimos para a composição, formação, implantação e reciclagem de brigadas, preparando-as para atuar na prevenção e no combate ao princípio de incêndio e primeiros socorros, visando, em caso de sinistro, proteger a vida e o patrimônio, reduzir as consequências sociais di sinistro e os danos ao meio ambiente”.

A norma apresenta as definições de termos associados às brigadas e suas ações, com destaque, considerando o contexto do presente trabalho, para a definição formal de uma brigada de incêndio: “grupo organizado de pessoas...treinadas e capacitadas para atuar na prevenção e no combate ao princípi ode incêndio...dentro de uma área pré-estabelecida na planta”. (ABNT NBR 14276, 2006).

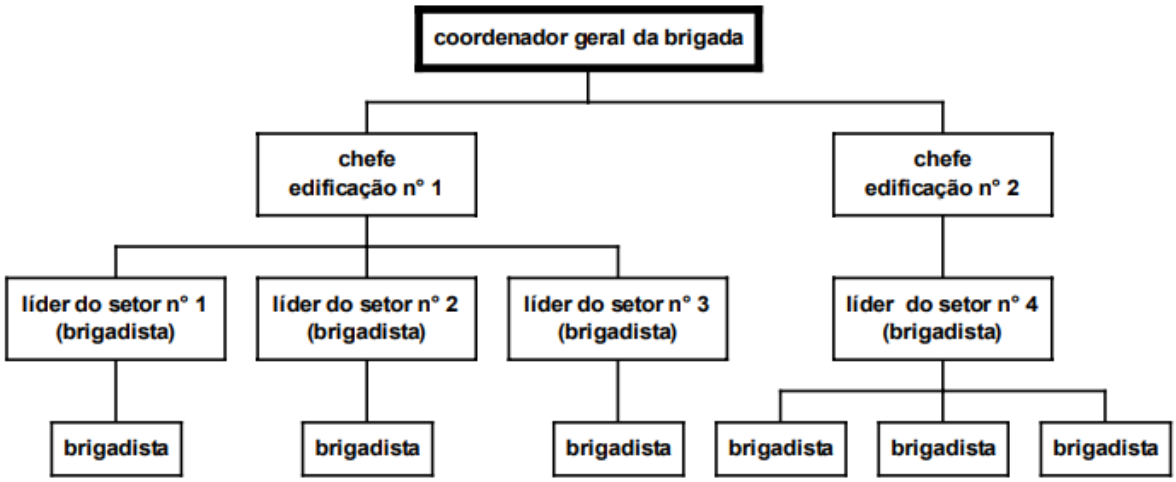
Já o “coordenador geral da brigada” é o “brigadista responsável pela coordenação e execução das ações de emergência de todas as edificações que compõe uma planta, independentemente do número de turnos” (ABNT NBR 14276, 2006).

A norma relaciona a composição da brigada de incêndio por pavimento ou compartimento, e as cargas mínimas de combate a incêndio em função do tipo da instalação e da categoria de risco associado, em função da energia em joules por metro quadrado:

- Risco alto: planta com carga de incêndio acima de 1.200 MJ/m²;
- Risco baixo: Planta com carga de incêndio até 300 MJ/m²;
- Risco médio: entre 300 MJ/m² e 1.200 MJ/m²;
- Risco iminente: risco que requer ação imediata.

A norma define o organograma para a formação das brigadas, como por exemplo: uma planta com duas edificações, a primeira com três pavimentos e dois brigadistas por pavimento, e a segunda com um pavimento e quatro brigadistas por pavimento. A Figura 10 apresenta o organograma para a estrutura mencionada.

Figura 10 – Exemplo de organograma de brigadas



Fonte: (ABNT NBR 14276, 2006)

2.3 DEFESA EM PROFUNDIDADE

Sklet (2006), descreve o princípio de defesa em profundidade da seguinte maneira:

- ✓ "*Para compensar falhas mecânicas e erros humanos, defesa em profundidade é implementada centrada em vários níveis de proteção, incluindo sucessivas barreiras prevenindo a liberação de material radioativo para o meio ambiente. O princípio inclui a proteção das barreiras para evitar danos à planta (processo) e para a proteção das próprias barreiras. Adicionalmente, inclui medidas para a proteção do público e do meio ambiente de riscos em caso das funções das barreiras não serem completamente efetivas*".

Nesse sentido, o conceito de defesa em profundidade é fundamental para se atingir um estado de segurança de um sistema, e acidentes tipicamente resultam da ausência ou brecha de defesas ou violação das restrições de segurança. (SALEH, MARAIS, *et al.*, 2010; BAKOLAS e SALEH, 2011).

O princípio de defesa em profundidade incorpora a ideia de múltiplas linhas de defesa, estabelecendo os caminhos ou cenários até a ocorrência de uma falha crítica, em

diferentes estágios, para auxiliar o projetista a incorporar as devidas barreiras de segurança para a prevenção da ocorrência da falha crítica.

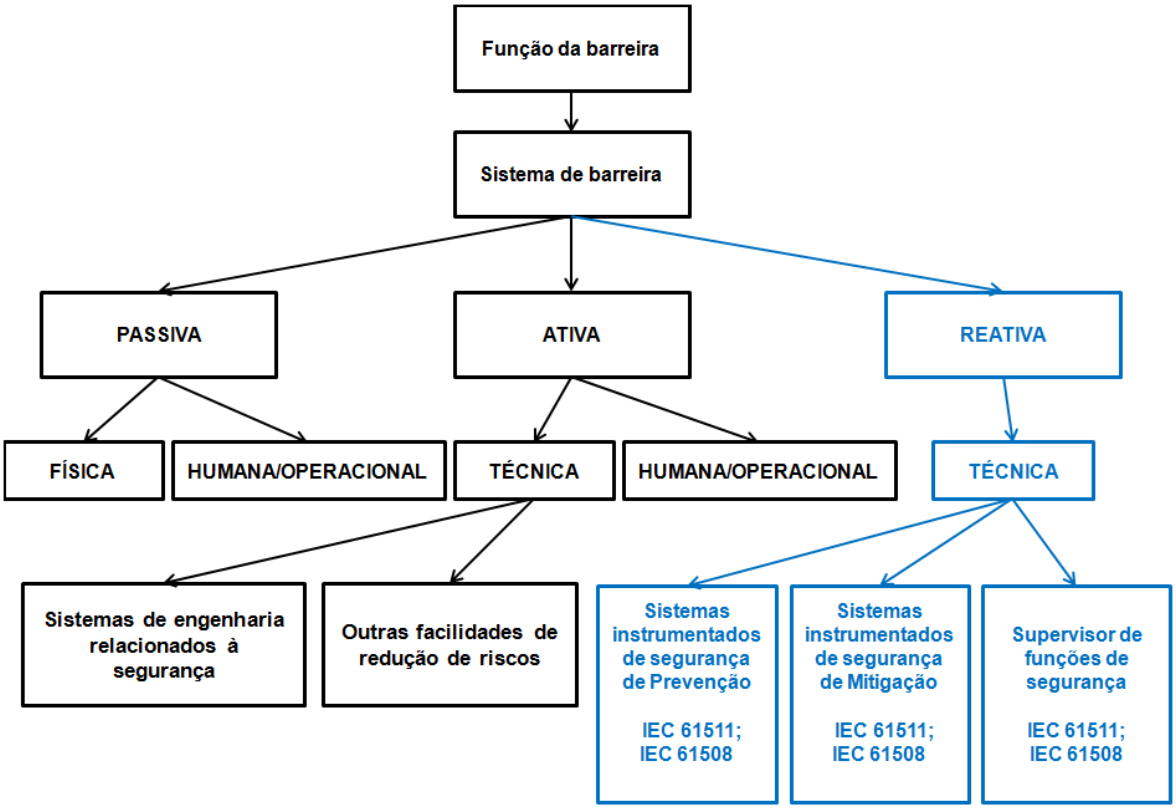
Caso uma determinada sequência de barreiras sejam ineficazes, e o evento topo indesejado ocorrer, um sistema de barreiras deverá ser inserido para mitigar os efeitos de ocorrência da falha crítica. Um dos efeitos indesejados é a escalação entre eventos topo, ou seja, a ocorrência dos demais eventos topo em função de seus efeitos.

As barreiras de segurança podem ser de diversas naturezas, do que resultou na classificação proposta por Sket (2006) da seguinte forma:

- Barreiras passivas físicas: funcionam continuamente e não necessitam ser ativadas. Exemplos: diques de contenção, paredes de proteção contra incêndio, muros etc).
- Barreiras passivas humanas/operacionais: distância segura de operadores em atividades / processos com elevada energia (HADDON, 1990).
- Barreiras ativas humanas/operacionais: barreiras implementadas por recursos humano-operacionais, em modo contínuo ou ativados sob demanda. Exemplo: acionamento manual de um alarme ou atuação humana quando um alarme é ativado, ou ainda a ação das brigadas de incêndio.
- Barreiras ativas técnicas: são implementadas por elementos de *hardware*, que por sua vez são constituídas por dispositivos elétricos, eletrônicos ou eletrônico-programáveis, que é performada quando detectado por um evento inicializador, detectado por exemplo por meio de um sensor.

Partindo-se das classificações de barreiras de Sklet (2006), Squillante Jr (2017) propõe uma nova classificação de barreiras de segurança, que são as barreiras reativas de prevenção e mitigação, implementadas por meio do conceito de SIS. A Figura 11 ilustra a nova classificação de barreiras proposta, a partir da classificação de Sklet (2006).

Figura 11 – Classificação das barreiras de segurança



Fonte: (SQUILLANTE JR, 2017)

O presente trabalho tem como base[2] a classificação de barreiras de segurança proposta por Squillante Jr (2017).

2.3.1 Camadas de Redução de Riscos

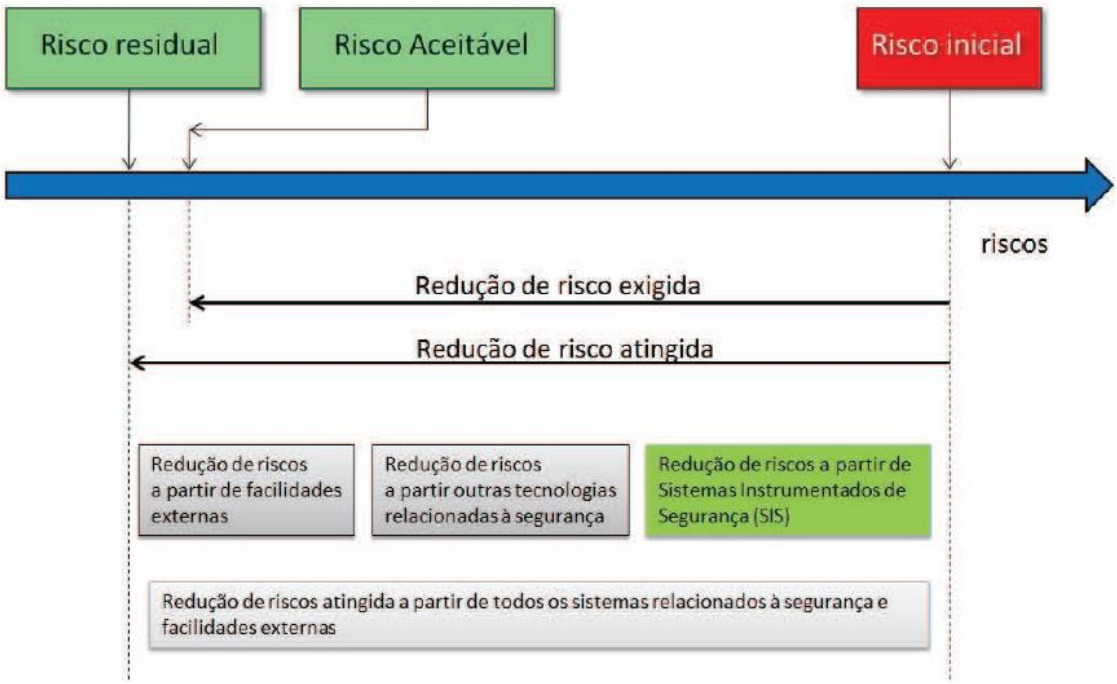
De acordo com a norma IEC 61508 (IEC, parte IV, 2010) e IEC 61511 (IEC, 2003), camadas de redução de riscos, baseadas em sistemas de controle, podem ser estruturadas de forma hierárquica, sendo compostas por dispositivos, sistemas ou ações capazes de prevenir e/ou mitigar cenários com consequências indesejáveis.

[2] O trabalho propõe uma nova classe de barreiras (seção 3.2)

Tais camadas devem ser independentes entre si (CRUZ-CAMPA e CRUZ-GOMEZ, 2009).

A Figura 12 apresenta a redução do risco inicial de um processo industrial ao nível de risco aceitável, uma vez que é impossível do ponto de vista prático, aplicar o princípio da eliminação de riscos (HOLLNAGEL, 2007).

Figura 12 - Redução de riscos – conceitos gerais.



Fonte: (SQUILLANTE JR, 2011)

As várias classes de medidas associadas à redução do risco de um processo podem ser representadas a partir de um modelo de camadas de redução de riscos. Considerando o escopo do presente trabalho, as camadas de prevenção e mitigação são implementadas por meio de barreiras de segurança reativas para a prevenção e para a mitigação, fazendo-se uso do conceito de Sistemas Instrumentados de Segurança - SIS (seção 2.4). A Figura 13 representa o modelo de camadas de redução de riscos proposto pela (IEC, 2010).

Figura 13 - Camadas de redução de riscos

Fonte: Adaptado da IEC 61511-1 (IEC, 2003)

De acordo com (GOBLE e CHEDDIE, 2005), o SIS monitora variáveis de processo e quando limites especificados de segurança são confirmados, o SIS inicia ações de prevenção e/ou mitigação. De acordo com (GOBLE e CHEDDIE, 2005), como a operação de um SCBP é continua e existe grande dinâmica na variação dos sinais desse sistema de controle, suas falhas podem ser mais facilmente detectadas pelo operador. No caso do SIS, como esse sistema de controle de segurança entra em ação somente quando uma condição potencialmente perigosa é detectada, pode ser muito difícil para o operador detectar alguns tipos de falhas sob controle exclusivo do SIS, principalmente quando, independentemente dessa falha, o processo continua aparentemente operando de forma normal para o SCBP.

Finalmente (GOBLE e CHEDDIE, 2005) argumentam que um SIS, como um sistema de controle básico de processo (SCBP), é composto de sensores, controladores e elementos finais. Embora boa parte do hardware pareça similar, esses sistemas têm semânticas de controle diferentes e é fundamental haver autonomia em termos de

sistema de controle entre eles, ou seja, um SIS jamais pode depender de controladores, sensores e elementos finais de um SCBP.

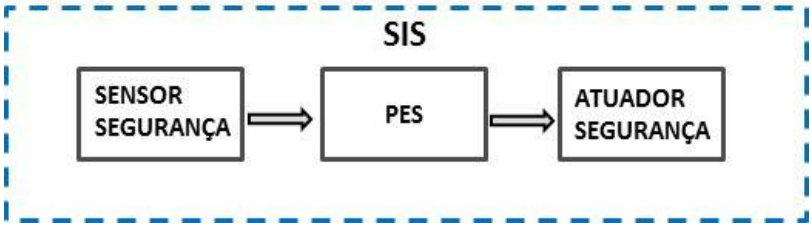
2.4 SISTEMAS INSTRUMENTADOS DE SEGURANÇA

Sistemas Instrumentados de Segurança (SIS) constituem uma solução tecnológica de um sistema de controle de segurança que tem como objetivo reduzir os riscos em processos industriais, quando estes riscos forem identificados e quantificados como inaceitáveis durante a operação desses processos IEC 61508 (IEC – parte IV, 2010). De uma forma geral, o SIS pode atuar de duas formas: (i) para prevenção da ocorrência de falhas críticas e/ou (ii) para mitigação as consequências geradas pela ocorrência de falhas críticas.

A implantação de um SIS é uma medida de segurança que constitui uma ou mais camadas de redução de riscos previstas na norma IEC 61511 (IEC, 2003) para manter a operação de um processo industrial com um nível aceitável de risco. Esta condição só é possível de ser atingida se todas as medidas de redução de risco forem planejadas de forma adequada, pois medidas isoladas ou mal gerenciadas não previnem contra a maioria dos acidentes.

O SIS pode ser implementado a partir do uso de sistemas mecânicos, elétricos, eletrônicos e eletrônicos programáveis (E/E/EPs). Este trabalho aborda o projeto de SIS a partir do uso de sistemas eletrônicos programáveis (PESs) ou controladores programáveis (CPs) de segurança. A Figura 14 ilustra em diagrama de blocos, os componentes de hardware de um SIS a partir do uso de PES. O SIS é constituído por um ou mais sensores de segurança, um ou mais controladores programáveis de segurança (PESs) e um ou mais atuadores de segurança (LUNDTEIGEN; RAUSAND, 2009).

Figura 14 - Componentes de hardware de um SIS a partir do uso de PES



Fonte: Adaptado de (LUNDTEIGEN e RAUSAND, 2009)

De acordo com Lundteigen e Rausand (2009), um SIS é instalado para detectar eventos críticos (ex.: vazamento de gás, altas pressões) para evitar ou mitigar suas consequências aos seres humanos, meio-ambiente e equipamentos. Adicionalmente, Rouvroye e Van Den Bliek (2002) argumentam que o SIS é aplicado para trazer o processo industrial a um estado seguro (ex.: desligamento de emergência quando pré-condições de variáveis de controle são violadas).

Neste contexto, a função de um SIS é monitorar através de sensores de segurança, eventos críticos no processo industrial e indicar alarmes ou executar ações pré-programadas, através de atuadores de segurança, para a prevenção de acidentes e/ou mitigação das consequências geradas pela ocorrência desses eventos (GOBLE, 1998).

Como consequência, o conceito de SIS promove a redução de riscos quantificados como inaceitáveis para níveis aceitáveis baseados em regras e decisões corporativas, por meio do controle de prevenção e/ou controle da mitigação de falhas críticas.

2.4.1 Função instrumentada de segurança (SIF)

O SIS implementa uma ou mais funções instrumentadas de segurança (*Safety Instrumented Function* (SIF)). Cada SIF objetiva detectar um evento indesejável e automaticamente tomar ações apropriadas para mover o processo para um estado seguro (CRUZ-CAMPA e CRUZ-GOMES, 2009).

Do ponto de vista de hardware, um SIS implementa suas SIFs por meio de:

• um ou mais sensores (ex.: temperatura, pressão, nível, fogo, fumaça, concentração de gás, etc.);

• um ou mais dispositivos elétricos / eletrônicos / eletrônico programáveis (E/E/EPs) onde EP também denominado de PES é um controlador programável de segurança;

• um ou mais atuadores (ex.: válvulas de segurança, chaves elétricas, etc.).

2.4.2 Nível de integridade de segurança (SIL)

O nível de integridade de segurança (*Safety Integrated Level* (SIL)) é a medida da segurança que se espera do SIS na realização de sua função quando solicitado (DUTUIT, INNAL, *et al.*, 2008), ou seja, o SIL reflete aquilo que os usuários finais podem esperar de um dispositivo ou sistema na sua função e, em caso de falha, que a falha ocorra de maneira segura. Falha segura é aquela que quando diagnosticada, faz com que o SIS degenere de forma controlada o processo industrial, levando este processo para um estado seguro. SILs podem ser definidos como medidas de segurança associadas a sistemas e seus componentes.

Neste contexto, a norma IEC 61508 (IEC parte IV, 2010), considera que existem quatro classes de SIL, representado por meio da Tabela 5.

Tabela 5 – Níveis de integridade de segurança (SIL)

Nível de Integridade de Segurança SIL	Fator de Redução de Risco RRF	Probabilidade média de falha na demanda PFD_{avg}
SIL 4	100000 a 10000	$>=10^{-5}$ a $<10^{-4}$
SIL 3	10000 a 1000	$>=10^{-4}$ a $<10^{-3}$
SIL 2	1000 a 100	$>=10^{-3}$ a $<10^{-2}$
SIL 1	100 a 10	$>=10^{-2}$ a $<10^{-1}$

Fonte: Adaptado de (IEC: 61508 PARTE IV, 2010)

2.5 DIAGNOSTICABILIDADE SEGURA

Bakolas e Saleh (2011) propõem que todos os eventos críticos (falhas críticas) e que demandam a função das barreiras de segurança sejam observados e diagnosticados sem a existência de ambiguidades na indicação/sinalização das falhas críticas.

O princípio tem como base a teoria de controle de sistemas a eventos discretos (SEDs) e é classificado como diagnosticável se um observador externo puder inferir sobre o sistema tendo alcançado um estado de risco, com pleno conhecimento de todos os eventos observados que o sistema executa (PAOLI, A. e LAFORTUNE, S., 2005).

Os autores defendem este princípio fundamental de segurança para o projeto e operação de sistemas complexos, o qual pode ser definido como: "*adicionalmente à estratégia de defesa em profundidade para se atingir a segurança de um sistema, propõe-se que todos os eventos indesejados para a segurança e que a defesa em profundidade pretende se proteger contra, seja diagnosticável".* Este princípio de diagnosticabilidade segura pode ser implementado de várias maneiras, por meio de escolhas de projeto e escolhas técnicas, assim como, por meio de procedimentos operacionais, assim como, defesa em profundidade e barreiras de segurança são implementadas por meio de uma variedade de meios.

O princípio da diagnosticabilidade segura não é proposta como uma alternativa para a estratégia de defesa em profundidade, uma vez que ele não atua sobre eventos adversos ou sequência de acidentes, que é o domínio das barreiras de segurança e defesa em profundidade. Entretanto, o princípio de diagnosticabilidade segura fornece um importante complemento sem o qual, a estratégia de defesa em profundidade poderá degenerar-se para uma estratégia de defesa cega, comprometendo a efetividade da defesa. A adoção deste princípio à estratégia de defesa em profundidade pode resultar em um estreitamento de relação de trabalho entre analistas de riscos, gestores de segurança, projetistas de sistemas, operadores e profissionais de manutenção; e como resultado ele deve contribuir para a melhoria da segurança de sistemas e prevenção de acidentes em muitas indústrias de processos (BAKOLAS e SALEH, 2011).

3. METODOLOGIA PROPOSTA

Uma vez que a indústria de processos é susceptível à ocorrência de eventos críticos que podem ocorrer de forma independente e provocar a interação entre falhas críticas, este capítulo descreve uma metodologia para o desenvolvimento de um sistema de controle de segurança para processos críticos, que seja capaz de atender aos princípios de segurança em profundidade e diagnosticabilidade segura. Desta forma, a proposta necessita atender aos seguintes requisitos fundamentais:

- Estabelecer a síntese de uma arquitetura modular, distribuída e integrada a um sistema supervisório de controle de segurança;
- Permitir a interação entre os módulos de controle para classificações distintas de barreiras;

Neste contexto, como premissa são definidas as hipóteses que são consideradas para o desenvolvimento da metodologia proposta:

- O uso da abordagem de controle de sistemas a eventos discretos (SEDs) é adequado à modelagem e análise de questões relacionadas a sistemas de segurança (BAKOLAS e SALEH, 2011);
- A dinâmica do comportamento de ocorrência de falhas críticas em indústria de processos é orientada pela ocorrência de eventos críticos que podem ser considerados instantâneos. Portanto, cada elemento / componente presente no sistema (planta/processo) pode ser modelado como pertencente a classe de sistemas do tipo SED, ou seja, cada item possui um conjunto finito de estados (m-ários) mutuamente exclusivos. Por sua vez, quanto à detecção de eventos críticos que podem ocorrer nestes sistemas, será considerada a hipótese de cada um de seus elementos poder assumir somente dois estados que são mutuamente exclusivos: estado normal (p.ex.: nível lógico 0) ou em estado de falha (p.ex.: nível lógico 1). (ABNT NBR 5462, 1994; N-2782, 2015; IEC 61508 parte IV, 2010; BASILIO, J.C., CARVALHO, L.K. e MOREIRA, M.V., 2010; SQUILLANTE JR, 2011);

- Considerando-se variáveis contínuas de monitoramento de equipamentos e/ ou variáveis de processos que podem estar associadas à ocorrência de falhas

críticas, o desvio (acima ou abaixo) fora dos limiares considerados seguros para a planta / processo, considerando-se critérios de filtragem espúrias, são considerados como variáveis binárias. (SOUZA, J.A.L, SANTOS FILHO, D.J., *et al.*, 2017);

- Considerando o contexto de sistemas críticos, em havendo probabilidade de ocorrência de um evento crítico, ainda que em frequência reduzida, o mesmo será considerado para a síntese dos algoritmos de controle de segurança;

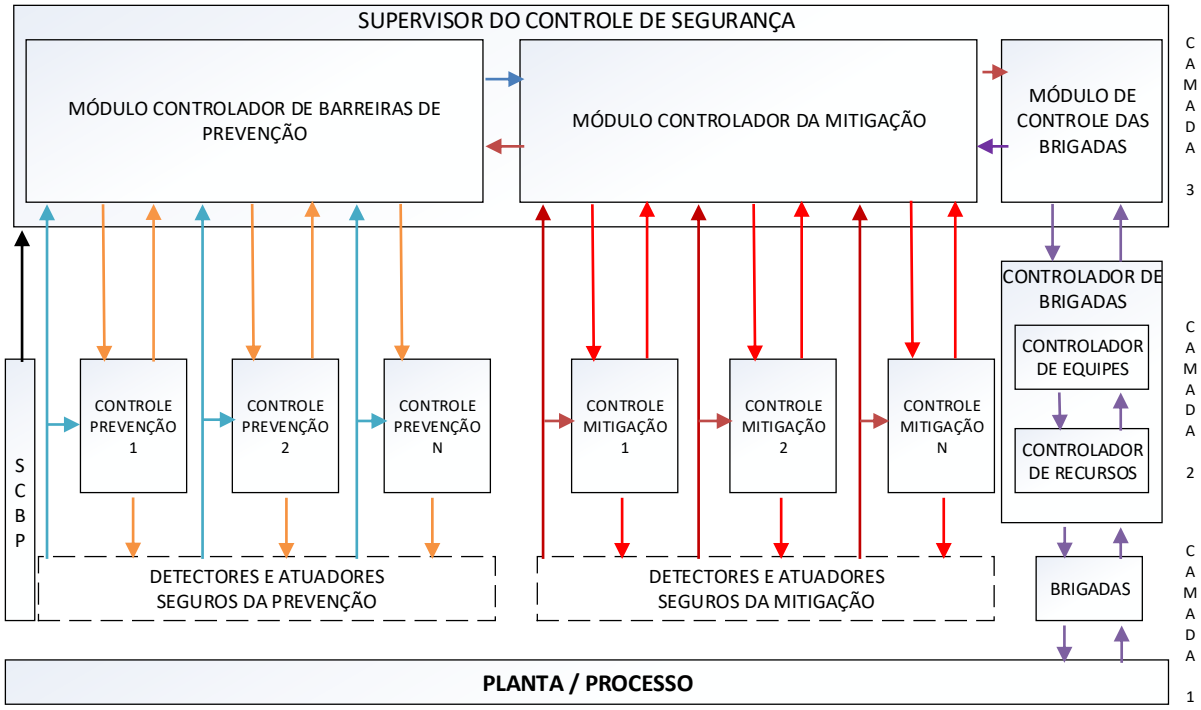
- Para a síntese dos algoritmos de controle de segurança os aspectos de observabilidade e rastreabilidade de eventos críticos devem ser satisfeitos de acordo com o conceito de diagnosticabilidade segura;

Na sequência, apresenta-se a metodologia proposta: a partir da exposição da arquitetura do sistema de controle de segurança, é feito o detalhamento das diversas funcionalidades para o comportamento dinâmico desejado.

3.1 ARQUITETURA DO SISTEMA DE CONTROLE DE SEGURANÇA

A Figura 15 apresenta o modelo estrutural da arquitetura proposta para implementação de sistemas de controle relacionados à segurança para indústria de processos.

Figura 15 – Arquitetura de controle de segurança proposta



Fonte: Próprio Autor

Esta proposta consiste em um modelo de arquitetura que atende aos requisitos de defesa em profundidade e diagnosticabilidade segura, sendo aderente à norma IEC 61511 (IEC: 61511, 2003). Por sua vez, a natureza heteráquica da arquitetura proposta permite modularização dos controladores de prevenção e de mitigação para que seja possível tratar a interação entre falhas críticas e permitir controlar a complexidade de falhas que podem se perpetuar sem que obrigatoriamente tenha ocorrido os respectivos eventos inicializadores. Portanto, destacam-se as seguintes características vinculadas à arquitetura em questão:

- A propriedade de sistema seguro está de acordo com Hollnagel (2007);
- Os controladores de prevenção de eventos inicializadores e críticos incorporam barreiras de segurança reativas, que atuam de forma controlada e progressiva na degeneração da planta / processo;

- Os controladores de mitigação de eventos críticos incorporam barreiras de segurança reativas, que respondam à mitigação antecipada destes eventos impedindo a propagação dos mesmos;
- O Supervisor do Controle de Segurança interage com o sistema de controle básico do processo – SCBP – além de interagir com os controladores de prevenção, mitigação e de brigadas;
- Controlador de brigadas atua mediante o insucesso das barreiras de segurança reativas da mitigação;
- Há um fluxo de informações de controle para a integração entre as barreiras técnicas reativas de prevenção e mitigação a barreiras não técnicas;

Desta forma, obtém-se como resultado uma arquitetura multicamadas englobando:

- Camada 1 – contêm os dispositivos seguros de detecção e atuação, responsáveis pela interface entre o sistema de segurança do processo – SCSP e os elementos de campo da planta / processo:
    - Os diversos elementos finais de controle e as brigadas, destacando-se os detectores seguros que se comunica diretamente com a Camada 3.
- Camada 2 – contém os módulos de controle de prevenção e mitigação de falhas críticas:
    - Controladores de prevenção - CPs;
    - Controladores de mitigação - CMs;
    - Controlador de Brigadas - CBRIG
        - Controlador de equipes de brigadas - CEBRIG;
        - Controlador de recursos das brigadas - CRBRIG.
- Camada 3 – módulo supervisor do controle de segurança – SCS, composto pelos módulos:
    - Módulo controlador das barreiras de prevenção – MCBP;
    - Módulo de controle da mitigação – MCM;
    - Módulo de controle das brigadas - MCB

A interação entre os controladores baseia-se nos seguintes aspectos:

- Os módulos de controle situam-se nas camadas 2 e 3, cada qual com sua função específica de segurança, associados a uma dinâmica de funcionamento, em que os fluxos de informações são representados pelas setas.
- Os módulos de prevenção e mitigação, camada 2, possuem uma arquitetura distribuída: cada módulo de prevenção e cada módulo de mitigação está associado ao seu respectivo evento topo ou falha crítica.
- Apesar de estar representado na arquitetura, o SBCP não realiza qualquer função de segurança (IEC: 61508, 2010) (IEC: 61511, 2003). Este comportamento justifica-se pelo fato do SBCP não tratar de falhas críticas.

  A seguir apresenta-se o detalhamento dos diversos módulos de controle.

3.1.1 Módulos de Controle de Prevenção - CPs

O presente trabalho considera que em uma planta / processo possam ser identificados múltiplos eventos topo ou falhas críticas. Nesse sentido, propõe-se uma arquitetura distribuída para os módulos de controle de prevenção de modo que a cada evento topo seja alocado o respectivo módulo.

A função de segurança de cada módulo é o de prevenir a ocorrência de eventos críticos antecedentes e associados a cada evento topo, minimizando a probabilidade de suas ocorrências.

A prevenção consiste na detecção e confirmação da transição do estado normal de funcionamento de determinados elementos / subsistemas para um estado de falha. Por estarem associados à ocorrência do evento topo, a planta / processo estaria, portanto, em uma condição crítica. A ação de controle de prevenção consiste na degeneração segura daqueles componentes em estado de falha crítica para que a planta / processo, em condição crítica, porém controlável, retorne não à sua condição normal, porém evolua, por meio de processos degenerativos, para uma condição segura.

Os módulos de controle de prevenção possuem seus próprios elementos finais de detecção e atuação, independentes entre si, e independentes do SCBP. Por sua vez,

a metodologia PFS/E-MFG com arcos comunicadores (Anexo A) é utilizada para a síntese formal dos algoritmos de controle, uma vez que permite a descrição formal dos processos de degeneração, utilizando-se sistematicamente uma abordagem baseada em refinamentos sucessivos em que os conceitos de funcionalidades, operações e ações são aplicados para modelar a execução do conjunto de atividades inerentes a cada processo de degeneração. Além disso, é possível utilizar recursos de encapsulamento de dados nas marcas individualizadas para que seja possível configurar as ações de controle de acordo com a especificada de cada item que for processado (seleção de recursos específicos para cada contexto de degeneração).

3.1.2 Módulos de controle de mitigação – CMs

Caso as ações de degeneração dos equipamentos / subsistemas associados à ocorrência de cada evento topo não sejam eficazes, os módulos de mitigação, também em uma arquitetura distribuída, têm a função de segurança de mitigar os possíveis efeitos da ocorrência do evento topo, com o objetivo de minimizar as consequências para a população, o meio ambiente e às instalações.

Em função da arquitetura distribuída dos controladores de prevenção e mitigação, integrados com o SCS, além das ações de controle da mitigação daquele evento topo, podem ser implementadas ações de controle adicionais, tais como a prevenção de ocorrência de outro evento topo, caso sejam verificados possíveis efeitos entre eventos topo.

Os módulos de controle de mitigação, a exemplo da prevenção, possuem seus próprios elementos de detecção e atuação, independentes entre si, e independentes do SCBP. Analogamente, a metodologia PFS/E-MFG com arcos comunicadores é utilizada para a síntese formal dos algoritmos de controle, considerando a modelagem dos diversos processos de mitigação e a possibilidade de compartilhamento de recursos, uma vez que pode haver um número limitado destes, que exige a representação de eventos de sincronização para alocação destes recursos, de acordo

com a prioridade que for estabelecida frente a uma diversidade de processos de mitigação que forem modelados.

Para a modelagem de cada conjunto de atividades de mitigação que compõem cada processo de mitigação serão aplicados, também, os conceitos de funcionalidades, operações e ações, conforme citado anteriormente para o caso dos CPs, com destaque para o controle de compartilhamento de recursos de acordo com as prioridades que forem estabelecidas nos modelos.

3.1.3 Módulo Controlador de Brigadas - CBRIG

Considerando as classificações de barreiras de segurança para a indústria de processos em humanas/ operacional e técnicas (SKLET, 2006), técnicas reativas (SQUILLANTE JR, 2017) e o conjunto de sistemas de barreiras técnicas e humano-operacionais e os aspectos entre suas interações, (YUAN, S., RENIERS, G., *et al.*, 2022) é fundamental enfatizar que:

- há a possibilidade de ocorrência de um eventual insucesso das funções instrumentadas de segurança pertinentes à mitigação;
- é obrigatória a presença de equipes de brigadistas (ABNT NBR 15219, 2019) (ABNT NBR 14276, 2006) e;
- existe a possibilidade de ocorrência de vários eventos topo na planta / processo.

Por estes motivos, surge a necessidade da interação entre as barreiras técnicas e não técnicas em função não só da probabilidade de insucesso das funções instrumentadas da mitigação, mas também da possibilidade da ocorrência simultânea de eventos topo.

Desta forma é necessário estabelecer regras de prioridade em função da dinâmica de insucessos das barreiras técnicas implementadas por meio das funções instrumentadas de segurança dos módulos da mitigação, estabelecendo uma

interface de comunicação por meio do SCS com o objetivo de aprimorar a efetividade das ações dos brigadistas [3].

O módulo de controle de brigadas é constituído por um módulo controlador de equipes de brigadas e por um módulo controlador de recursos / equipamentos para as ações das brigadas.

A alocação das equipes e equipamentos é feita mediante um conjunto de regras estabelecida no SCS em função dos possíveis efeitos de ocorrência dos eventos topo. A metodologia PFS/E-MFG com arcos comunicadores é utilizada para a síntese formal dos algoritmos de controle.

3.1.4 Módulo Supervisor do Controle de Segurança– SCS

O módulo supervisor do controle de segurança atua na integração e gerenciamento dos módulos de controle da camada 2, compreendidos pelos módulos de controle das barreiras técnicas de prevenção e mitigação distribuídos, além da integração com o controlador das barreiras não técnicas das brigadas. Para tanto, o SCS é composto por três módulos de controle:

a) Módulo controlador de barreiras de prevenção – MCBP
b) Módulo de controle da mitigação – MCM
c) Módulo de controle das brigadas - MCBRIG

Estes módulos interagem entre si de forma colaborativa, gerando o aspecto heterárquico intrínsico à arquitetura proposta em que cada módulo executa a detecção, o diagnóstico e a supervisão das respectivas barreiras de segurança associadas a cada domínio de controle modularizado na camada 2 (BASILIO, J.C., CARVALHO, L.K. e MOREIRA, M.V., 2010).

---

[3] Em função das especificidades de cada planta / processo, não faz parte do escopo deste trabalho a definição própria das brigadas (como, por exemplo, o número de equipes e equipamentos para a realização das atividades).

A detecção, diagnóstico e filtragem de sinais espúrios é feita em cada módulo, conforme requisito da propriedade de diagnosticabilidade segura (PAOLI, A. e LAFORTUNE, S., 2005) na medida em que satisfaz a condição de exigência de um diagnosticador local para cada evento crítico durante sua dinâmica.

Os módulos MCBP e MCM são responsáveis pela supervisão das barreiras pertinentes a cada estado crítico controlável da planta / processo, considerando-se múltiplos eventos topo e aspectos de suas interações. Já o módulo MCBRIG é responsável pela interface entre as barreiras técnicas reativas e as barreiras humano-operacionais das brigadas.

A supervisão das barreiras e as relações entre eventos topo são obtidas por meio de um conjunto de regras, definidas a partir da aplicação de técnicas de análises de riscos da equipe multidisciplinar especialista na planta / processo.

A metodologia PFS/E-MFG é utilizada para a síntese dos algoritmos de controle de cada módulo, a comunicação entre os módulos da camada 3 e entre os módulos das camadas 2 e 3.

3.2 CLASSIFICAÇÃO DAS BARREIRAS DE SEGURANÇA

Em virtude da modularização da arquitetura proposta, que permite com que os módulos de prevenção e de mitigação operem de forma autônoma e colaborativa por meio de uma arquitetura heterárquica, o trabalho propõe uma nova classificação para as barreiras condizente com a arquitetura proposta que suporta um sistema de controle supervisório para estas barreiras. Desta forma, permite-se implementar os recursos humano-operacionais em colaboração com as barreiras reativas de prevenção e mitigação, conectadas ao sistema de controle supervisório em questão[4].

[4] Um exemplo para que a comunicação seja efetiva entre recursos humano-operacionais e o sistema supervisório, é por meio de tecnologias como óculos de Realidade Aumentada, que permite a interação desejada e é capaz de potencializar a ação humana.

Nesse sentido, é proposta uma nova classificação para as barreiras de segurança, em que o sistema de barreiras de segurança de uma planta / processo, gerenciado pelo sistema de controle supervisório da camada 3, incorpore, além das barreiras técnicas reativas, as barreiras semi-reativas. O conjunto de barreiras de segurança de uma planta / processo, situadas na camada 2 da arquitetura, são descritas da seguinte forma:

- Barreiras reativas de prevenção: barreiras técnicas, suportadas pelas normas IEC 61508 / IEC 61511;
- Barreiras reativas de mitigação: barreiras técnicas, suportadas pelas normas IEC 61508 / IEC 61511;
- Barreiras semi-reativas: barreiras humano-operacionais, suportadas pelas normas (ABNT NBR 14276, 2006; ABNT NBR 15219, 2019).

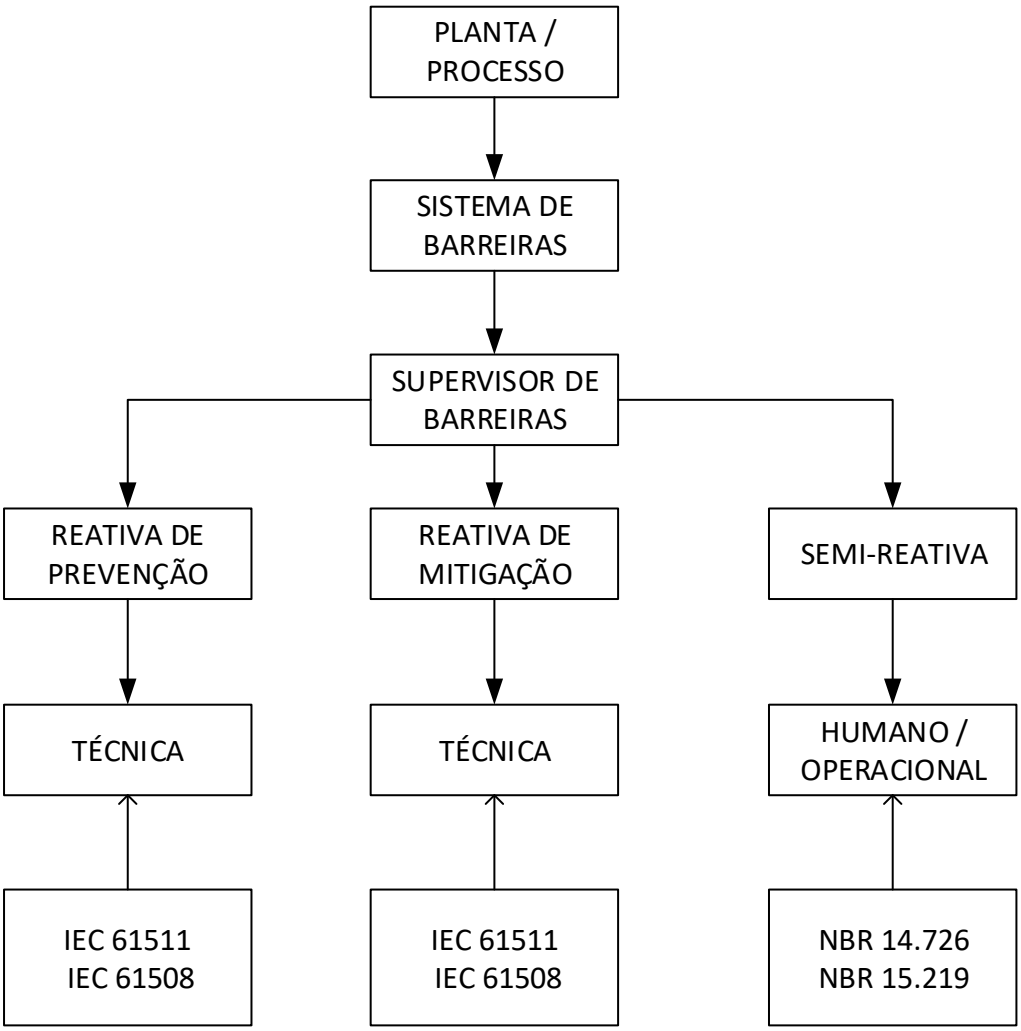
As barreiras reativas de mitigação e de prevenção são projetadas tendo como fundamento os princípios de segurança em profundidade e diagnosticabilidade segura. O escopo técnico é suportado, aplicando o conceito de SIS e as funções instrumentadas de segurança pertinentes. Para lidar com a complexidade do sistema, os processos foram modularizados por meio do uso de grafos E-MFG que são uma classe de redes de Petri Interpretadas com individualização das marcas por meio de atributos. Desta forma é possível emular as regras de controle que permitem a interface com o sistema supervisório para tratar a complexidade oriunda da possível interação entre falhas. Os sistemas de controle, de malha fechada, garantem a reatividade diante da ocorrência de eventos externos.

Por sua vez, as barreiras semi-reativas foram propostas utilizando-se de forma análoga os recursos técnicos das barreiras de mitigação e prevenção. Entretanto, os elementos finais de controle que permitem a atuação e sensoriamento dos processos são emulados por meio de recursos humanos que mantêm a autonomia para interagir com a planta por meio da expertise que possuem. Por este motivo, o sistema supervisório atua no sentido de potencializar as ações destes recursos humanos para que possam promover ações de maior impacto para a solução dos problemas de mitigação. Neste contexto, as atividades desenvolvidas são híbridas, no sentido de

poderem ser desenvolvidos nos âmbitos técnicos e não técnicos conforme a classificação apresentada em (YUAN, S., RENIERS, G., *et al.*, 2022).

Considerando o exposto, a Figura 16 apresenta a nova classificação para barreiras de segurança.

Figura 16–Classificação das barreiras de segurança



Fonte: Próprio Autor

Assim, a proposta da nova classificação adéqua-se aos conceitos de defesa em profundidade e diagnosticabilidade segura, intrínsecos ao desenvolvimento de sistemas de controle de segurança para sistemas complexos e críticos que é o escopo deste trabalho.

3.3 SISTEMÁTICA PARA A SÍNTESE DO SISTEMA DE CONTROLE DE SEGURANÇA

Esta seção apresenta uma sistemática para a síntese dos algoritmos de controle dos módulos da arquitetura proposta.

A camada 2 caracteriza-se pela modularidade de processos que é uma condição necessária para garantir a autonomia de cada processo de prevenção e de cada processo de mitigação que são elaborados de acordo com cada evento topo que foi diagnosticado e suas consequências.

Uma vez que estes processos são autônomos, a complexidade de promover a interação entre eles, exige a processamento de um modelo de controle supervisório que é capaz de mapear o estado global deste conjunto finito de processos de prevenção e de mitigação que são independentes e assíncronos, no contexto da camada 2. A solução adotada foi desenvolver um sistema de controle supervisório que também é modular, capaz de mapear o estado global deste conjunto de processos da camada 2 para promover a interação entre esses processos de forma colaborativa nesta camada 3 e, de forma hierárquica, controlar os processos da camada 2. Neste contexto, em função da distribuição dos controladores da camada 2, os algoritmos podem realizar a troca de sinais de forma colaborativa para que se possa efetivamente resultar em uma integração entre os módulos distribuídos da camada 2 e entre os módulos da camada 3

Para atingir o objetivo, a sistemática propõe com que sejam realizadas as seguintes etapas:

- Definição dos cenários críticos e das barreiras de segurança reativas;
- Síntese dos algoritmos dos módulos da camada 2;
    - Síntese do algoritmo da prevenção;
    - Síntese do algoritmo da mitigação;
- Síntese dos algoritmos dos módulos da camada 3;
    - Síntese do algoritmo do módulo de controle das barreiras de prevenção;

- Síntese do algoritmo do módulo de controle da mitigação;
- Síntese do algoritmo de controle das brigadas.

A ênfase dada a questão de se modularizar a síntese dos algoritmos está relacionada à questão de modelagem estruturada de processos, conforme Santos Filho (2000). Desta forma, têm-se três aspectos fundamentais importantes:

- O processo de verificação dos modelos pode ser realizado de forma sistemática, considerando as boas propriedades como vivacidade, limitabilidade e reiniciabilidade na análise comportamental de cada grafo que modelo cada um dos processos.
- Cada modelo de processo deve ser construído considerando-se o fato de serem utilizados componentes conservativos (baseado no conceito de invariante linear de lugar) no processo de modelagem para evitar o problema de contato.
- A utilização do sistema de controle distribuído em camadas com diferentes semânticas permite que a interação entre os módulos de controle de diferentes camadas ocorra via comunicadores. Desta forma, não haverá quebra da estruturação e integridade dos módulos que poderia ser causado por intrusão ou vazamento de marcas,

Nos itens subsequentes são detalhados os aspectos formais, os métodos e as ferramentas para contemplar cada etapa da sistemática proposta.

3.3.1 Etapa 1: Definição dos cenários críticos e barreiras de segurança

Nesta etapa é feita a definição do escopo da planta / processo, sua atual fase do ciclo de vida, o descritivo do funcionamento dos elementos / subsistemas que compõe o processo, histórico de falhas, além da análise dos seguintes documentos, se possível:

- ✓ Diagramas de processo e da instrumentação P&ID (ISA S-5.1-1984, 2009);
- ✓ Faixa de operação normal de cada instrumento e os limites máximo e mínimo de referência permitidos;
- ✓ Descritivo de funcionamento dos elementos que compõe cada subsistema da planta / processo;
- ✓ Lista de I\O´s do SCBP;
- ✓ Manuais técnicos de cada equipamento do subsistema;

Por meio de técnicas de análises de riscos implementadas por uma equipe multidisciplinar especialista no processo, são definidos os eventos topo, os cenários críticos que antecedem sua ocorrência, as consequências de seus efeitos e as medidas para a sua prevenção e mitigação.

O presente trabalho propõe um método (Apêndice A1), com base em normas de segurança vigentes, para a determinação dos elementos críticos e dos cenários críticos associados a um evento topo.

Após a definição de todos os cenários críticos da planta / processo em estudo, o presente trabalho propõe um método (Apêndice A2) para a inserção de barreiras reativas de prevenção e mitigação, com referência às normas de segurança vigentes.

Os métodos propostos nos Apêndices A1 e A2 fornecem os subsídios para a elaboração das etapas subsequentes da sistemática proposta.

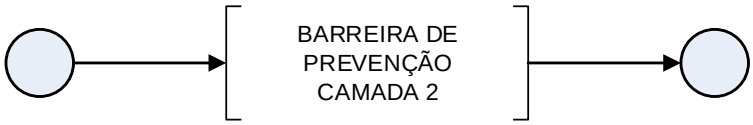
3.3.2 Etapa 2: Síntese dos algoritmos de controle da camada 2

Para a modelagem dos módulos de controle de cada processo de prevenção e de cada processo de mitigação da camada 2 foi utilizada a metodologia PFS/E-MFG. Desta forma é possível realizar a modelagem a partir de grafos PFS e obter o detalhamento necessário com os recursos de interpretação disponíveis nos grafos E-MFG com comunicadores.

a) Algoritmos de prevenção – camada 2

O modelo PFS de cada uma das barreiras de prevenção da camada 2 de controle é representado na Figura 17.

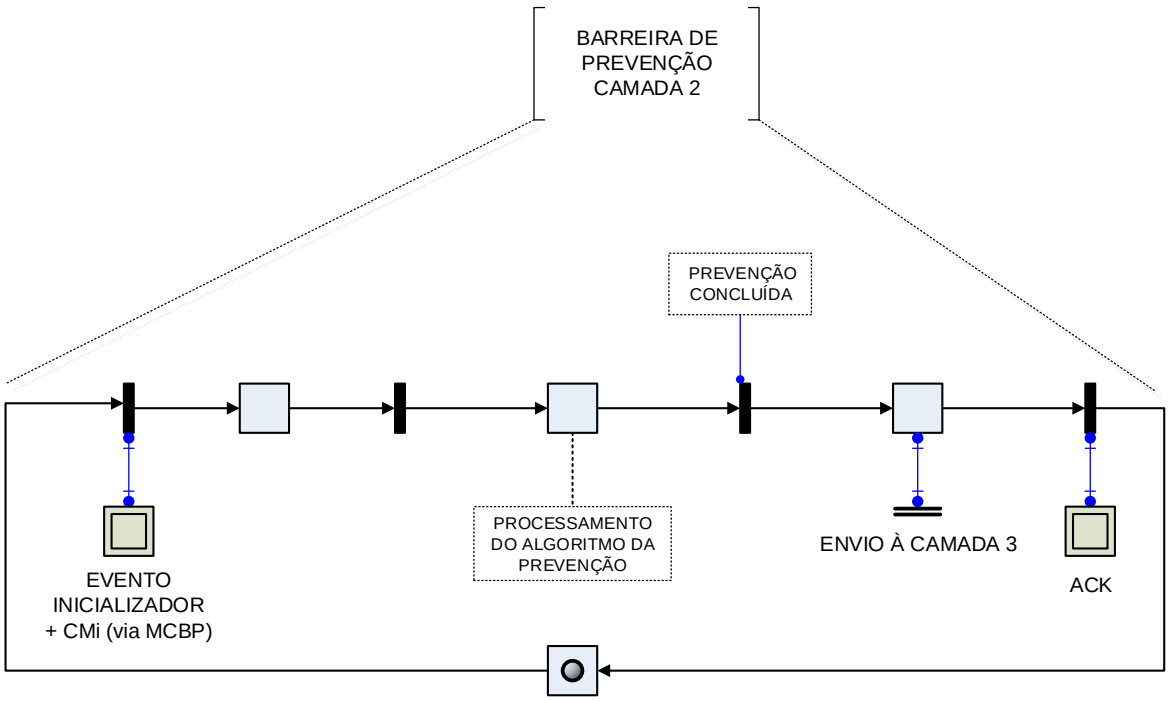
Figura 17 – Modelo PFS das barreiras de segurança da camada 2 de controle



Fonte: Próprio Autor

O refinamento E-MFG com arcos comunicadores da atividade de segurança de prevenção de cada uma das barreiras de prevenção da planta / processo é representado por meio da Figura 18.

Figura 18 – Modelo E-MFG de refinamento da atividade “Barreira de Prevenção”



A dinâmica de funcionamento de cada uma das barreiras de prevenção da camada 2 de controle consiste no recebimento do respectivo evento inicializador, ou de comando do módulo de controle das barreiras de prevenção – MCBP, em função da interação entre falhas críticas[5], e o processamento do respectivo algoritmo da prevenção.

Após a confirmação da conclusão do algoritmo de prevenção, é feito o envio à camada 3 de controle por meio de arco comunicador. O grafo reinicializa após a confirmação do recebimento da camada 3 (ACK).

O modelo E-MFG com arcos comunicadores da Figura 18 é aplicado à todas as barreiras reativas de prevenção, associadas a cada uma das estruturas de árvores de falhas, de cada evento topo.

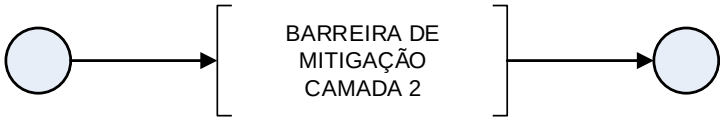
Para cada evento topo, há o conjunto dos possíveis cenários críticos até sua ocorrência. O conjunto de barreiras reativas de prevenção é então definido (Anexo A2). Para este evento topo, será alocado um controlador de segurança de prevenção na camada 2, que conterá cada um dos algoritmos de prevenção, representados no modelo E-MFG da Figura 18, associados respectivamente aos seus eventos inicializadores, ou em função de comando do módulo MCBP, camada 3.

b) Algoritmos de mitigação – camada 2

O modelo PFS de cada uma das barreiras de mitigação da camada 2 de controle é representado na Figura 19.

[5] A ocorrência de uma falha crítica pode ter efeitos sobre outros eventos topo. Nesse sentido, o trabalho propõe que as barreiras reativas de prevenção, associadas aos efeitos da ocorrência daquele evento topo, sejam performadas, evitando-se o efeito da escalação (efeito dominó) entre falhas críticas.

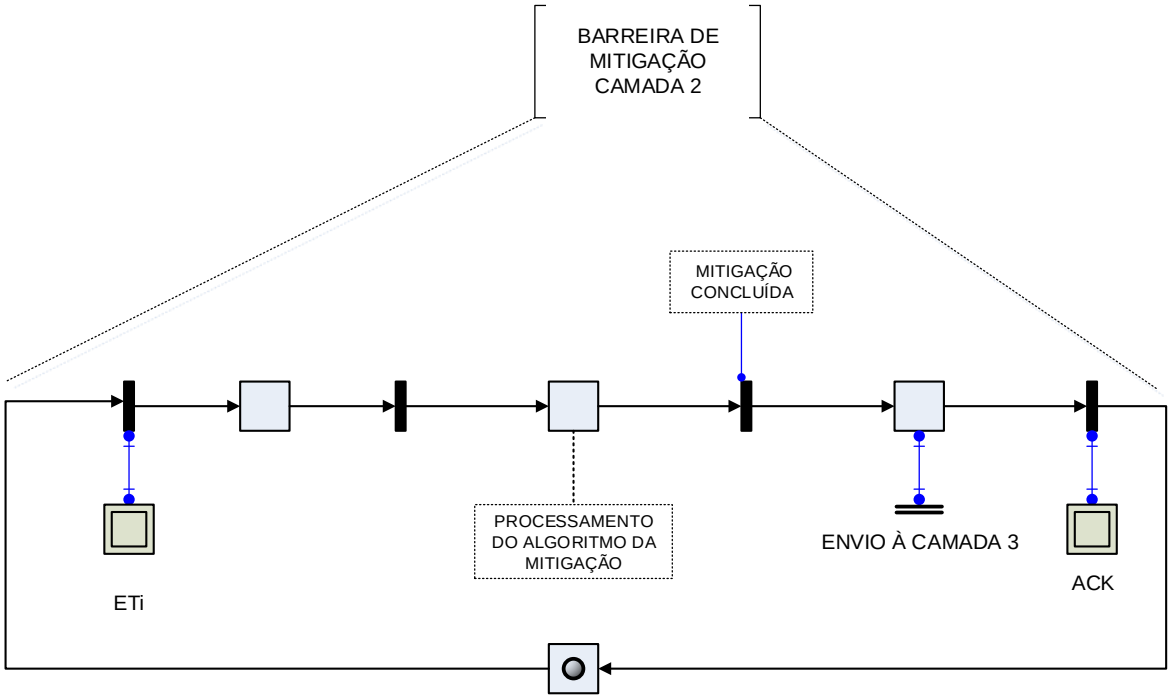
Figura 19 – Modelo PFS das barreiras de mitigação



Fonte: Próprio Autor

O refinamento E-MFG com arcos comunicadores da atividade de segurança da mitigação de cada uma das barreiras de mitigação da planta / processo é representado por meio da Figura 20.

Figura 20- Modelo E-MFG de refinamento da atividade “Barreira de Mitigação”



Fonte: Próprio Autor

A dinâmica de funcionamento de cada uma das barreiras de mitigação da camada 2 de controle consiste no recebimento da confirmação de ocorrência do respectivo evento-topo, ou por meio da ineficácia das respectivas barreiras de prevenção associadas a um dos cenários críticos até a ocorrência do evento topo. Para o caso das ineficácias, o módulo MCBP envia os insucessos da prevenção ao módulo MCM,

que realiza, por meio de arco comunicador, o envio ao respectivo controlador da mitigação, camada 2, que irá performar o algoritmo da mitigação, conforme Figura 20.

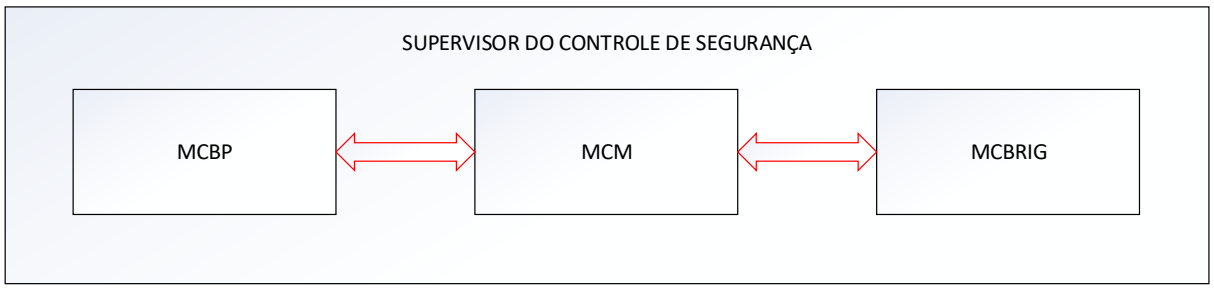
Após a confirmação da conclusão do algoritmo da mitigação, é feito o envio à camada 3, módulo MCM por meio de arco comunicador. O grafo retorna após o recebimento da confirmação (ACK).

O modelo E-MFG da Figura 20 é aplicado à todas as barreiras reativas de mitigação, associadas aos seus respectivos eventos topo. Cada evento topo terá um controlador de segurança de mitigação, camada 2.

3.3.3 Etapa 3: Síntese dos algoritmos de controle da camada 3

Considerando a proposta da arquitetura de controle distribuída e a colaboração entre os módulos da camada 3, a Figura 21 ilustra o fluxo de informações entre os módulos de controle da camada 3 da arquitetura proposta.

Figura 21 – Arquitetura do módulo supervisor de controle. - SCS



Fonte: Próprio Autor

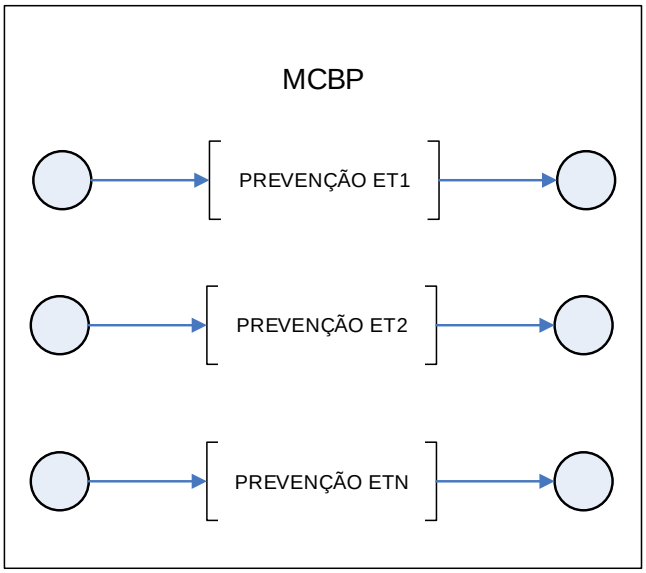
As atividades de prevenção são realizadas no módulo controlador de barreiras de prevenção – MCBP, já as atividades de mitigação, no módulo de controle da mitigação - MCM, e as atividades de brigadas, no módulo de controle das brigadas – MCBRIG.

Nas seções subsequentes será apresentado o refinamento PFS das atividades de cada módulo da camada 3.

3.3.3.1 Módulo controlador das barreiras de prevenção – MCBP

Considerando a estrutura distribuída dos módulos de controle de prevenção na camada 2 e da supervisão de todos estes módulos na camada 3, por meio do MCBP, o conjunto de atividades PFS de prevenção associadas a cada evento topo no módulo MCBP é representado na Figura 22.

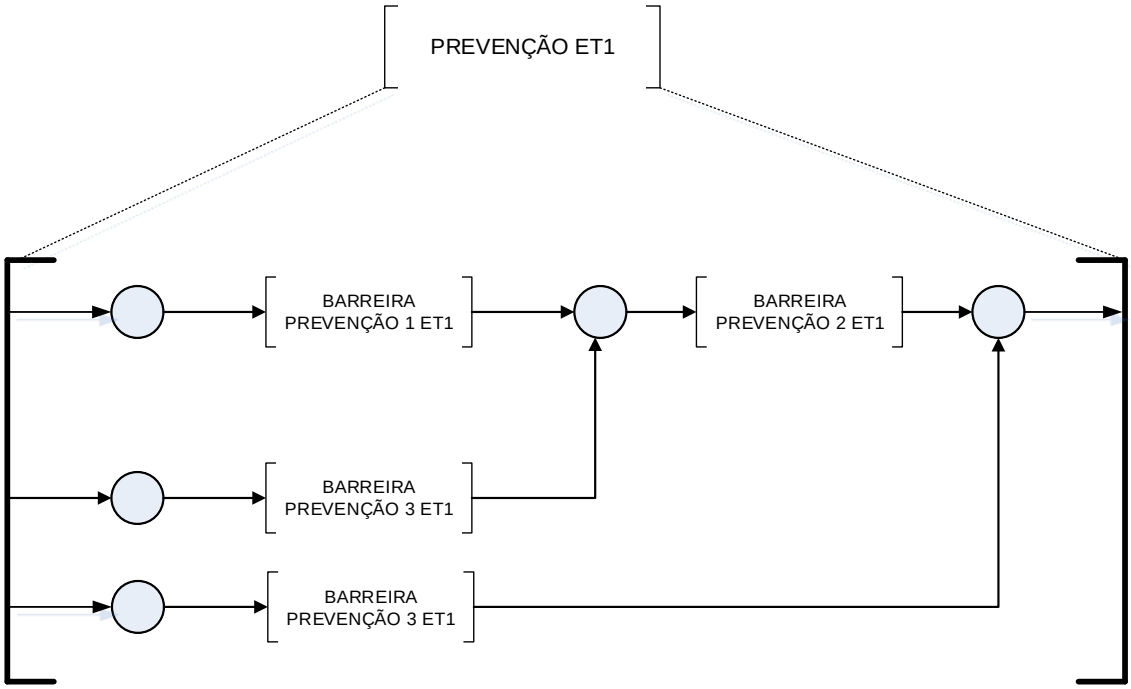
Figura 22 – Atividades de prevenção - MCBP



Fonte: Próprio Autor

O refinamento dos modelos PFS de cada uma das atividades de prevenção é representado, por exemplo, por meio da atividade “PREVENÇÃO ET1” da Figura 23.

Figura 23 – Refinamento PFS da atividade “Prevenção ET1.



Fonte: Próprio Autor

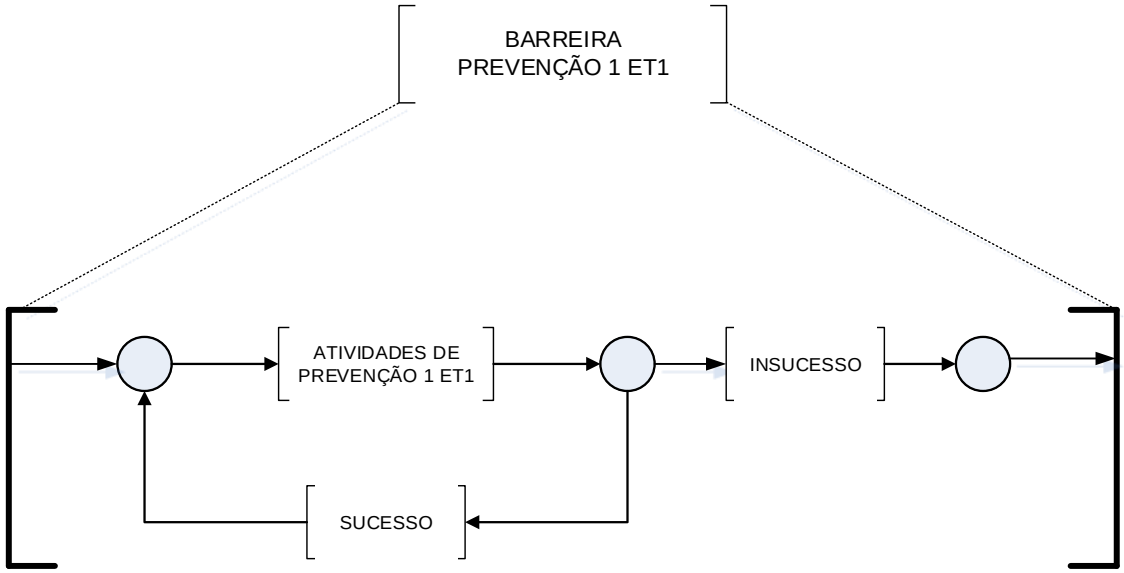
No exemplo, a estrutura da árvore de falhas associada à ocorrência do evento topo 1, e consequente conjunto de barreiras reativas de prevenção, são representados por meio da sequência de barreiras “BARREIRA PREVENÇÃO 1 ET1” e “BARREIRA PREVENÇÃO 2 ET1”, ou pela sequência “BARREIRA PREVENÇÃO 3 ET1” e “BARREIRA PREVENÇÃO 2 ET1” ou ainda por meio da “BARREIRA PREVENÇÃO 3 ET1”. O evento topo 1 irá ocorrer pela ineficácia das SIFs de prevenção, desempenhadas pelo controlador de prevenção 1 (camada 2).

Caso se tenha sucesso, o evento topo não irá ocorrer, e as barreiras de prevenção realizaram suas funções de segurança com êxito.

Obviamente, cada evento topo terá a sua própria estrutura de árvore de falhas e o respectivo conjunto de barreiras reativas de prevenção. Os modelos PFS devem, necessariamente, representar os respectivos caminhos críticos até a ocorrência do evento topo associado.

O refinamento da atividade “BARREIRA DE PREVENÇÃO 1 ET1” é representado no modelo PFS da Figura 24. As atividades de prevenção podem resultar em sucesso ou insucesso.

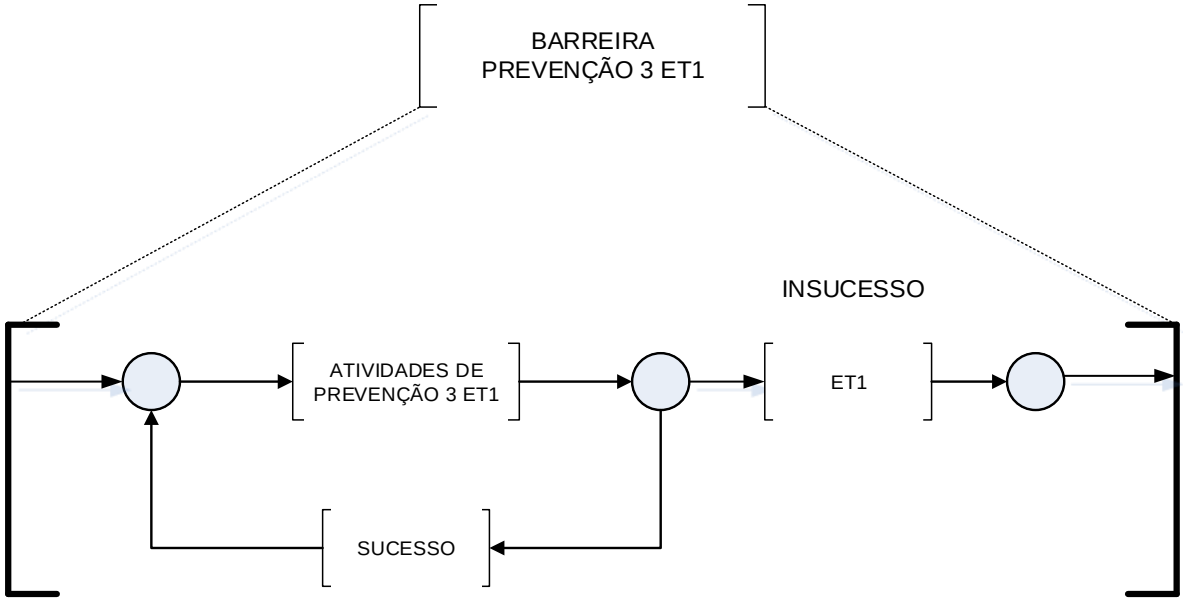
Figura 24 – Refinamento PFS “Barreira de Prevenção 1 ET1”



Fonte: Próprio Autor

Note, como exemplo, que o insucesso da barreira de prevenção 3 associada ao ET1 resulta na ocorrência do evento topo 1 (decorrente da particularidade da estrutura da árvore de falhas). O refinamento da atividade “BARREIRA DE PREVENÇÃO 3 ET1” é representado no modelo PFS da Figura 25. Note que o insucesso resultou em ET1.

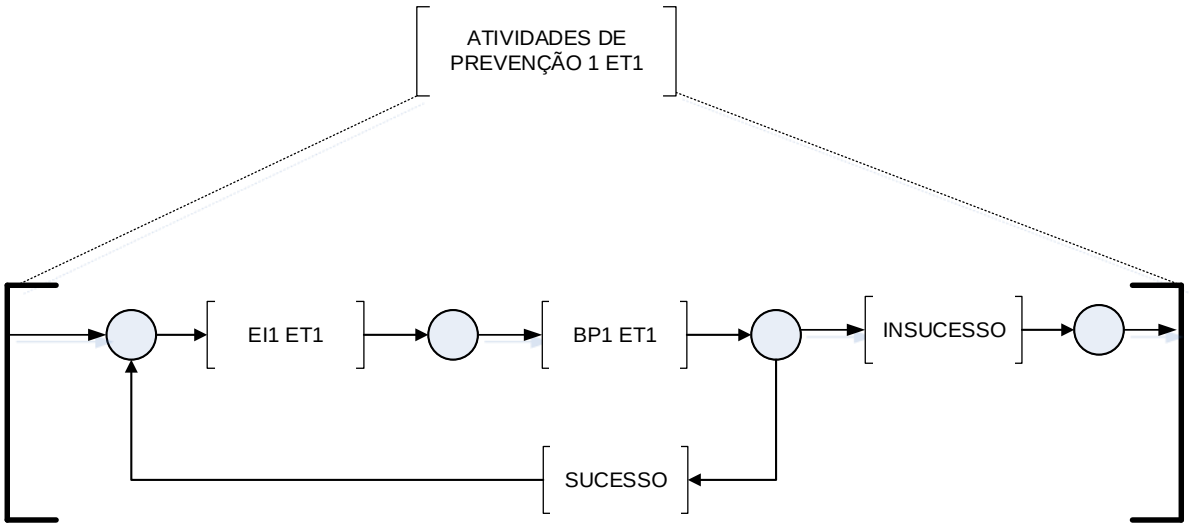
Figura 25 – Refinamento PFS “Barreira de Prevenção 3 ET1”



Fonte: Próprio Autor

Por sua vez, o refinamento de cada uma das atividades de prevenção ao evento topo são representadas por meio do modelo PFS da Figura 26. Foi utilizado, como exemplo, “ATIVIDADES DE PREVENÇÃO 1 ET1”

Figura 26 – Refinamento PFS “Atividades de Prevenção 1 ET1”



Fonte: Próprio Autor

O próximo passo consiste no refinamento das atividades de confirmação dos respectivos eventos inicializadores, como por exemplo a atividade “EI 1 ET1”[6] que significa: “Evento Inicializador 1 do Evento Topo 1”.

O refinamento da atividade “EI1 ET1” dependerá do critério adotado para a votação dos sensores para a sua confirmação[7]. Um exemplo do modelo E-MFG para o critério de votação 2oo3 é sugerido no Apêndice B.

Tal procedimento é feito para todos os eventos inicializadores associados a todos os eventos topo da planta / processo.

No entanto, diante da possibilidade de interação entre falhas críticas, a atividade “EI1 ET1” pode ser iniciada pela confirmação de seu respectivo evento inicializador, ou por meio do recebimento de mensagem do módulo de controle da prevenção, MCBP, recebida, por sua vez, do módulo de controle da mitigação – MCM.

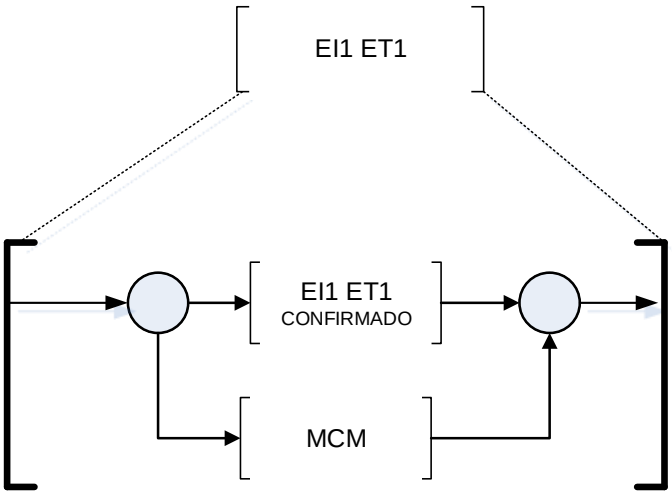
Considerando o exposto, o refinamento da atividade “EI1 ET1” é representado por meio do modelo PFS da Figura 27.

---

[6] “EI1 ET1” significa evento inicializador 1, associado ao evento topo 1. Em função dos caminhos críticos, outros eventos inicializadores podem estar associados ao ET1: EI2, EI3, EI4 etc, com as respectivas barreiras reativas de prevenção: BP1 ET1, BP2 ET1...

[7] Considerando o princípio de diagnosticabilidade segura, as etapas de detecção, coordenação e filtragem espúria são realizadas no Sistema Supervisório de Controle – SCS.

Figura 27 – Refinamento do PFS “EI1 ET1”

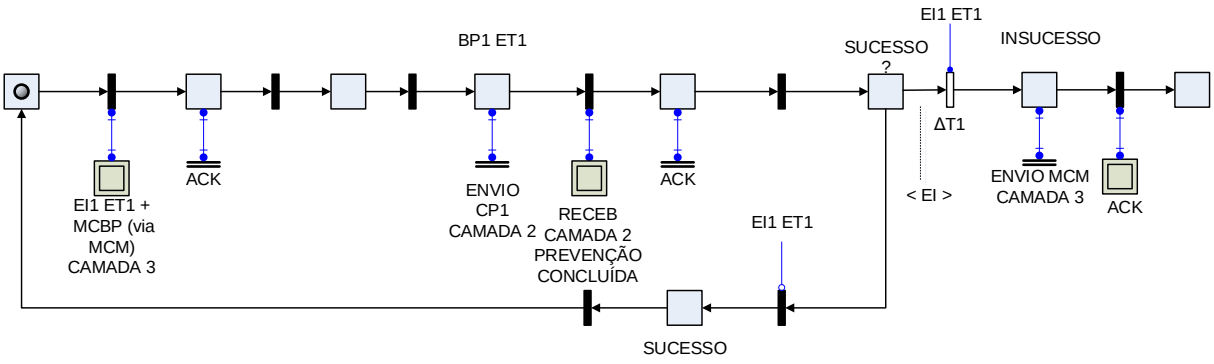


Fonte: Próprio Autor

Já a atividade “BP1 ET1” do modelo PFS da Figura 26, de posse da informação de confirmação do evento inicializador da respectiva barreira de prevenção, do respectivo evento topo, realiza o envio ao respectivo controlador de prevenção da camada 2, que irá performar o algoritmo da prevenção.

A próxima etapa do refinamento consiste no modelo E-MFG com arcos comunicadores do algoritmo de controle da prevenção do módulo MCBP, camada 3, de uma barreira de prevenção, associado a um único evento topo. O modelo do algoritmo é representado por meio da Figura 28.

Figura 28 – Modelo E-MFG da “Atividade de prevenção ET1”



Fonte: Próprio Autor

Tendo-se a confirmação do evento inicializador 1 do evento topo 1 (ET1), ou o recebimento de mensagem do módulo MCBP (via MCM), é feita a confirmação do recebimento (ACK), e a barreira de prevenção (BP1 ET1) realiza o envio ao respectivo controlador de prevenção 1, camada 2, que irá processar o respectivo algoritmo da prevenção (Figura 18).

Na camada 2, após a confirmação da conclusão da prevenção, o respectivo controlador realiza o envio para a camada 3. O resultado da prevenção pode ser o sucesso, em que o evento inicializador retorna à condição normal em um intervalo de tempo inferior ao Δt (determinado pela equipe de especialistas), após a conclusão do algoritmo da prevenção, camada 2.

Caso o evento inicializador se mantenha habilitado, conclui-se que o algoritmo da prevenção não foi eficaz, o que se entende como uma ineficácia da respectiva barreira de prevenção. No exemplo, a BP1 ET1.

A ocorrência do evento topo dependerá dos insucessos das barreiras de prevenção associados aos cenários críticos de sua respectiva estrutura de árvore de falhas.

Considerando os aspectos de interação entre falhas críticas, as atividades de prevenção, camada 2, podem ser performadas por meio de mensagem recebida do módulo MCM em função dos efeitos de ocorrência de um outro evento topo, previsto no modelo E-MFG da Figura 28.

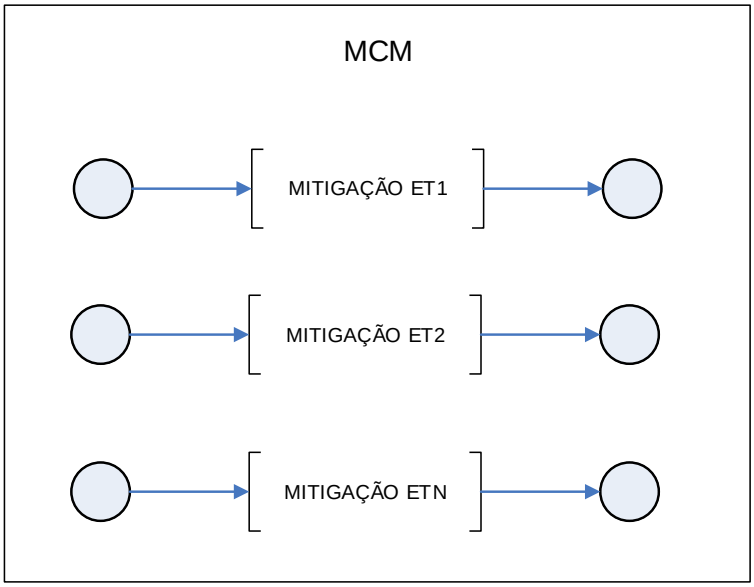
No entanto, não faria sentido avaliar o sucesso ou o insucesso da barreira de prevenção, pois não foi confirmado o seu respectivo evento inicializador.

Para tais casos, por meio da distinção das marcas, a avaliação do insucesso só será feita com o atributo “< EI >”.

3.3.3.2 Módulo de controle da mitigação – camada 3

Considerando a estrutura distribuída dos módulos de controle da mitigação na camada 2 e da supervisão de todos estes módulos na camada 3, por meio do MCM, o conjunto de atividades PFS de mitigação associadas à ocorrência de cada evento topo no módulo MCM é representado na Figura 29.

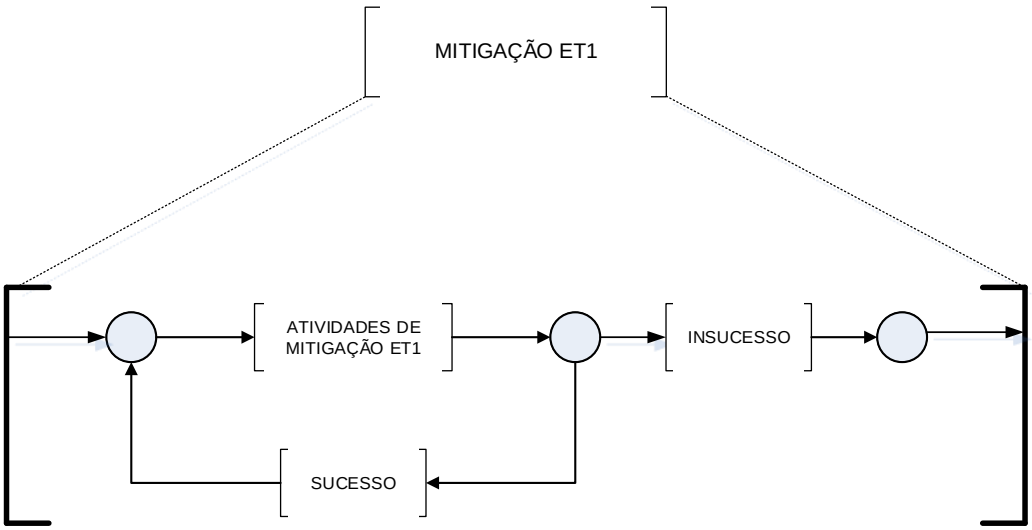
Figura 29 - Atividades de mitigação - MCM



Fonte: Próprio Autor

O refinamento dos modelos PFS de cada uma das atividades de mitigação é representado no exemplo do modelo PFS “MITIGAÇÃO ET1” da Figura 30. As atividades de mitigação associadas à ocorrência dos demais eventos topo é feita de forma análoga. As atividades de mitigação podem resultar em sucesso ou insucesso.

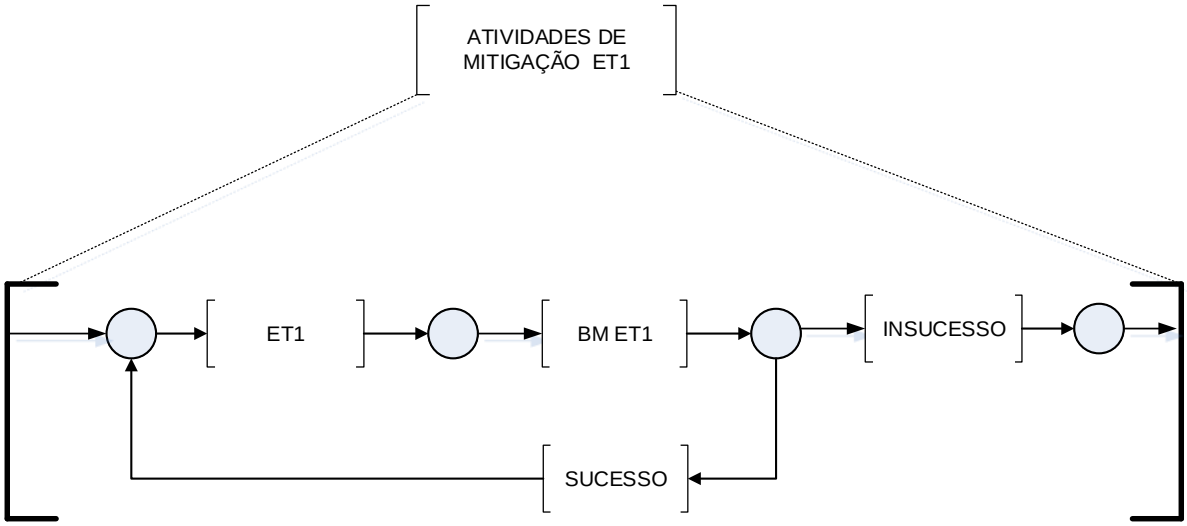
Figura 30 – Refinamento PFS “Mitigação ET1”



Fonte: Próprio Autor

Considera-se, no presente trabalho, que após a ocorrência de um evento topo há somente uma barreira reativa de mitigação[8], ou seja, todas as SIFs de mitigação serão performadas após a ocorrência de um evento topo. O modelo PFS do refinamento "ATIVIDADES DE MITIGAÇÃO ET1" é representado na Figura 31.

Figura 31 – Modelo PFS "Atividades de mitigação ET1"



Fonte: Próprio Autor

Um evento topo pode ocorrer por meio de seus eventos inicializadores, por meio de sensores seguros, independentes da prevenção. A confirmação, assim como é feito na prevenção, é feita na camada 3[9], utilizando-se, por exemplo, o modelo E-MFG do Apêndice A.

Outra forma de considerar, de forma antecipativa, a ocorrência do evento topo, é por meio das ineficácias das respectivas barreiras de prevenção, associadas aos cenários críticos associados à sua ocorrência (exemplo PFS Figura 23).

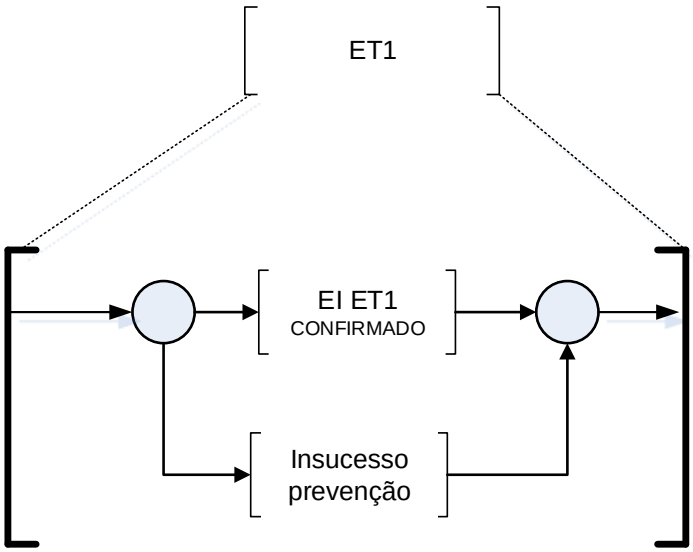
---

[8] O detalhe da estrutura da árvore de eventos a cada evento topo é apresentada no Anexo A2

[9] Considerando o princípio de diagnosticabilidade segura, as etapas de detecção, coordenação e filtragem espúria são realizadas no Sistema Supervisório de Controle – SCS.

Nesse sentido, a Figura 32 ilustra o refinamento do modelo PFS representativo à ocorrência de um evento topo, como por exemplo o ET1.

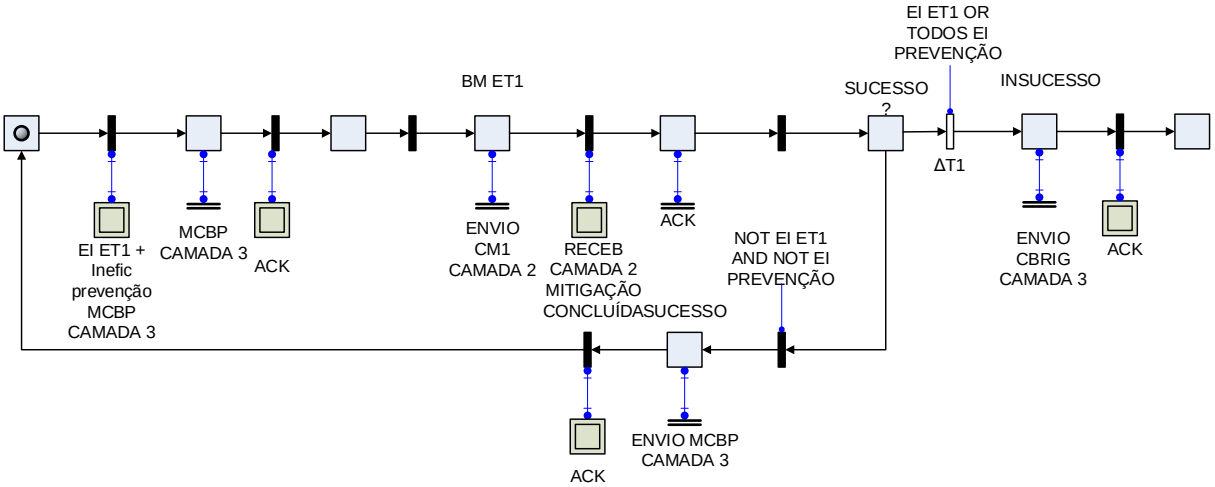
Figura 32 – Modelo PFS de ocorrência do ET1



Fonte: Próprio Autor

O respectivo modelo E-MFG do modelo PFS da Figura 31, com arcos comunicadores, é representado na Figura 33.

Figura 33 – Modelo E-MFG da “Atividade de mitigação ET1”



Fonte: Próprio Autor

Tendo-se a confirmação da ocorrência do evento topo 1 (evento inicializador ou ineficácia da prevenção), é feito o envio ao MCBP do conjunto de barreiras de prevenção[10] associadas a outros eventos topo que, em função da interação entre falhas críticas, devem ser performadas para se evitar o indesejado efeito dominó. Após o recebimento de confirmação (ACK), a "BM ET1" realiza o envio ao respectivo controlador de mitigação, camada 2, que irá processar o algoritmo da mitigação (Figura 20).

Na camada 2, após a confirmação da conclusão da mitigação, o respectivo controlador realiza o envio para a camada 3.

Considerando que o evento topo pode ocorrer ou por meio de seu respectivo evento inicializador, ou por meio da ineficácia de uma sequência de barreiras de prevenção, o resultado de sucesso da mitigação é verificado por uma lógica "E" da condição desabilitada tanto do evento inicializador da mitigação, quanto de todos os eventos inicializadores da prevenção.

Resultando em sucesso, é feito o envio para o MCBP, camada 3, que retorna ao MCM (ACK)

O insucesso é verificado com o sinal habilitado de uma lógica "OU" de quaisquer um dos sensores mencionados, decorridos o intervalo de tempo Δt (determinado pela equipe de especialistas), após a conclusão do algoritmo da mitigação, camada 2.

Para o caso do insucesso é feito o envio ao controlador de brigadas, CBRIG, para que se dê início às barreiras semi-reativas, ou seja, as funções de mitigação das equipes de brigadas, orientadas pelo módulo controlador da mitigação, MCM, camada 3.

[10]Para cenários não observáveis, a falha crítica pode ocorrer sem que se tenha confirmado os eventos inicializadores das respectivas barreiras de prevenção. Nesse sentido, o evento inicializador da mitigação, confirmado, realizará, via MCBP, a execução de todas as barreiras de prevenção associadas ao seu evento topo.

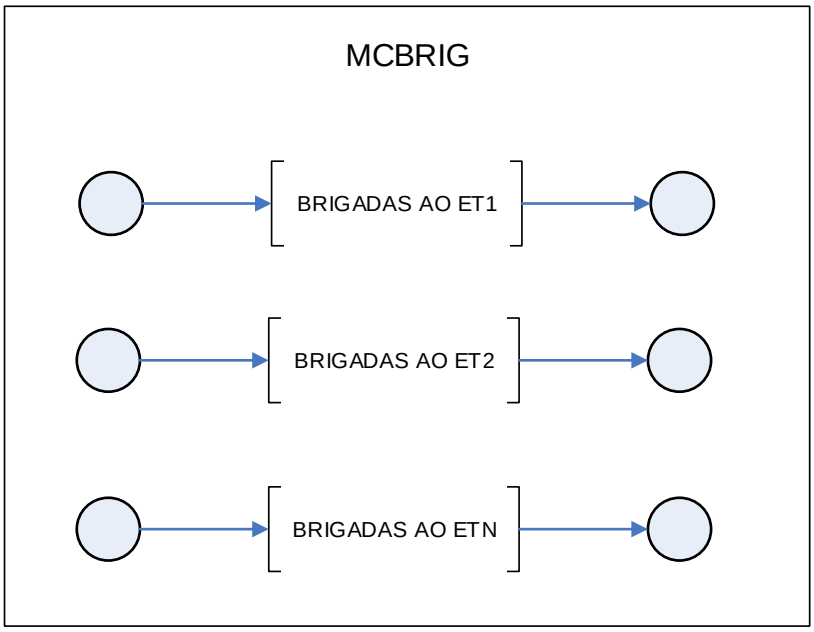
3.3.3.3 Módulo de controle das brigadas – camada 3

Diante do insucesso da barreira reativa de mitigação associado a um evento topo, e do recebimento da mensagem proveniente do MCM, o MCBRIG deverá encaminhar a solicitação das ações das brigadas ao controlador de brigadas, camada 2 que, de posse da informação do evento topo, irá alocar as respectivas equipes e recursos como medida complementar à mitigação das barreiras reativas.

Não faz parte do escopo deste trabalho a definição específica da equipe e dos recursos por conta da especificidade da planta / processo.

O conjunto de atividades PFS de brigadas associadas ao insucesso da mitigação de cada evento topo no módulo MCBRIG é representado na Figura 34.

Figura 34 – Modelo PFS das brigadas, MCBRIG



Fonte: Próprio Autor

Em função de eventual demanda simultânea de brigadas, em que o número de brigadas é menor que o número de processos a serem mitigados, o MCBRIG deverá ter um conjunto de regras de prioridades em função da avaliação do potencial do dano (ABNT NBR 14276, 2006) de cada evento topo, e irá enviar, caso ocorram

simultaneidades, qual(is) o evento(s) topo terá(ão) prioridades para as brigadas, em função da troca de informações entre os módulos.

Ao sucesso das brigadas, o controlador local envia a informação ao MCBRIG, que envia a informação ao MCM.

Ao insucesso, é feito o alarme à comunidade e a solicitação de recursos suplementares à mitigação (ABNT NBR 14276, 2006).

3.4 RESUMO DO CAPÍTULO

Definido o escopo e as hipóteses consideradas, o capítulo apresenta a proposta de uma arquitetura de controle de segurança para a processos críticos, composta por camadas e módulos de controle que operam de forma colaborativa. Um sistema supervisório de segurança interage com módulos distribuídos para a prevenção e mitigação de falhas críticas, além da colaboração de um módulo de controle de brigadas, que atua como interface de controle entre as barreiras de segurança técnicas e as barreiras até então classificadas como não técnicas.

Em função da arquitetura de controle proposta permitir a interação entre barreiras de segurança de naturezas distintas, foi proposta uma nova classificação às barreiras de segurança. Além das barreiras técnicas reativas, é proposta a classificação das barreiras semi-reativas, interligadas ao sistema supervisório do controle de segurança, de forma com que as barreiras de segurança implementadas por recursos humano-operacionais tenham uma melhor orientação em relação às suas funções.

O capítulo faz referência a uma sistemática para a identificação dos cenários de risco de uma planta / processo, a proposta das barreiras de segurança de prevenção e mitigação (Apêndices A1 e A2, própria autoria) e, com base na arquitetura de controle proposta, apresenta a síntese formal dos algoritmos de controle de cada módulo da camada 2 de controle e a síntese dos algoritmos de cada módulo do sistema supervisório de segurança, evidenciando o fluxo de informações decorrente da interação colaborativa, permitindo que aspectos de interação entre falhas críticas possa ser devidamente tratado.

4. RESULTADOS

Neste capítulo é apresentado um exemplo de indústria de processo caracterizada por complexidade e criticidade, em que foram identificados múltiplos eventos topo.

Nesse sentido, o primeiro passo da metodologia é aplicado para a definição dos múltiplos cenários de riscos associados a cada evento topo. Aspectos de interação entre falhas críticas são identificados. A complexidade da síntese do algoritmo de controle, considerando-se uma única camada de controle de segurança é claramente evidenciada.

No entanto, em função da modularização da arquitetura proposta, os diversos algoritmos de controle de cada módulo são gerados e integrados, evidenciando a contribuição da metodologia.

4.1 EXEMPLO DE APLICAÇÃO

Com o objetivo de exemplificar a metodologia proposta, será feito o estudo de um processo produtivo de extração e compressão de gás natural. A planta é caracterizada por sua complexidade na medida em que o processo produtivo é composto por diversos subsistemas, cada qual com suas especificidades funcionais.

O fluido de trabalho é o gás natural, cuja composição é uma mistura de hidrocarbonetos altamente inflamáveis com a presença de impurezas. A ocorrência de falhas críticas pode resultar em sérias consequências ao homem, ao meio ambiente e às próprias instalações. Considerando a densidade de energia / m², a instalação é caracterizada por um risco alto / iminente (ABNT NBR 14276, 2006) (N-2782, 2015) (HSE, 2006a).

Evidentemente trata-se de um processo crítico.

De forma resumida, a planta / processo é constituída dos seguintes subsistemas:

- Duas unidades de filtros coalescedores, ligados a dutos para a reserva natural;
- Duas unidades de filtros para o gás combustível dos geradores elétricos e das turbinas da instalação;
- Dois trocadores de calor (aquecedores), que promovem o pré-aquecimento do gás combustível das turbinas e geradores;
- Quatro turbinas para a movimentação dos compressores de gás;
- Dois geradores de energia;
- Duas unidades compressoras para ar comprimido de instrumento;
- Quatro unidades compressoras do gás natural;
- Quatro trocadores de calor (resfriadores), ligados aos compressores;
- *Header* de descarga;
- Tanque de dreno de impurezas

De forma resumida, duas unidades de filtros coalescedores (disposição em paralelo), ligados à reserva natural realizam a separação das impurezas, e o gás é enviado a quatro unidades compressoras, responsáveis pelo aumento da pressão do fluido. Devido ao aumento da temperatura (decorrido do aumento da pressão), à saída de cada compressor é instalado um resfriador (*after cooler*) para o restabelecimento da temperatura nominal. Os quatro resfriadores são ligados ao *header* de descarga, em que o gás, filtrado e pressurizado, é enviado aos centros consumidores por meio de um gasoduto.

Parte do gás filtrado passa por outros dois filtros (em paralelo), que por sua vez é enviado a duas unidades de troca de calor (paralelo) para pré-aquecimento[11] (passo 1 de trocador). O gás então alimenta quatro turbinas, cada uma ligada solidariamente ao respectivo compressor.

[11] Aumento de eficiência na combustão

Além dos filtros citados, há ainda dois filtros (paralelo ativo) responsáveis pelo gás combustível aos geradores de energia elétrica da instalação, e para a alimentação de compressores de ar para instrumento.

O gás para os geradores também passa pelos dois trocadores de calor mencionados, porém pelo passo 2. O aquecimento dos trocadores utiliza esta tomada de gás, perfazendo o passo 3.

A atual fase do ciclo de vida da instalação é operacional, e a planta dispõe dos seguintes documentos:

- ✓ Diagramas de processo e da instrumentação P&ID[12] (ISA S-5.1-1984, 2009);
- ✓ Faixa de operação normal de cada instrumento e os limites máximo e mínimo de referência permitidos;
- ✓ Descritivo de funcionamento dos elementos que compõe cada subsistema da planta / processo;
- ✓ Lista de I'Os do SCBP;
- ✓ Manuais técnicos de cada equipamento do subsistema;

Além do SCBP, a planta conta com um módulo de controle de prevenção e um módulo de controle de mitigação de falhas críticas. Em um primeiro estudo de avaliação de riscos, foram identificadas quatro falhas críticas, e as respectivas SIFs de prevenção e mitigação foram definidas.

O estudo contemplou somente os eventos imediatamente anteriores à ocorrência do evento topo (não foram considerados os cenários que antecedem a ocorrência). Como consequência, a planta apresenta um excesso de paradas espúrias, com perdas financeiras significativas, além de elevado risco em seu funcionamento.

[12] Para o melhor entendimento do processo, parte dos diagramas de instrumentação constam no Anexo B.

Nesse sentido, uma equipe multidisciplinar promoveu a reavaliação dos riscos da instalação, com foco nos conceitos de defesa em profundidade (múltiplas linhas de defesa), diagnosticabilidade segura e modularização da arquitetura de controle.

O método para a definição dos cenários críticos (Apêndice A1) foi implementado para a reavaliação do risco da instalação e para a definição de todos os cenários críticos.

Para a planta em estudo, a nova análise de riscos identificou sete eventos topo e respectivas estruturas de árvores de falhas.

Com base no método proposto no Apêndice 2, as barreiras de segurança foram inseridas, e as SIFs de prevenção e mitigação de cada barreira foram determinadas por meio do estudo Hazop.

4.1.1 Etapa 1: Definição dos cenários críticos e das barreiras de segurança reativas

Após a identificação da planta / processo, do estudo da documentação e da definição da equipe de especialistas no processo, foram aplicados os métodos constantes nos Apêndices A1 e A2.

Foram identificados sete eventos topo, os respectivos cenários críticos, e a inserção das respectivas barreiras de segurança. O estudo Hazop permitiu a definição das SIFs de prevenção e mitigação desempenhadas por cada barreira de segurança.

Os resultados dos estudos Hazop e das respectivas árvores de falhas e as barreiras reativas de prevenção[13], são apresentados:

[13] Após a obtenção das estruturas de árvores de falhas, as barreiras estão representadas por barras horizontais, com a função de prevenir o sequenciamento até a ocorrência do evento topo. Não se trata de uma nova proposta de estrutura da técnica de árvore de falhas, rferenciada na IEC 61025.

Tabela 6 – Estudo Hazop para as barreiras de prevenção – evento topo 1

Barreira	Elemento	Evento crítico / desvio	Possíveis causas	Consequências	Ação	Equipamento	Sensores	otação	Atuadores	SIL
BP1 ET1	Não se aplica	pressão baixa na entrada	Obstrução / variação de especificação	Danos aos elementos por arraste condensado	By-pass do ramo	FT-12001A	PIT-003	1oo1	XV-001; XV-017	1
BP2 ET1	Não se aplica	pressão baixa na entrada	Obstrução / variação de especificação	Danos aos elementos por arraste condensado	By-pass do ramo	FT-12001B	PIT-024	1oo1	XV-019; XV-020	1
BP3 ET1	Filtro coalescedor 1	nível alto de condensado	Baixa pressão, falha BP1 ET1	Danos aos elementos por arraste condensado	Isolar e drenar o Filtro 1	FT-12001A	LIT-006 / LIT-007	1oo1	XV-005; XV-001; XV-017; XV-006; XV-007	1
BP4 ET1	Filtro coalescedor 2	nível alto de condensado	Baixa pressão, falha BP2 ET1	Danos aos elementos por arraste condensado	Isolar e drenar o Filtro 2	FT-12001B	LIT013 / LIT-014	1oo1	XV-022; XV-019; XV-020; XV-023; XV-024	1
BP5 ET1	Filtro coalescedor 1	diferencial de pressão elevado	Falha válvulas alívio e ajuste de pressão	Danos aos elementos, pressão não nominal	Isolar e drenar o Filtro 1	FT-12001A	PDIT-005	1oo1	XV-005; XV-001; XV-017; XV-006; XV-007	1
BP6 ET1	Filtro coalescedor 2	diferencial de pressão elevado	Falha válvulas alívio e ajuste de pressão	Danos aos elementos, pressão não nominal	Isolar e drenar o Filtro 2	FT-12001B	PDIT-025	1oo1	XV-022; XV-001; XV-017; XV-006; XV-007	1
BP7 ET1	Filtros 1 e 2	nível alto de condensado	Falha da BP3 ET1, BP4 ET1, BP1 ET1 E BP2 ET1	Danos aos elementos por arraste condensado	By pass da estação, *shutdown* dos compressores	FT-12001 A e B	PIT-003, PIT 004 LIT-006, LIT-007 LIT-013 e LIT-014	1oo1	XV-001; XV-017; XV-019; XV-020; XV-005;XV-006; XV-007; XV-020;XV-022; XV-023; XV-024, *shutdown* compressores	1
BP8 ET1	Filtros 1 e 2	diferencial de pressão elevado	Falha da BP5 ET1 E BP6 ET1	Danos aos elementos, pressão não nominal	By pass da estação, *shutdown* dos compressores	FT-12001 A e B	PDIT-005 PDIT-025	1oo1	XV-001; XV-017; XV-019; XV-020; XV-005;XV-006; XV-007; XV-020;XV-022; XV-023; XV-024, *shutdown* compressores	1

Figura 35 – FTA do evento topo 1 -: Falha no processo de filtragem – FT 12001 A/B

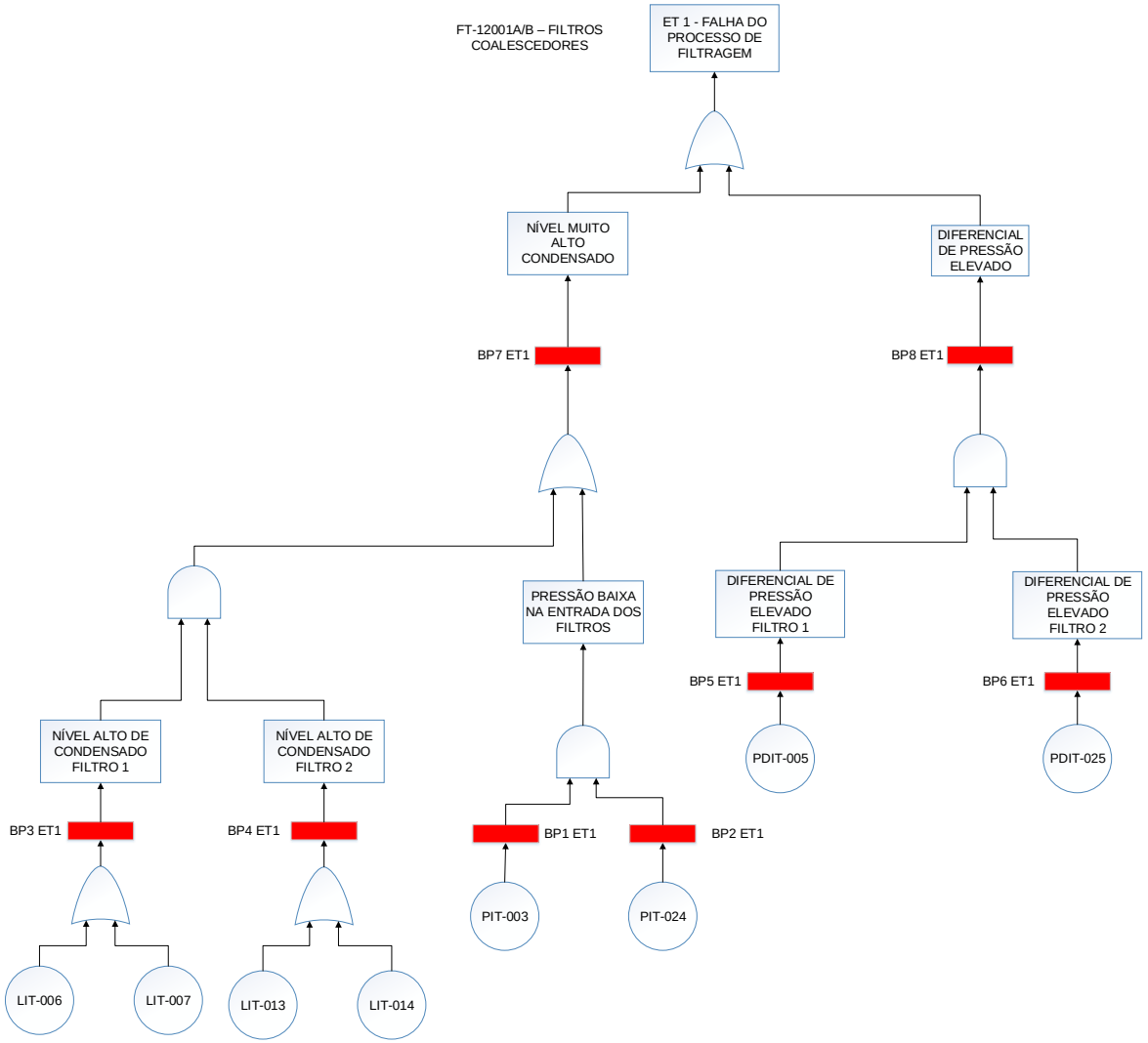


Tabela 7 - Estudo Hazop para as barreiras de prevenção – eventos topo 2 e 3

Barreira	Elemento	Evento crítico / desvio	Possíveis causas	Consequências	Ação	Equipamento	Sensores	otação	Atuadores	SIL
BP1 ET2	Compressor A	pressão e temperatura elevada saída do compressor	alta pressão na linha	Danos ao compressor fluxo reverso	*shutdown* do compressor	Compressor A	TIT-206A; PIT-206A	1oo1	*shutdown* compressor A	1
BP2 ET2	Compressor B	pressão e temperatura elevada saída do compressor	alta pressão na linha	Danos ao compressor fluxo reverso	*shutdown* do compressor	Compressor B	TIT-206B; PIT-206B	1oo1	*shutdown* compressor B	1
BP3 ET2	Compressor C	pressão e temperatura elevada saída do compressor	alta pressão na linha	Danos ao compressor fluxo reverso	*shutdown* do compressor	Compressor C	TIT-206C; PIT-206C	1oo1	*shutdown* compressor C	1
BP4 ET2	Compressor D	pressão e temperatura elevada saída do compressor	alta pressão na linha	Danos ao compressor fluxo reverso	*shutdown* do compressor	Compressor D	TIT-206D; PIT-206D	1oo1	*shutdown* compressor D	1
BP5 ET2	Não se aplica	pressão muio alta no header de descarga	Pressão alta nas saídas dos compressores	Danos no header de descarga	Liberação da pressão; compressores em lenta	Header de descarga	PIT-006A; PIT-006B; PIT-006C	2oo3	XV-003; XV-018; compressores em marcha lenta	3
Barreira	**Elemento**	**Evento crítico / desvio**	**Possíveis causas**	**Consequências**	**Ação**	**Equipamento**	**Sensores**	**otação**	**Atuadores**	**SIL**
BP1 ET3	Filtro 1 para gás combustível das turbinas	Baixa pressão / nível de condensado elevado	Falha no processo de filtragem coalescente - ET1	Danos às turbinas	Isolar o filtro A	FT-12002 A	LIT-101A/ PI-120A	1oo1	XV-112	1
BP2 ET3	Filtro 2 para gás combustível das turbinas	Baixa pressão / nível de condensado elevado	Falha no processo de filtragem coalescente - ET1	Danos às turbinas	Isolar o filtro B	FT-12002 B	LIT-101B/ PI-120B	1oo1	XV-110	1
BP3 ET3	Filtros 1 e 2 para gás combustível das turbinas	Baixa pressão / nível de condensado elevado	FALHA BP1 ET3 E BP2 ET3	Danos às turbinas e compressores	Isolar os filtros	FT-12002 A e B	LIT-101A/ PI-120A/ LIT-101B/ PI-120B	1oo1	XV-125	1

Figura 36 - Evento topo 2 -: Danos no *header* de descarga

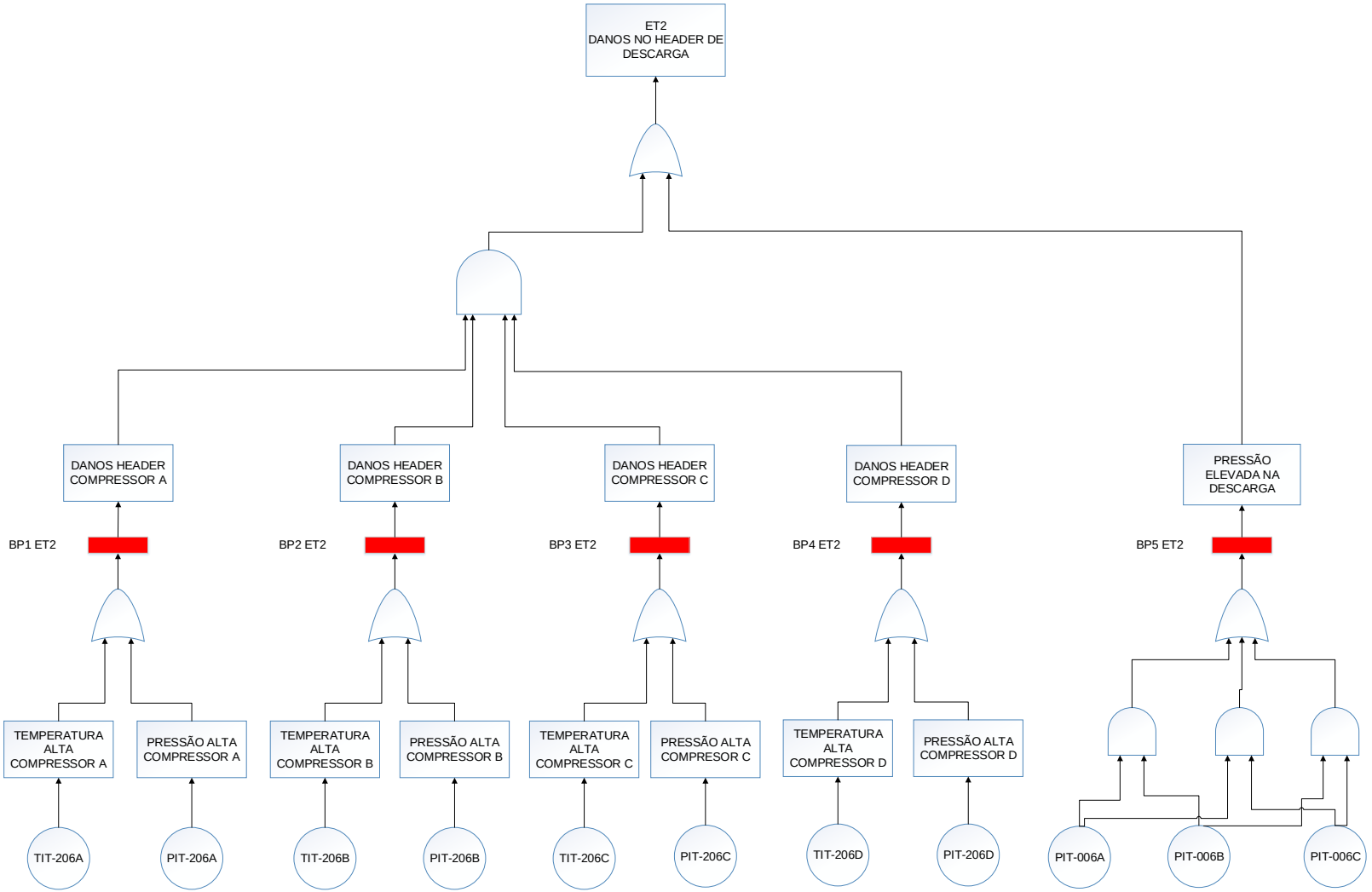


Figura 37 - Evento topo 3 -: Falha filtragem para combustível dos compressores

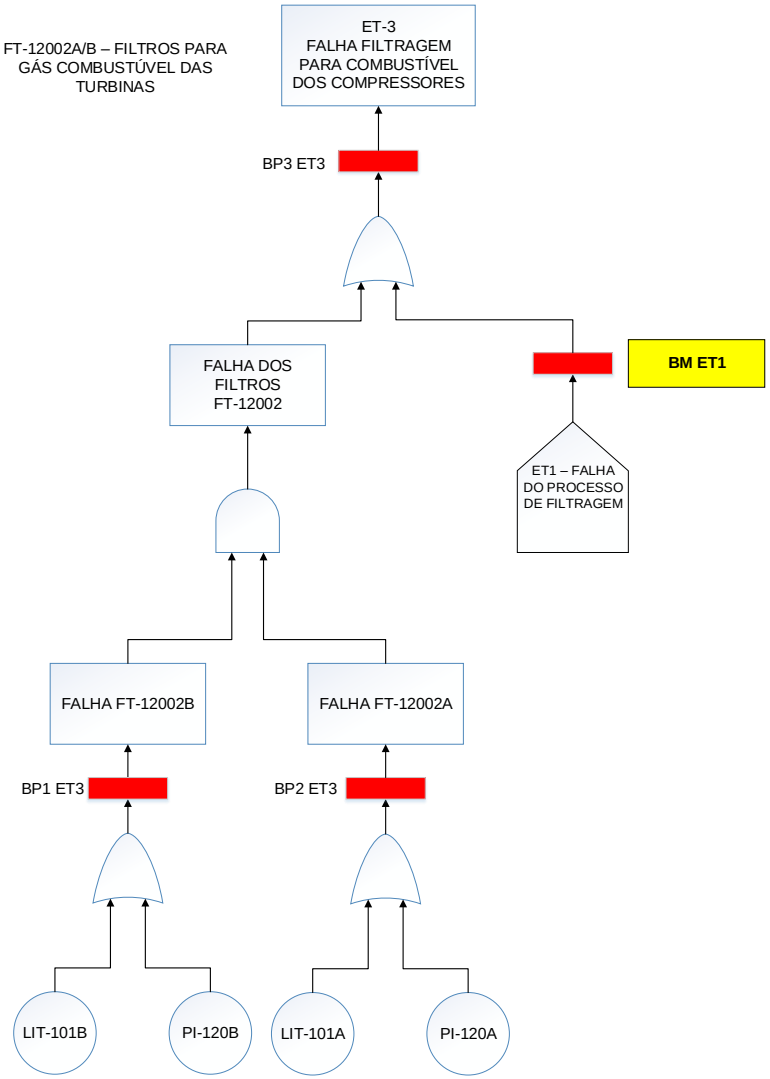


Tabela 8 - Estudo Hazop para as barreiras de prevenção – eventos topo 4 e 5

Barreira	Elemento	Evento crítico / desvio	Possíveis causas	Consequências	Ação	Equipamento	Sensores	otaçã	Atuadores	SIL
BP1 ET4	Filtro 1 para gás combustível dos geradores	Baixa pressão e aumento de nível de condensado filtro 1	Obstrução / variação de especificação	Danos aos elementos do gerador	Isolar o filtro 1	FT-12003A	LIT-102A / PI-121A	1oo1	XV-123	1
BP2 ET4	Filtro 2 para gás combustível dos geradores	Baixa pressão e aumento de nível de condensado filtro 2	Obstrução / variação de especificação	Danos aos elementos do gerador	Isolar o filtro 2	FT-12003B	LIT-102B / PI-121B	1oo1	XV-121	1
BP3 ET4	Filtros 1 e 2 para gás combustível dos geradores	Baixa pressão e aumento de nível de condensado filtros	FALHA BP1 ET4 E BP2 ET4	Danos aos elementos do gerador	Isolar os filtros	FT-12003A FT-12003B	LIT-102A / PI-121A / LIT-102B / PI-121B	1oo1	XV-121 e XV-123	1
Barreira	**Elemento**	**Evento crítico / desvio**	**Possíveis causas**	**Consequências**	**Ação**	**Equipamento**	**Sensores**	**otaçã**	**Atuadores**	**SIL**
BP1 ET5	Aquecedor A para gás combustível compressores passo 1	Excesso temperatura, passo 1 trocador A	Falha no trocador de calor A, passo 1	Possíveis danos aos compressores, combustível fora da especificação	*by-pass* do passo 1	P-12002A	TIT-109A	1oo1	TV-106A	1
BP2 ET5	Aquecedor 1 para gás combustível compressores	Excesso temperatura trocador A	Falha no trocador de calor A	Possíveis danos aos compressores e geradores	Isolar o trocador A	P-12002A	TIT-114A	1oo1	XV-127	1
BP3 ET5	Aquecedor 2 para gás combustível compressores passo 1	Excesso temperatura, passo 1 trocador B	Falha no trocador de calor B, passo 1	Possíveis danos aos compressores, combustível fora da especificação	*by-pass* do passo 2	P-12002B	TIT-109B	1oo1	TV-106B	1
BP4 ET5	Aquecedor 2 para gás combustível compressores	Excesso temperatura trocador B	Falha no trocador de calor B	Possíveis danos aos compressores e geradores	Isolar o trocador B	P-12002B	TIT-114B	1oo1	XV-129	1

Figura 38 – Evento topo 4: Falha filtragem para combustível dos geradores

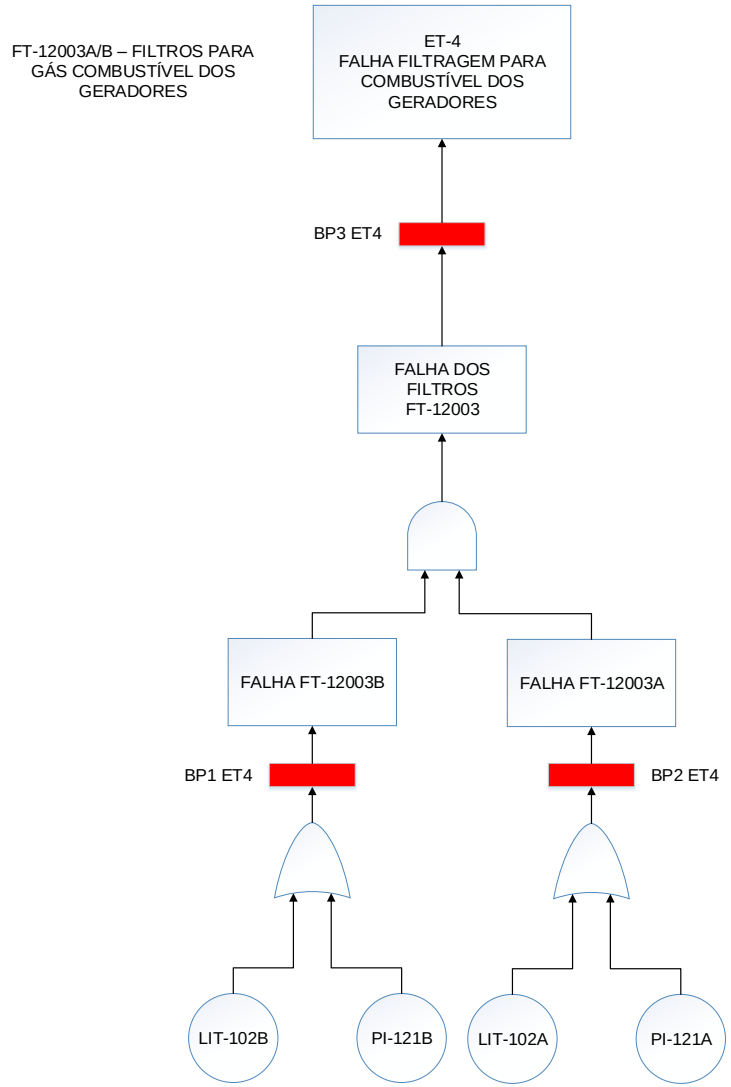


Figura 39 – Evento topo 5: Falha no aquecimento do gás combustível dos compressores

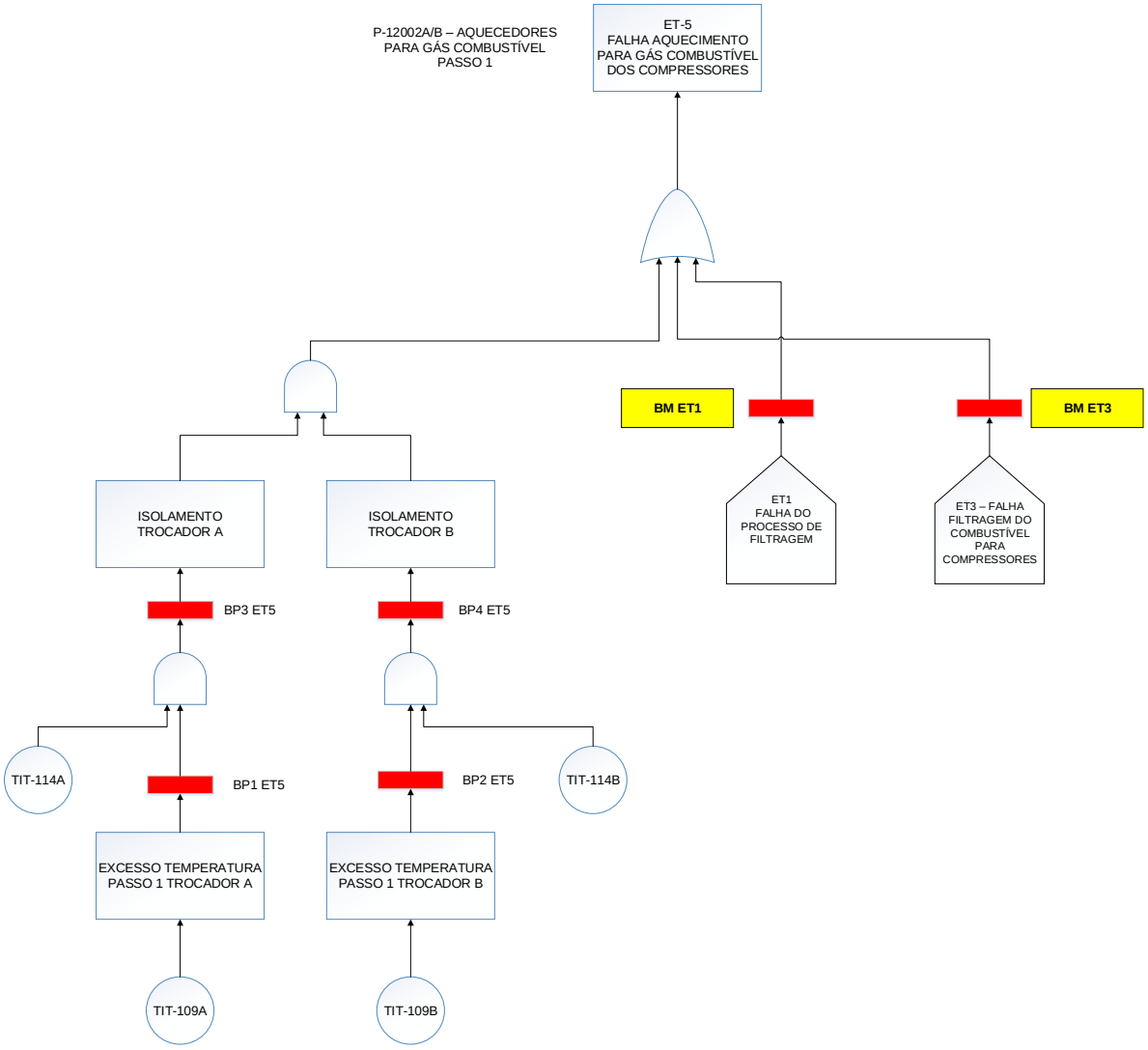


Tabela 9 – Estudo Hazop para os eventos topo 6 e 7

Barreira	Elemento	Evento crítico / desvio	Possíveis causas	Consequências	Ação	Equipamento	Sensores	otaçã	Atuadores	SIL
BP1 ET6	Aquecedor A para gás combustível geradores, passo 2	Excesso temperatura, passo 2 trocador A	Falha no trocador de calor A, passo 2	Possíveis danos aos geradores, combustível fora da especificação	Isolar o passo 2 trocador A	P-12002A	TIT-105A	1oo1	TV-107A	1
BP2 ET6	Aquecedor B para gás combustível geradores, passo 2	Excesso temperatura, passo 2 trocador B	Falha no trocador de calor B, passo 2	Possíveis danos aos geradores, combustível fora da especificação	Isolar o passo 2 trocador B	P-12002B	TIT-105B	1oo1	TV-107B	1
BP3 ET6	Aquecedores A e B para gás combustível geradores, passo 2	Excesso de pressão nos trocadores de calor, passo 2	Excesso de pressão da linha de filtragem	Possíveis danos aos geradores, combustível fora da especificação	Isolar os trocadores de calor, passo 2	P-12002 A/B	PIT-114	1oo1	XV-126 e XV-128	1
Barreira	**Elemento**	**Evento crítico / desvio**	**Possíveis causas**	**Consequências**	**Ação**	**Equipamento**	**Sensores**	**otaçã**	**Atuadores**	**SIL**
BP1 ET7	Aquecedor A passo 3	Nível alto / baixo de condensado, falha chama piloto, passo 3 do aquecedor A	Problemas de pressão / filtragem, falha aquecedor	Falha na troca de calor para os passos 1 e 2	Isolar o queimador	P-12002 A	LIT-103A / LSLL-104A/ BSLL-104A	1oo1	XV-104A	1
BP2 ET7	Aquecedor B passo 3	Nível alto / baixo de condensado, falha chama piloto, passo 3 do aquecedor B	Problemas de pressão / filtragem, falha aquecedor	Falha na troca de calor para os passos 1 e 2	Isolar o queimador	P-12002 B	LIT-103B/ LSLL-104B/ BSLL-104B	1oo1	XV-104B	1
BP3 ET7	Aquecedores A e B passo 3	Nível alto / baixo de condensado, falha chama piloto, passo 3 dos aquecedores	Falha BP1 ET7 Falha BP2 ET7	Variações de pressão e temperatura nas linhas combustíveis	Isolar os queimadores	P-12002 A P-12002 B	PIT-113 / TIT-113	1oo1	XV-104A e XV-104B	1

Figura 40 – Evento topo 6: Falha no aquecimento do gás para geradores

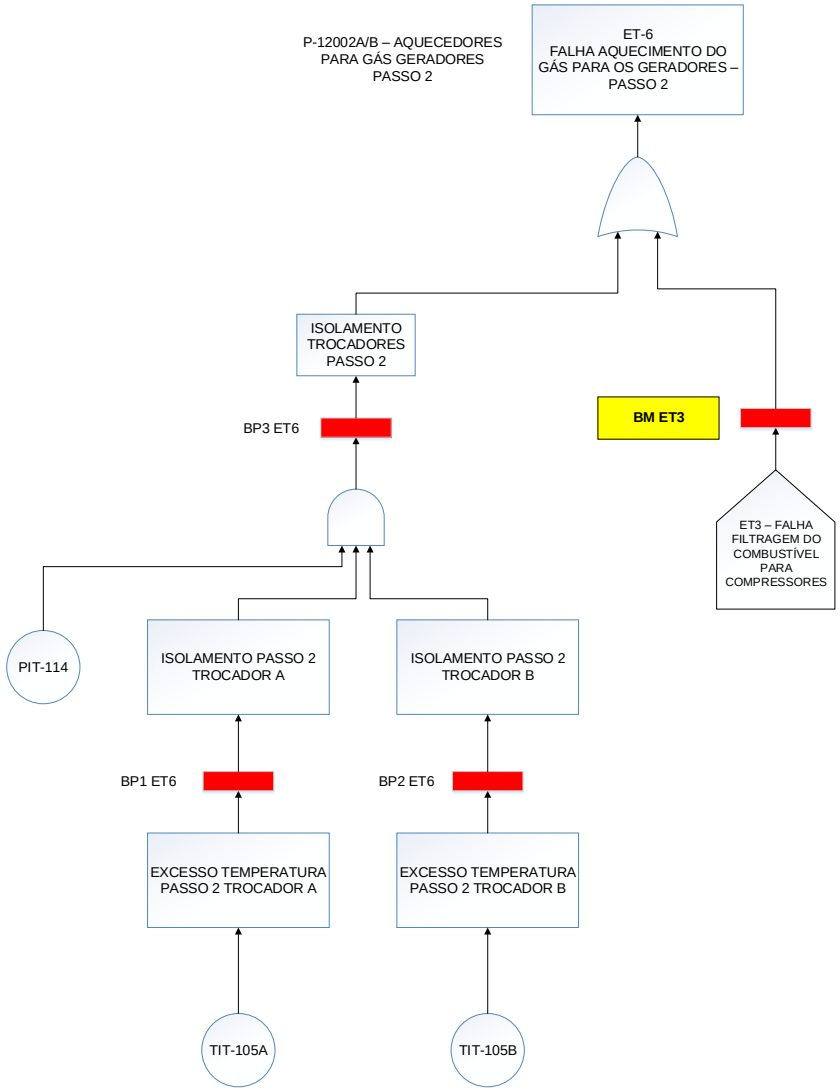
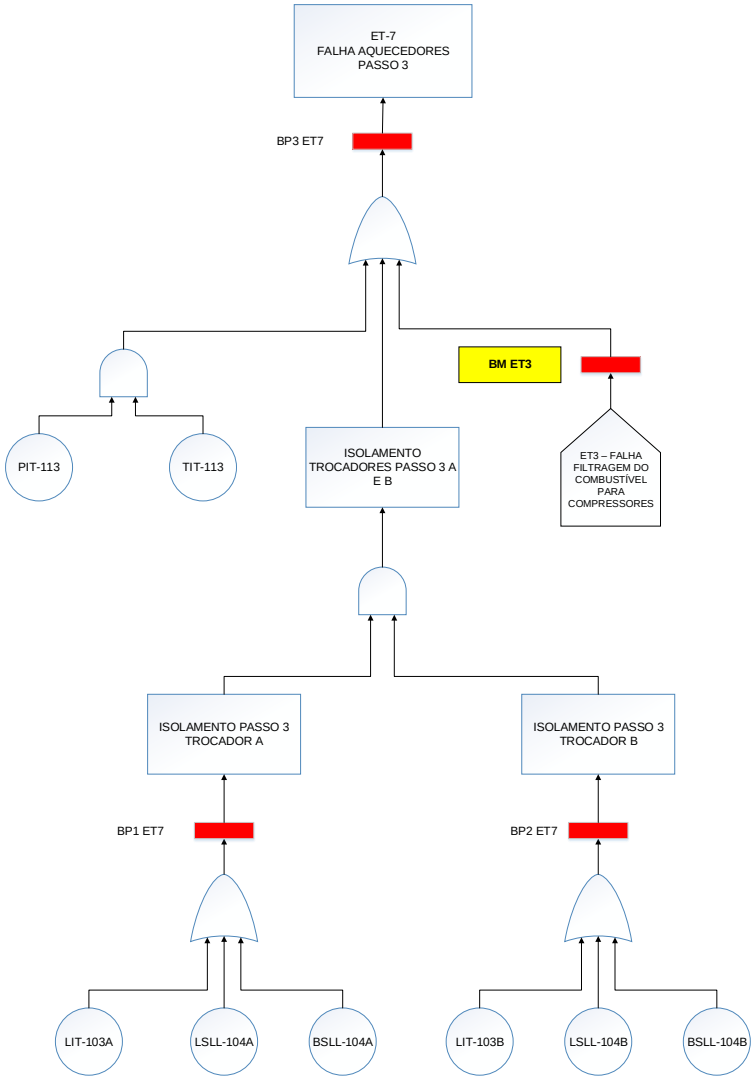


Figura 41 – Evento topo 7: falha nos aquecedores, passo 3



Dos resultados obtidos por meio dos métodos propostos nos Apêndices A1 e A2, nota-se a complexidade do processo, o elevado número de cenários críticos e a quantidade considerável do número de barreiras de segurança reativas de prevenção.

Utilizando-se arquiteturas em um mesmo nível, o algoritmo de controle de segurança seria de difícil modelagem e até, em certo sentido, muito perigoso, pois a abordagem centralizada não teria a capacidade de compreensão da interação entre os diversos eventos topo identificados. As medidas de prevenção e de mitigação, mesmo tendo-se como objetivo a prevenção e mitigação, poderia levar a planta / processo a um cenário catastrófico.

Note, na estrutura de árvore de falhas referente ao evento topo 5 “Falha no aquecimento para gás combustível dos compressores”, a presença dos elementos externos “ET1 Falha no processo de filtragem” e “ET3 –Falha filtragem combustível para compressores”.

Nesse sentido, a ocorrência de um evento topo, referente a uma estrutura de árvore de falhas externa, pode levar à ocorrência do evento topo 5. A interação entre falhas é constatada.

Considerando a arquitetura modular distribuída em camadas, à ocorrência do evento topo 1 (ou 3), o MCM irá enviar ao MCBP para que, de forma preventiva, performar as respectivas barreiras reativas de prevenção associadas ao evento topo 5, enquanto o módulo de controle da mitigação (MCM) realiza o envio ao respectivo controlador de mitigação da camada 2 para que sejam implementadas as SIFs de mitigação.

Caso a mitigação seja ineficaz, o MCM envia a informação ao Módulo de Controle das Brigadas – MCBRIG, de forma a solicitar ao controlador de brigadas - CBRIG, camada 2, as respectivas ações de mitigação das barreiras semi-reativas da nova classificação de barreiras proposta.

Partindo-se dos resultados obtidos, a próxima etapa consiste na síntese dos algoritmos de controle de cada módulo da arquitetura distribuída, para cada evento topo.

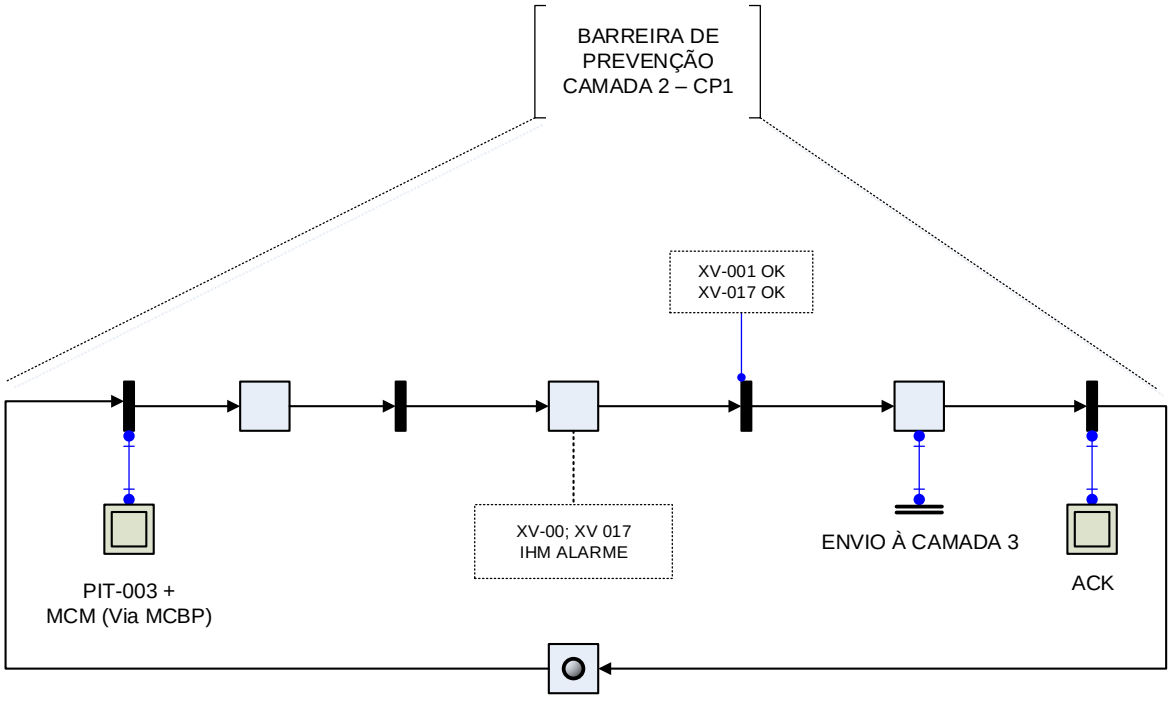
4.1.2 Síntese dos algoritmos de controle da camada 2

a) Algoritmos de prevenção – camada 2

Para a síntese dos algoritmos de prevenção da camada 2, cada controlador de prevenção, associado ao seu respectivo evento topo, irá desempenhar as respectivas SIFs em cada uma das barreiras reativas de prevenção, alocadas nas respectivas estruturas de árvores de falhas de seus eventos topo.

Como exemplo, consideremos o estudo Hazop para o evento topo 1, barreira de prevenção 1: BP1 ET1. O algoritmo de controle da barreira de prevenção da camada 2 da arquitetura de controle é representado na Figura 42.

Figura 42 – Algoritmo de prevenção – Camada 2, BP1 ET1



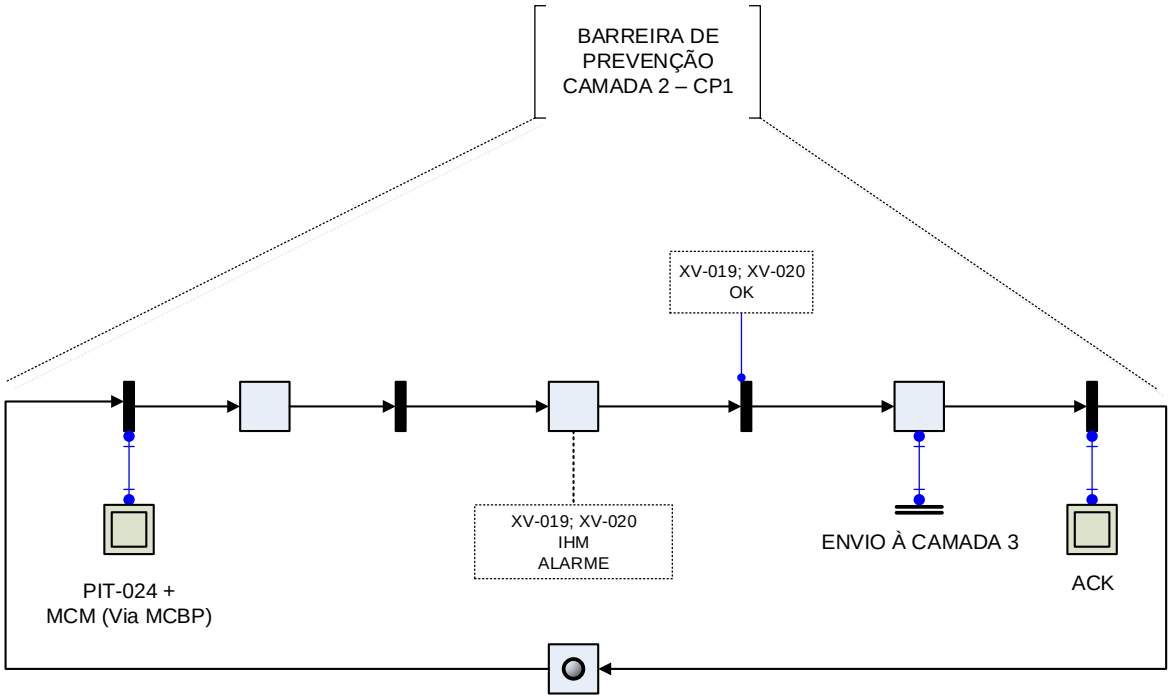
Fonte: Próprio Autor

Confirmada a ocorrência do evento inicializador “PIT-003”, ou comando enviado do módulo MCM, via MCBP, o CP de prevenção 1 irá performar o algoritmo de prevenção

que, para o exemplo, consiste no acionamento das válvulas de segurança “XV-001” e “XV-017”, e o registro da ocorrência na IHM e respectivo alarme. Após a confirmação de fechamento das respectivas válvulas, é feito o envio à camada 3, módulo MCBP. O grafo reinicia com a confirmação do recebimento “ACK”, enviada pelo módulo MCBP, camada 3.

Como outro exemplo, considere o resultado do estudo Hazop da barreira de prevenção 2 do evento topo 1, BP2 ET1. O algoritmo de prevenção da camada 2 é representado na Figura 43.

Figura 43 - Algoritmo de prevenção – Camada 2, BP2 ET1



Fonte: Próprio Autor

Confirmada a ocorrência do evento inicializador “PIT-024”, ou comando enviado do módulo MCM, via MCBP, o CP de prevenção 1 irá performar o algoritmo de prevenção que, para o exemplo, consiste no acionamento das válvulas de segurança “XV-019” e “XV-020”, e as informações na IHM e respectivo alarme. Após a confirmação de fechamento das respectivas válvulas, é feito o envio à camada 3, módulo MCBP. O grafo reinicia com a confirmação do recebimento “ACK”, enviada pelo módulo MCBP, camada 3.

Os demais algoritmos da camada 2 de prevenção são gerados por modelos análogos, em que os resultados do estudo Hazop para cada barreira de prevenção, de cada estrutura de árvore de falhas, são diretamente utilizados para a síntese dos respectivos algoritmos de prevenção da camada 2 de controle. Verifica-se, portanto, que a modularidade permitiu a quebra da complexidade na síntese dos algoritmos.

b) Algoritmos da mitigação – camada 2

Os algoritmos da mitigação são obtidos por meio dos resultados do estudo Hazop para a mitigação, com a confirmação de ocorrência do evento topo por meio de seus eventos inicializadores, ou por meio do insucesso das barreiras de prevenção de um dos possíveis caminhos críticos.

O modelo E-MFG representativo de todos os algoritmos de controle da mitigação, camada 2, são análogos aos da Figura 20.

Os resultados do estudo Hazop para o exemplo de aplicação são apresentados na seção 4.1.2.2, bem como o detalhamento dos algoritmos da mitigação, camada 2.

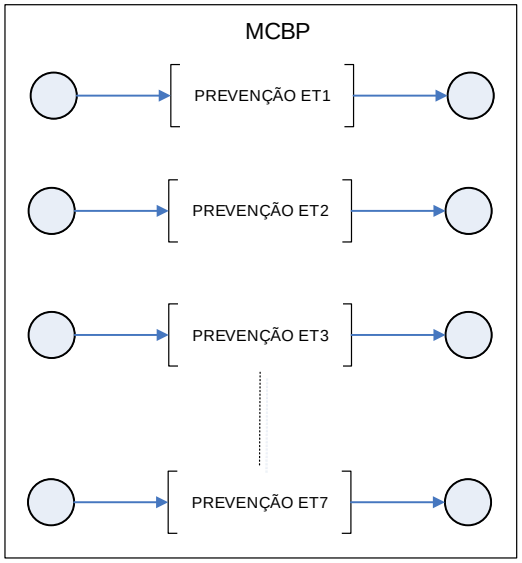
4.1.2 Síntese dos algoritmos da camada 3

Definidos os algoritmos de prevenção e mitigação da camada 2 da arquitetura proposta, o próximo passo consiste na síntese dos algoritmos da camada 3 de controle.

4.1.2.1Algoritmos de controle do MCBP

Identificados os eventos topo e os cenários críticos até sua ocorrência, o modelo PFS do MCBP é representado por meio da Figura 44

Figura 44 – Modelos PFS dos algorimos do MCBP, camada 3



Fonte: Próprio Autor

O refinamento de cada um dos modelos PFS dependerá da respectiva estrutura da árvore de falhas, representando todos os caminhos críticos até a ocorrência do respectivo evento topo. Para facilitar a compreensão da sistemática, serão definidas as etapas:

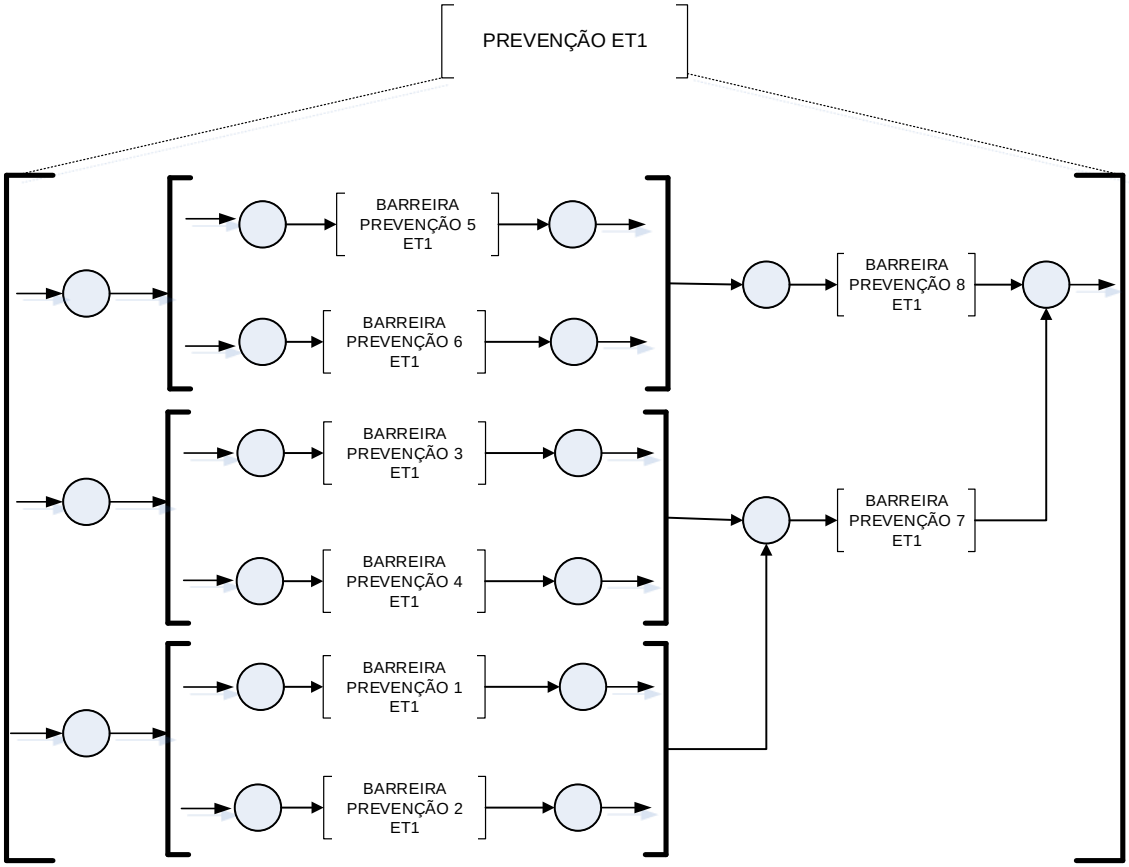
a) Síntese dos modelos PFS das estruturas das árvores de falhas de cada evento topo.

Considerando as árvores de falhas e os conjuntos de barreiras de prevenção associados a cada evento topo, o refinamento PFS de cada uma das atividades “PREVENÇÃO ETi”, da Figura 44, é representado nos modelos PFS das Figuras subsequentes[14]. Para facilitar a compreensão da sistemática, serão definidas as etapas:

A Figura 45 representa o refinamento PFS “PREVENÇÃO ET1”.

[14] Cada modelo PFS representa o conjunto de barreiras com as sequências críticas e os conectores lógicos das estruturas de árvores de falhas de cada evento topo.

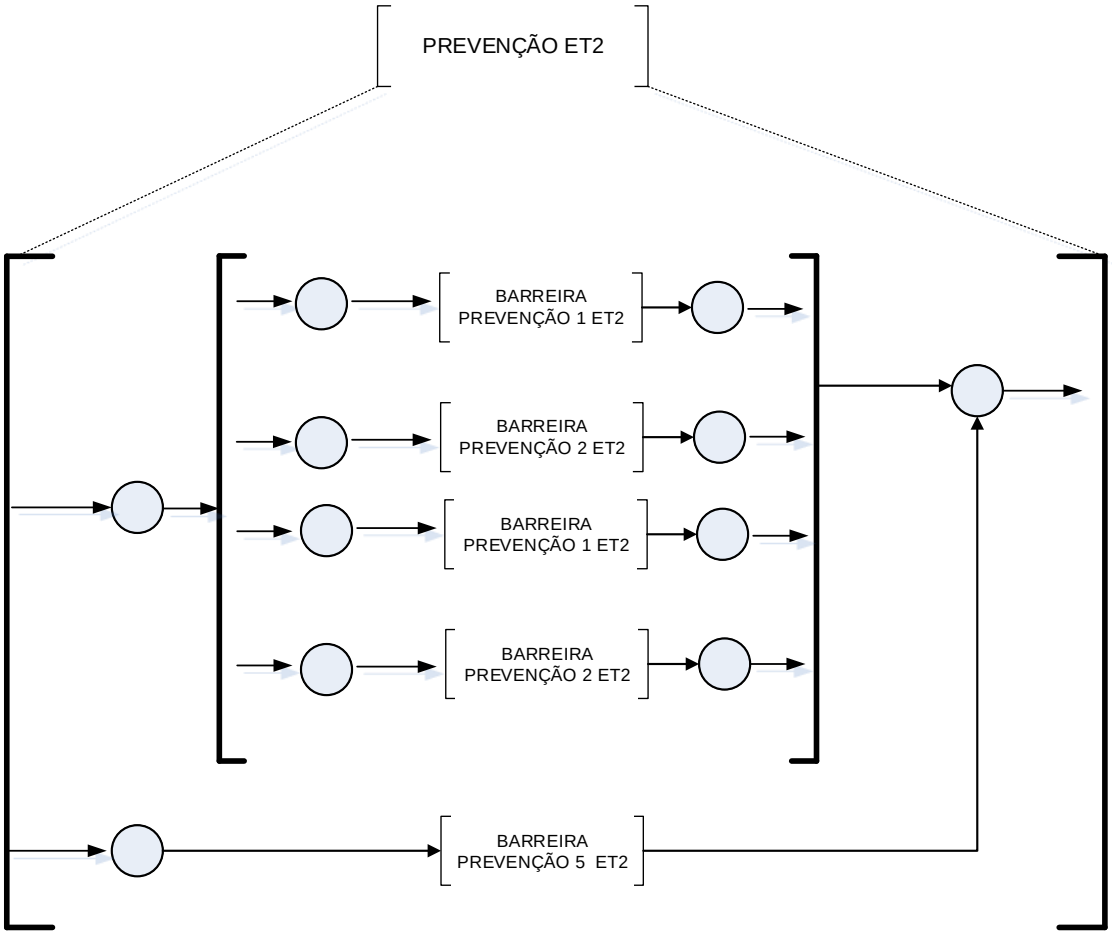
Figura 45 – Refinamento PFS “PREVENÇÃO ET1”



Fonte: Próprio Autor

A Figura 46 representa o refinamento PFS “PREVENÇÃO ET2”.

Figura 46 – Refinamento PFS “PREVENÇÃO ET2”



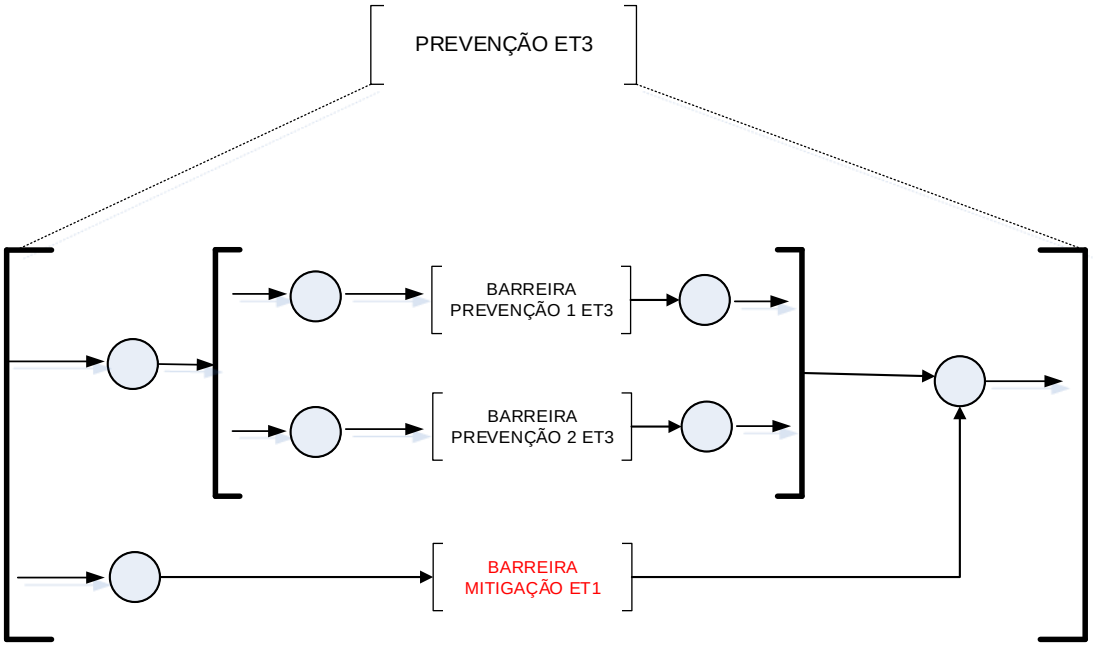
Fonte: Próprio Autor

A Figura 47 representa o refinamento PFS “PREVENÇÃO ET3”. Note que consta uma barreira de mitigação em seu conjunto de barreiras, evidenciando a questão da interação entre falhas críticas. A semântica da mitigação é distinta da prevenção, portanto tais interações serão tratadas no módulo de controle da mitigação – MCM.

Logo, tal barreira, embora conste na estrutura da árvore de falhas, não constituirá parte do algoritmo do módulo MCBP, e sim do MCM.

Situação análoga será considerada caso constem outras barreiras de mitigação em outros modelos PFS relativos ao MCBP.

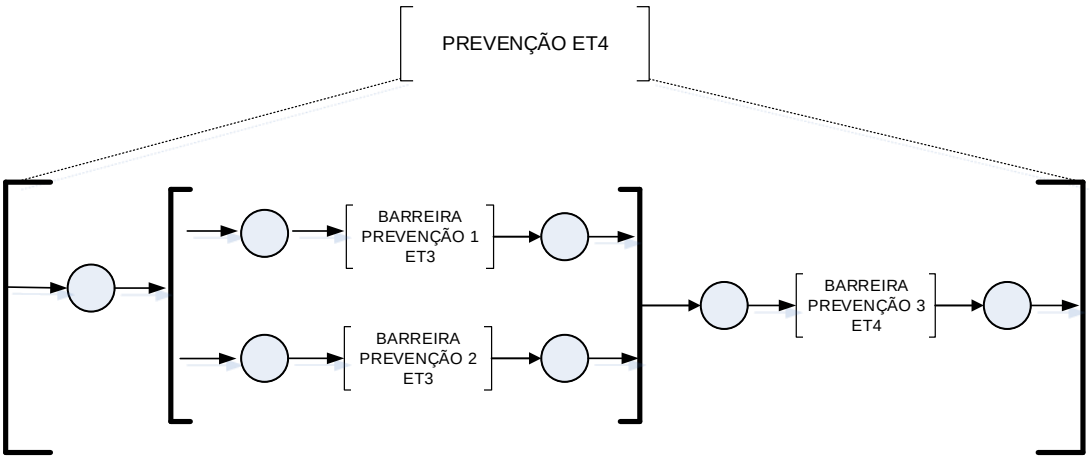
Figura 47 - Refinamento PFS “PREVENÇÃO ET3”



Fonte: Próprio Autor

A Figura 48 representa o refinamento PFS “PREVENÇÃO ET4”.

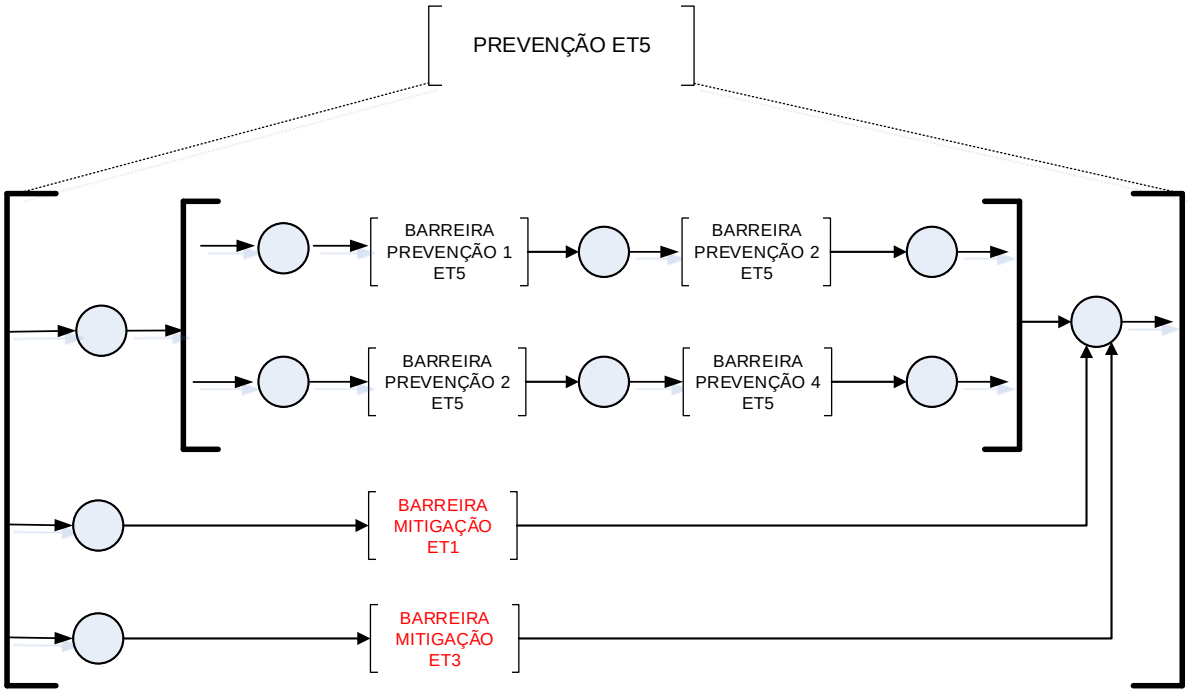
Figura 48 - Refinamento PFS “PREVENÇÃO ET4”



Fonte: Próprio Autor

A Figura 49 representa o refinamento PFS “PREVENÇÃO ET5”.

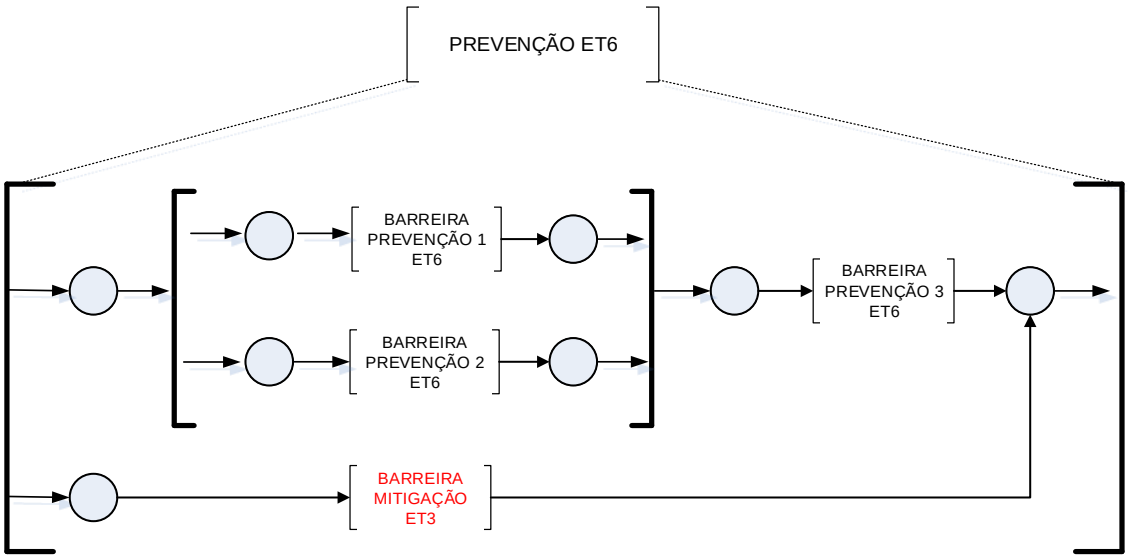
Figura 49 - Refinamento PFS “PREVENÇÃO ET5”



Fonte: Próprio Autor

A Figura 50 representa o refinamento PFS “PREVENÇÃO ET6”.

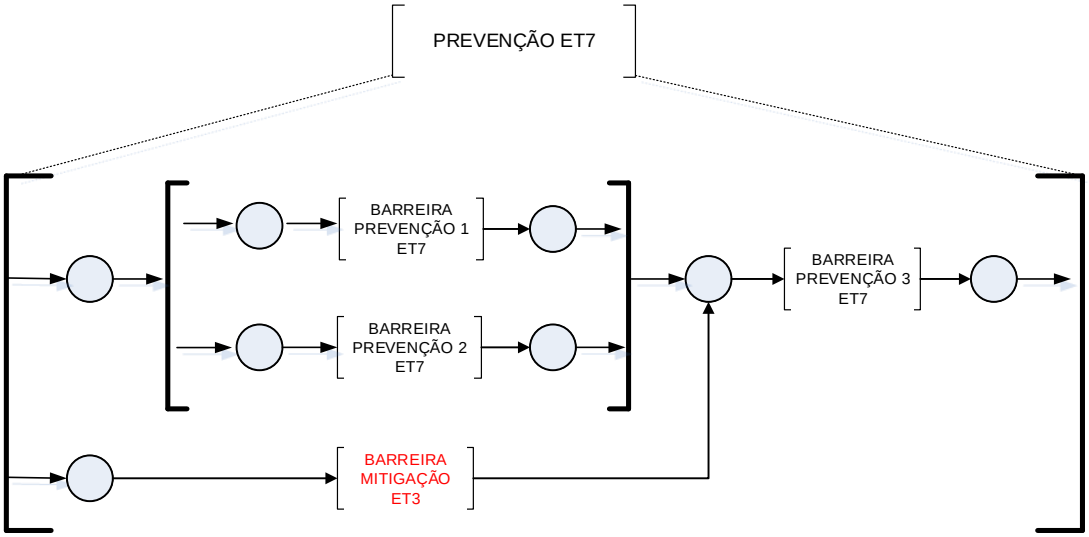
Figura 50 - Refinamento PFS “PREVENÇÃO ET6”



Fonte: Próprio Autor

A Figura 51 representa o refinamento PFS “PREVENÇÃO ET7”.

Figura 51 - Refinamento PFS “PREVENÇÃO ET7”



Fonte: Próprio Autor

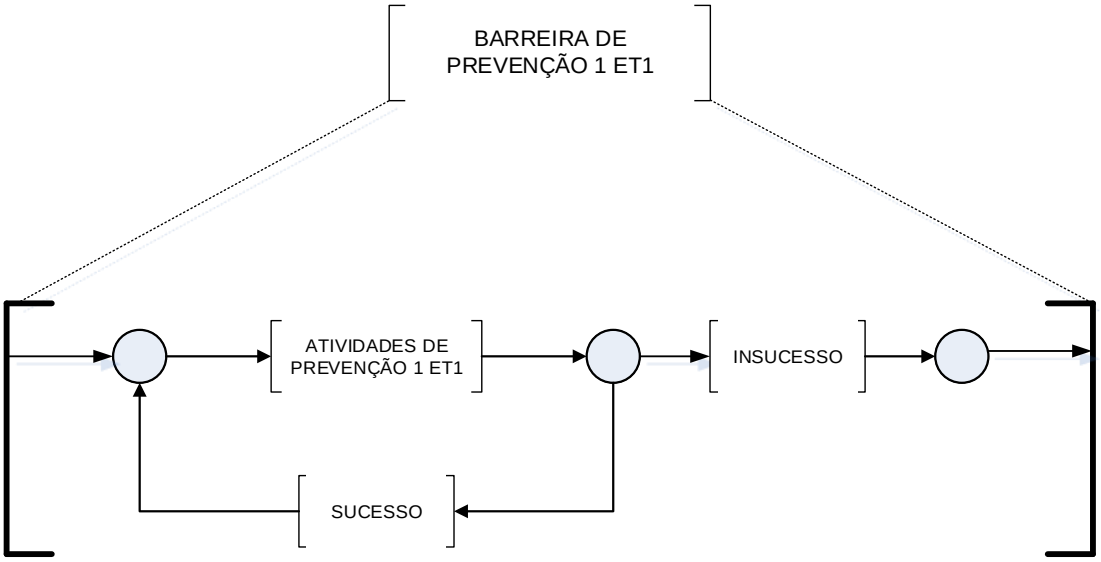
Definidos os modelos PFS das barreiras de prevenção das estruturas de árvores de falhas de cada evento topo, o próximo passo consiste em refinar cada uma das atividades “BARREIRAS DE PREVENÇÃO i ET i”

b) Refinamento das atividades “BARREIRAS DE PREVENÇÃO”

Para cada uma das barreiras de prevenção de cada uma das estruturas das árvores de falhas, é feito o refinamento PFS, representado por meio do exemplo da “BARREIRA DE PREVENÇÃO 1 ET1” da Figura 52.

O processo é análogo a todas as demais barreiras de prevenção.

Figura 52 – Refinamento PFS “Barreira de Prevenção 1 ET1”

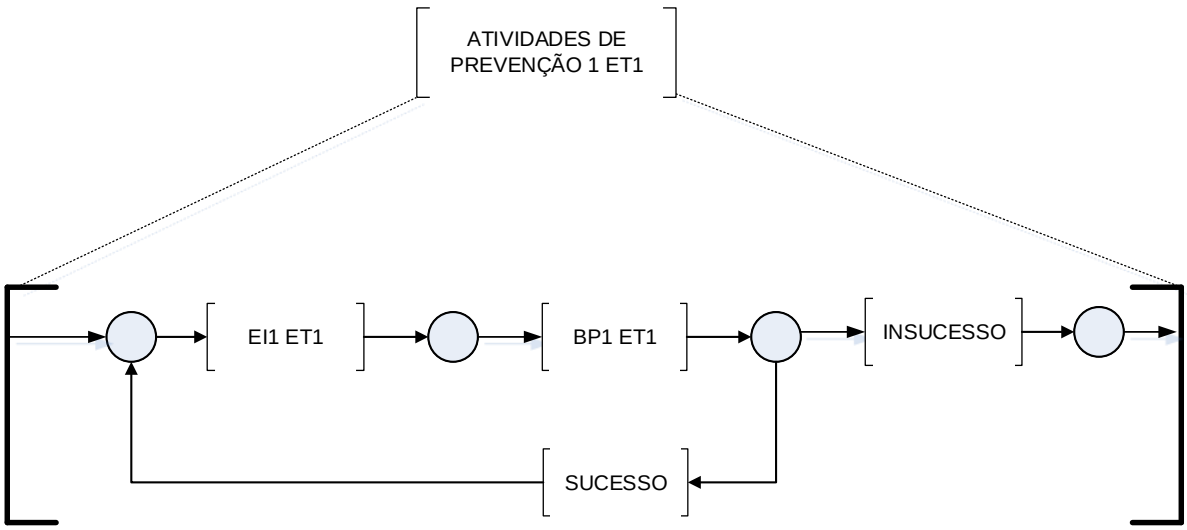


Fonte: Próprio Autor

c) Refinamento das atividades “ATIVIDADES DE PREVENÇÃO”

O próximo passo consiste no refinamento PFS “ATIVIDADES DE PREVENÇÃO”, representado por meio do modelo “ATIVIDADES DE PREVENÇÃO 1 ET1” da Figura 53.

Figura 53 – Refinamento do modelo PFS “Atividades de prevenção 1 ET1”



Fonte: Próprio Autor

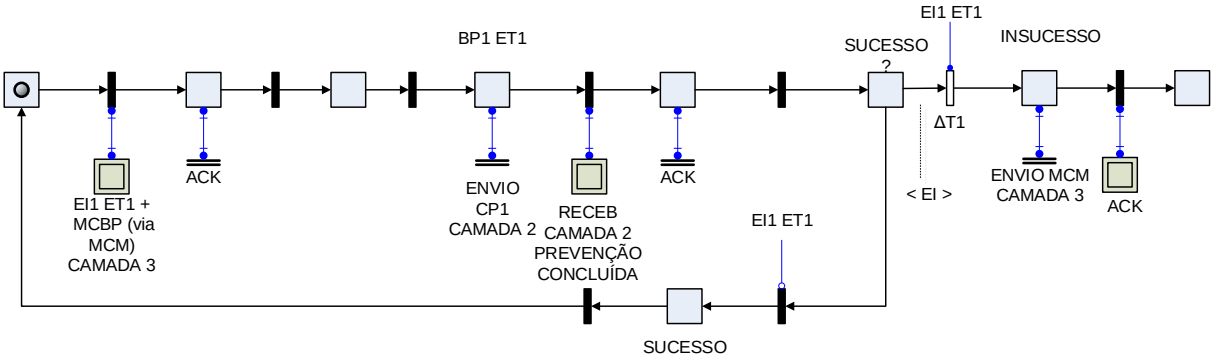
O modelo PFS da Figura 53 é análogo a todas as atividades de prevenção, de todas as barreiras de prevenção, associados a cada evento topo da planta / processo.

O refinamento para da atividade de detecção, coordenação e filtragem de falhas espúrias para o evento inicializador 1 do evento topo 1 (EI1 ET1), considerando-se o critério de votação 1oo1 adotado no estudo Hazop, é feito com base no modelo do Apêndice A.

d) Refinamento da atividade “BPi ETi”

O modelo E-MFG do algoritmo de controle, utilizando-se como exemplo o “BP1 ET1”, camada 3, MCBP, é representado por meio da Figura 54.

Figura 54 – Modelo E-MFG da “BP1 ET1”, MCBP, camada 3.



Fonte: Próprio Autor

A síntese dos demais algoritmos de controle do módulo MCBP, para cada barreira de prevenção associado à ocorrência de cada evento topo, é feito de forma análoga.

Verifica-se que, nesta etapa, é feita uma transcrição direta dos resultados do estudo Hazop para a definição do conjunto das SIFs de prevenção associadas às respectivas barreiras de prevenção a determinado evento topo. O respectivo algoritmo da camada 2, CP1, foi representado no modelo E-MFG da Figura 42.

4.1.2.2 Algoritmos de controle do MCM

Caso ocorra a ineficácia de todas as barreiras de prevenção associadas a um cenário crítico, ou ocorra o evento inicializador da ocorrência de um evento topo, o MCM implementará os respectivos algoritmos da mitigação, considerando-se os aspectos de interação entre falhas críticas, como por exemplo evidenciado no modelo PFS da Figura 47.

Em função da modularidade da arquitetura proposta, o estudo Hazop para a mitigação foi elaborado, considerando-se não só os aspectos de interação entre falhas críticas, evidenciado nos modelos PFS da camada 3 do módulo MCBP, mas também considerando os fluxos de hidrocarbonetos do exemplo de aplicação, e consequentes degenerações que devem ocorrer a montante e a jusante de cada subsistema. Adotou-se, para a elaboração do estudo, o modelo de energia proposto por (HADDON, 1990).

A consequência da ineficácia das barreiras de prevenção pode ocasionar sobrecarregamentos de pressão / temperatura, com consequências de vazamentos de gás natural ou ainda a ocorrência de chamas. A planta / processo já dispõe da instrumentação para detecção e gás e fogo em cada subsistema e, além dos respectivos atuadores seguros da mitigação, foi proposto o uso de gás carbônico pressurizado com válvulas de segurança.

No entanto, a detecção de fogo e gás pode ocorrer de forma independente das barreiras de segurança de prevenção, isto é, sem a confirmação de ocorrência dos eventos inicializadores da prevenção. Portanto, para cada barreira de mitigação do estudo Hazop, é feito o acionamento de todas as SIFs de prevenção associadas àquele evento topo, com o envio do módulo MCM ao módulo MCBP, com a inscrição “BP ETi”, ou seja, não há distinção do número da barreira, devendo ser performadas todas as barreiras de prevenção associadas àquele evento topo (p. ex. BP ET1), além das prevenções dos eventos topo a montante e a jusante, que possuem relação de fluxo de processo / estrutura das árvores de falhas.

Os resultados do estudo Hazop para as barreiras de mitigação à ocorrência de cada evento topo são representados por meio da Tabela 10.

Tabela 10 – Estudo Hazop para as SIFs de mitigação

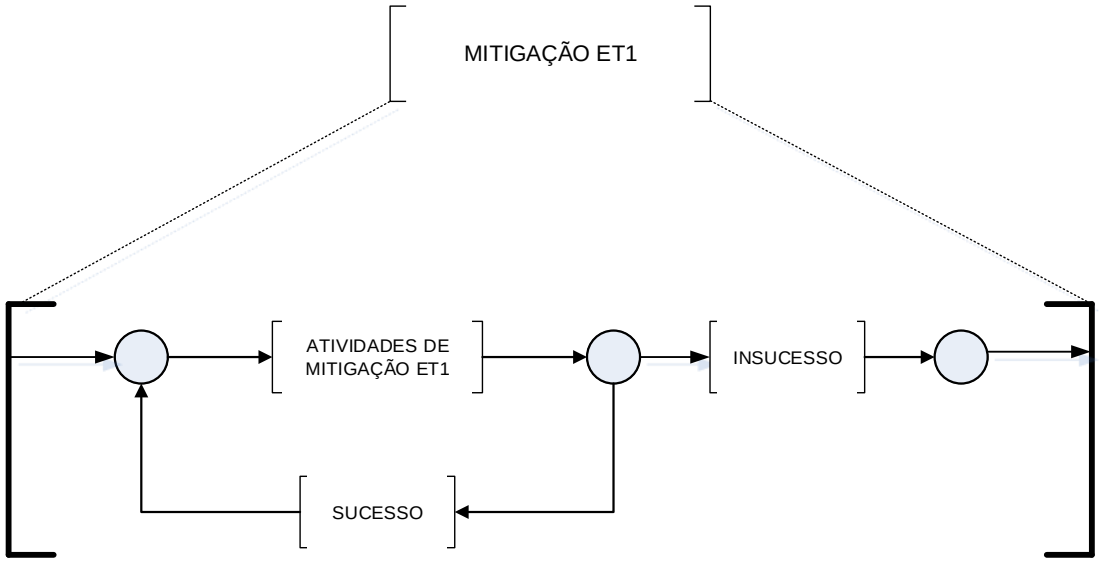
Barreira	Elemento	Evento crítico / desvio	Possíveis causas	Consequências	Ação	Equipamento	Sensores	Vot	Atuadores	SIL
BM ET1	ET1 - FT 12001 A/B	Falha no processo de filtragem - FT 12001 A/B ou gás ou fogo	INEFICÁCIA PREVENÇÃO / vazamentos	Incêndios, efeito dominó	BP ET1, BP ET3, BP ET5	FT-12001A/B	ASH-512A; ASH-512B; ASH-512C; ASH-512D	1oo1	XV-001; XV-017; XV-019; XV-020; XV-005;XV-006; XV-007; XV-020;XV-022; XV-023; XV-024, *shutdown* compressores gás carbônico, alarme	1
BM ET2	*Header* / compressores	Pressão muito alta ou gás / fogo em cada compressor	INEFICÁCIA PREVENÇÃO / vazamentos	Danos ao *header* incêndio nos compressores	BP ET2 / extinção	Compressores *header*	ASH 201; ASH 202; ASH 203; ASH 204	1oo1	*Shutdown* compressores XV-020;XV-022; XV-023; XV-024, gás carbônico, alarme	1
BM ET3	ET3 FT-12002 A/B	Falha no processo de filtragem - FT 12002 A/B ou gás ou fogo	INEFICÁCIA PREVENÇÃO / vazamentos	Incêndios, efeito dominó	BP ET3, BP ET2, BP ET5, BP ET6, BP ET7	FT-12002 A/B	ASH 101; ASH 102; ASH 103A; ASH 103B	1oo1	XV-110; XV-112; XV-125; gás carbônico, alarme	1
BM ET4	ET4 FT-12003 A/B	Falha no processo de filtragem - FT 12003 A/B ou gás ou fogo	INEFICÁCIA PREVENÇÃO / vazamentos	Incêndios, efeito dominó	BP ET4, BP ET2	FT-12003 A/B	BSH-501; BSH-502; BSH-503; BSH-504	1oo1	XV-121; XV-123; gás carbônico, alarme	1
BM ET5	ET5 P-12002 A/B	Falhas no aquecimento comb. compressores, gás ou fogo	INEFICÁCIA PREVENÇÃO / vazamentos	Danos aos compressores, incêndio, efeito dominó	BP ET5, BP ET2	P-12002 A/B	ASH-505A; ASH-505B; ASH 506	1oo1	XV-127; XV-129; gás carbônico, alarme	1
BM ET6	ET6 P-12002A/B	Falhas no aquecimento comb. geradores, gás ou fogo	INEFICÁCIA PREVENÇÃO / vazamentos	Danos aos geradores, incêndio, efeito dominó	BP ET6, BP ET2	P-12002 A/B	ASH-505A; ASH-505B; ASH 506	1oo1	XV-126; XV-128; gás carbônico, alarme	1
BM ET7	ET7 P-12002A/B	Falha nos aquecedores, gás ou fogo	INEFICÁCIA PREVENÇÃO / vazamentos	Danos aos geradores e compressores, incêndio, efeito dominó	BP ET7, BP ET2, BP ET5, BP ET6	P-12002 A/B	ASH-505A; ASH-505B; ASH 506	1oo1	XV-104A; XV-104B; gás carbônico, alarme	1

De posse dos resultados das SIFs de mitigação e da síntese dos algoritmos do módulo MCM (camada 3) e dos controladores da mitigação (camada 2), temos os seguintes resultados:

a) Barreira de mitigação ao evento topo 1 – BM ET1

O refinamento “MITIGAÇÃO ET1” é apresentado no modelo PFS da Figura 55.

Figura 55 – Refinamento PFS da mitigação do ET1

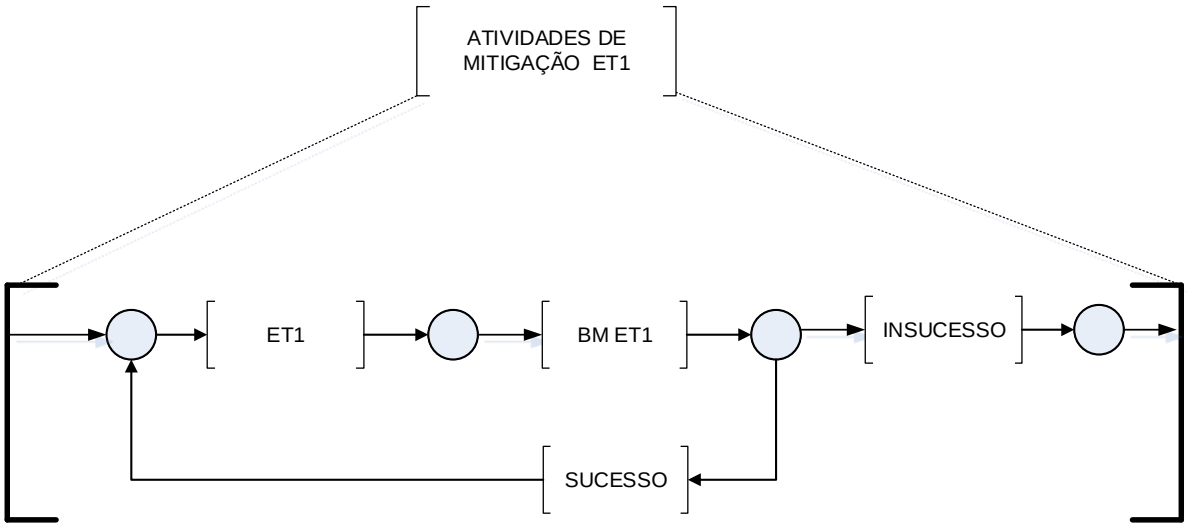


Fonte: Próprio Autor

O mesmo procedimento é adotado para todas as atividades “MITIGAÇÃO ETi” de todos os eventos topo.

O modelo PFS do refinamento das “ATIVIDADES DE MITIGAÇÃO ET1” é representado no modelo da Figura 56.

Figura 56 – Refinamento da atividade “Atividades de mitigação ET1”

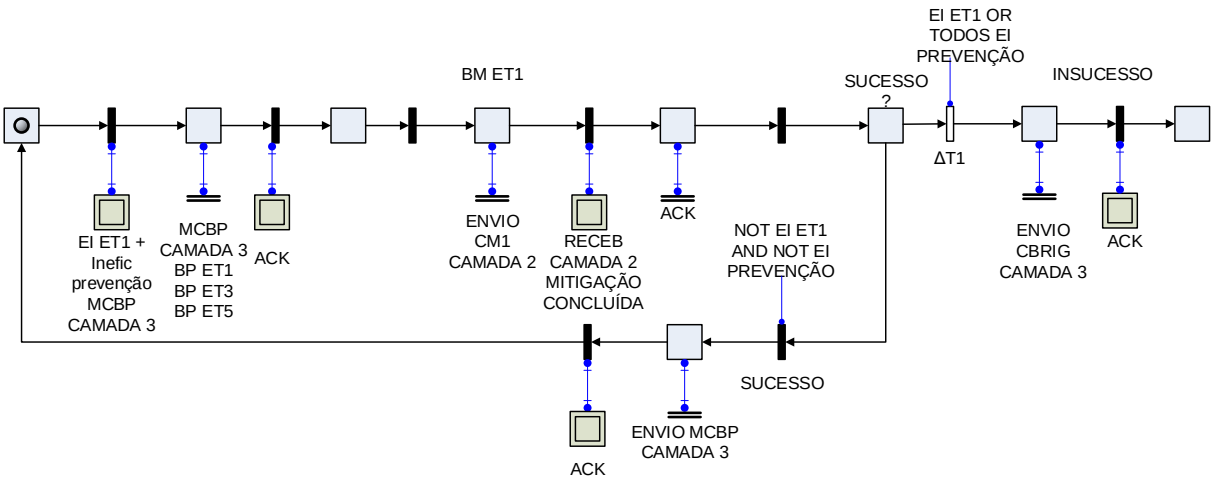


Fonte: Próprio Autor

O mesmo procedimento é adotado para todas as “ATIVIDADES DE MITIGAÇÃO ETi“ de todos os eventos topo.

O modelo E-MFG do algoritmo de controle da camada 3, MCM, do refinamento do modelo PFS das “ATIVIDADES DE MITIGAÇÃO ET1”, é representado por meio da Figura 57.

Figura 57 – Algoritmo de controle MCM– mitigação ET1.



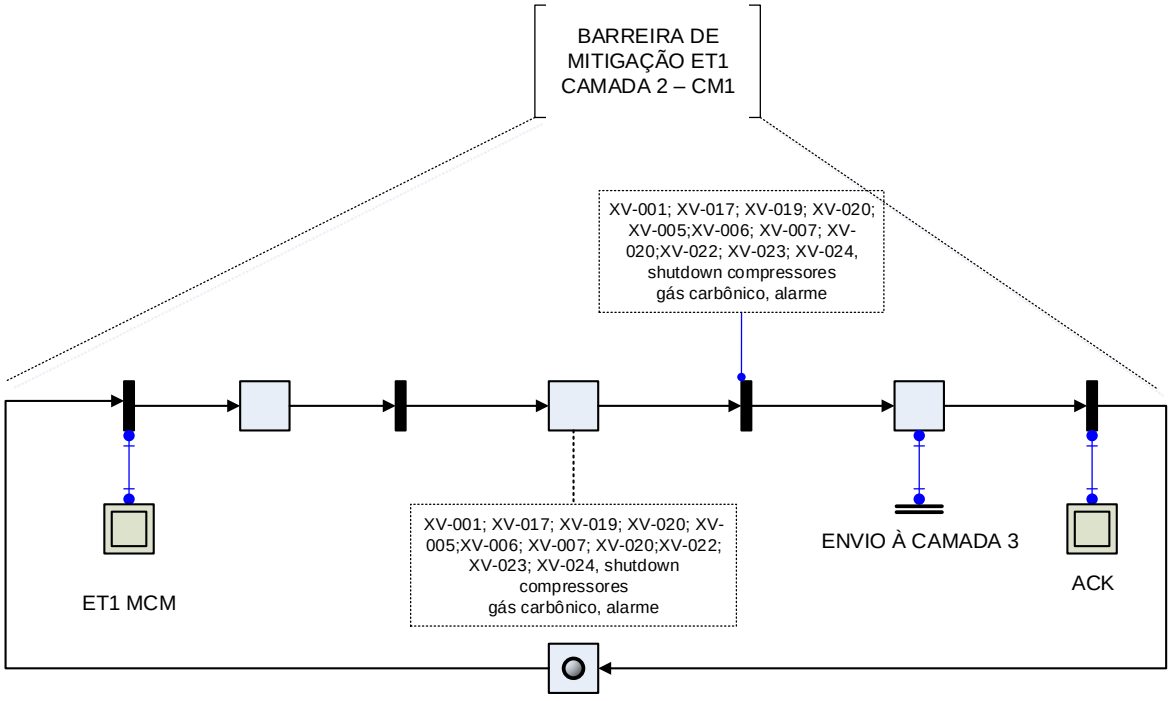
Fonte: Próprio Autor

O evento inicializador do ET1, de acordo com o estudo Hazop, é a ineficácia das barreiras de prevenção associadas a um dos caminhos críticos da estrutura da árvore de falhas, ou ainda a confirmação de um dos sensores de gás e fogo: “ASH-512A; ASH-512B; ASH-512C; ASH-512D”

O MCM envia mensagem ao MCBP para que todas as barreiras de prevenção, associadas aos respectivos eventos topo, sejam performadas (sem o atributo “EI”): “BP ET1, BP ET3, BP ET5”.

Na sequência, o MCM envia, ao controlador de mitigação 1 (CM1), camada 2, mensagem para que sejam performadas as respectivas SIFs de mitigação. O modelo E-MFG do algoritmo de controle é representado por meio da Figura 58

Figura 58 – E-MFG do algoritmo do CM1, camada 2



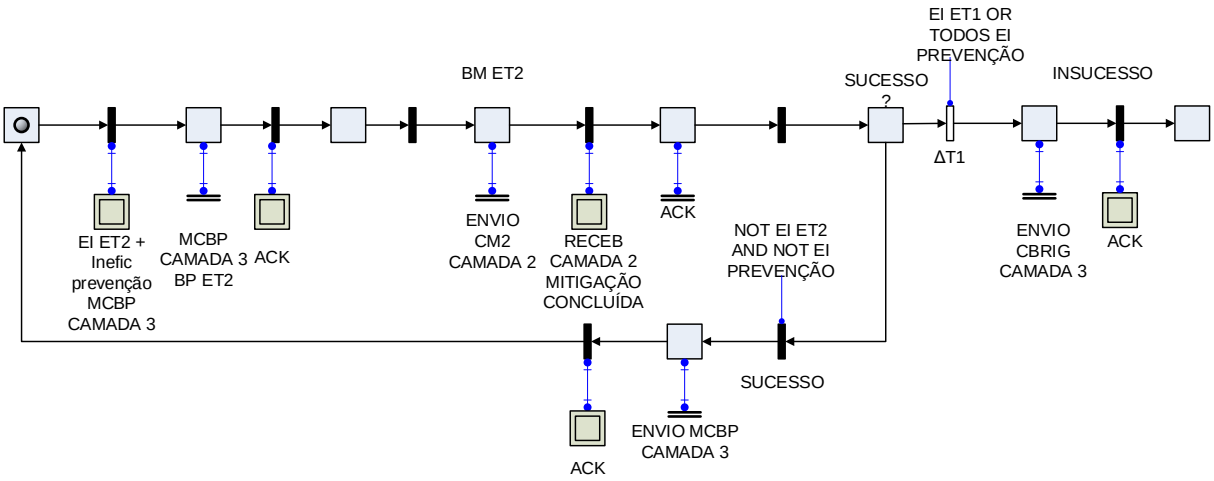
Fonte: Próprio Autor

Considerando-se as demais SIFs de mitigação obtidas por meio do estudo Hazop, temos:

b) Barreira de mitigação ao evento topo 2 – BM ET2

O modelo E-MFG do algoritmo de controle da camada 3, MCM, do refinamento do modelo PFS das “ATIVIDADES DE MITIGAÇÃO ET2”, é representado por meio da Figura 59.

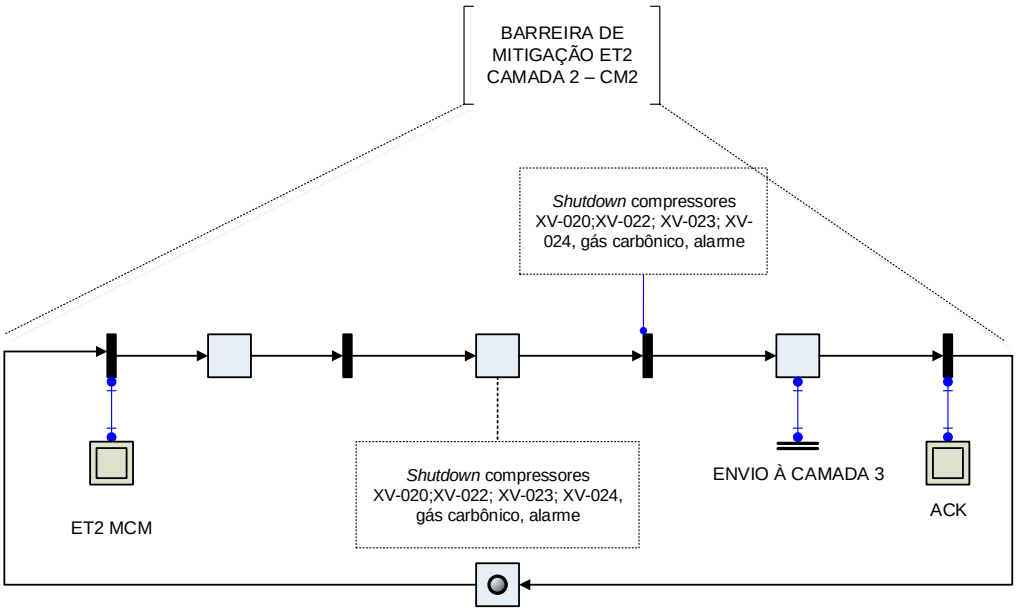
Figura 59 – E-MFG do algoritmo MCM – mitigação ET2.



Fonte: Próprio Autor

Já o algoritmo da mitigação, controlador de mitigação 2, camada 2, é representado na Figura 60.

Figura 60 - E-MFG do algoritmo do CM2, camada 2

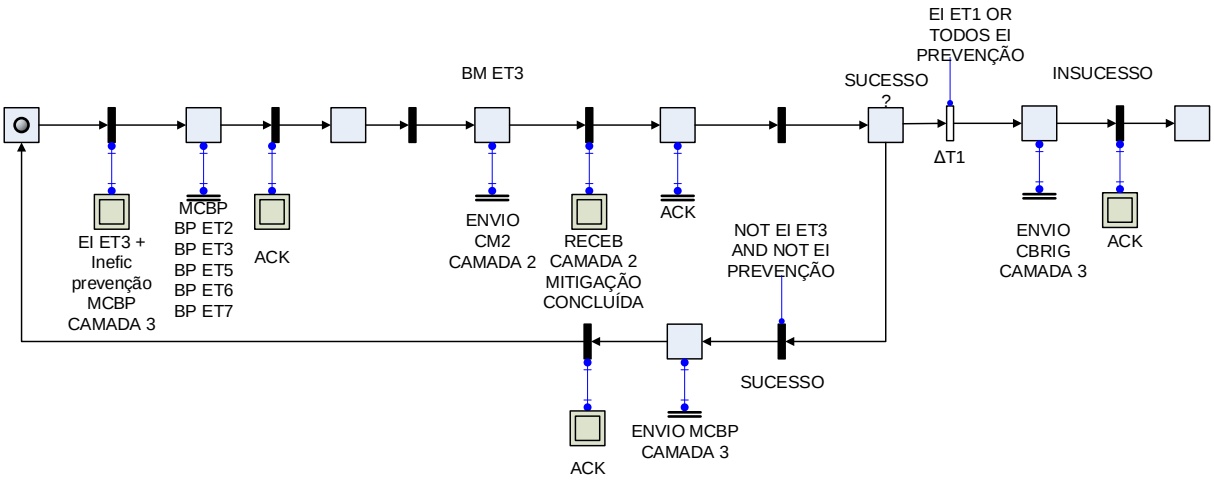


Fonte: Próprio Autor

c) Barreira de mitigação ao evento topo 3 – BM ET3

O modelo E-MFG do algoritmo de controle da camada 3, MCM, do refinamento do modelo PFS das “ATIVIDADES DE MITIGAÇÃO ET3”, é representado por meio da Figura 61.

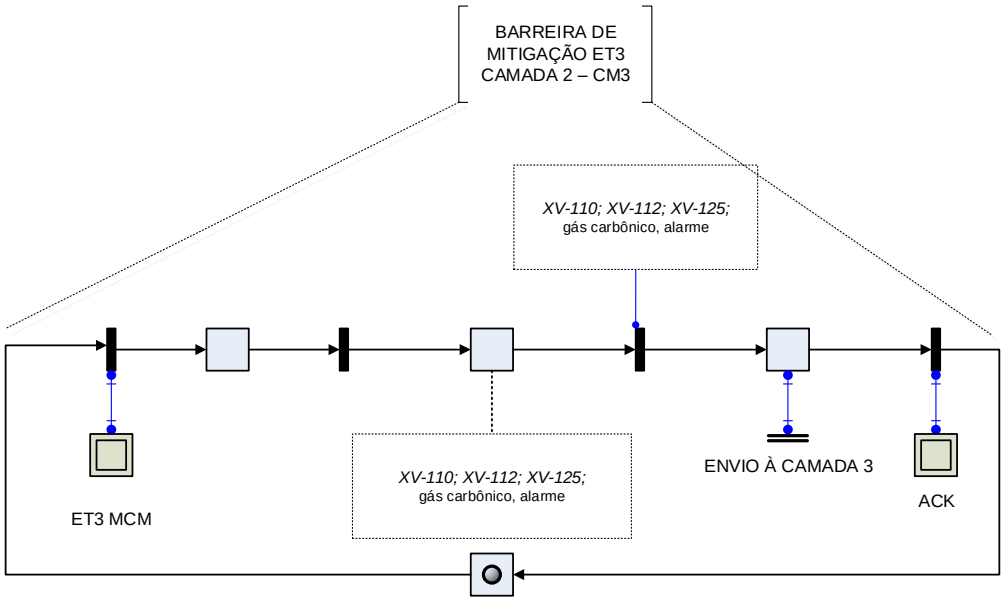
Figura 61 - E-MFG do algoritmo MCM – mitigação ET3.



Fonte: Próprio Autor

O algoritmo da mitigação, controlador de mitigação 3, camada 2, é representado na Figura 62 - E-MFG do algoritmo do CM3, camada 2.

Figura 62 - E-MFG do algoritmo do CM3, camada 2

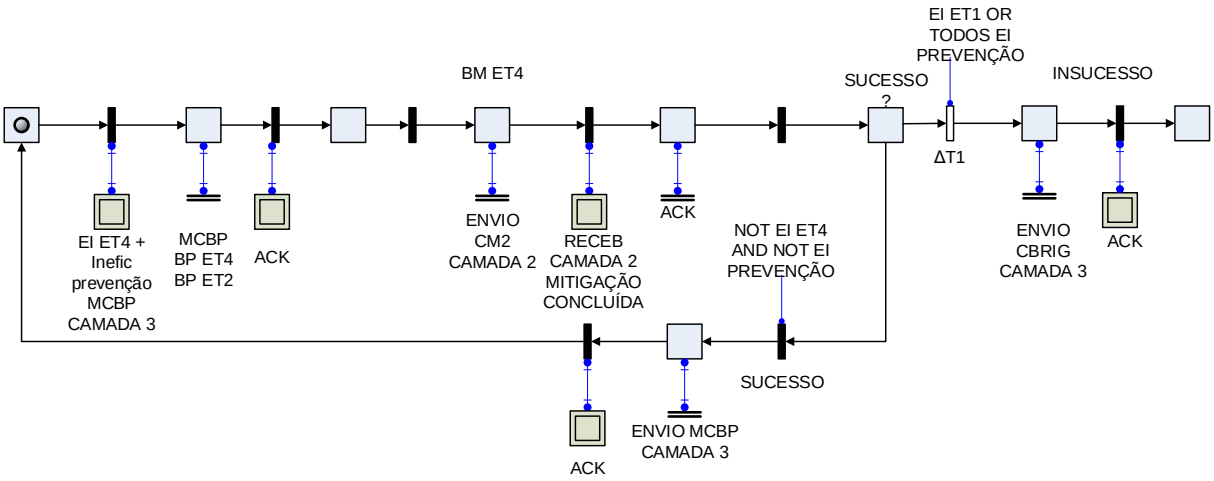


Fonte: Próprio Autor

d) Barreira de mitigação ao evento topo 4 – BM ET4

O modelo E-MFG do algoritmo de controle da camada 3, MCM, do refinamento do modelo PFS das “ATIVIDADES DE MITIGAÇÃO ET4”, é representado por meio da Figura 63.

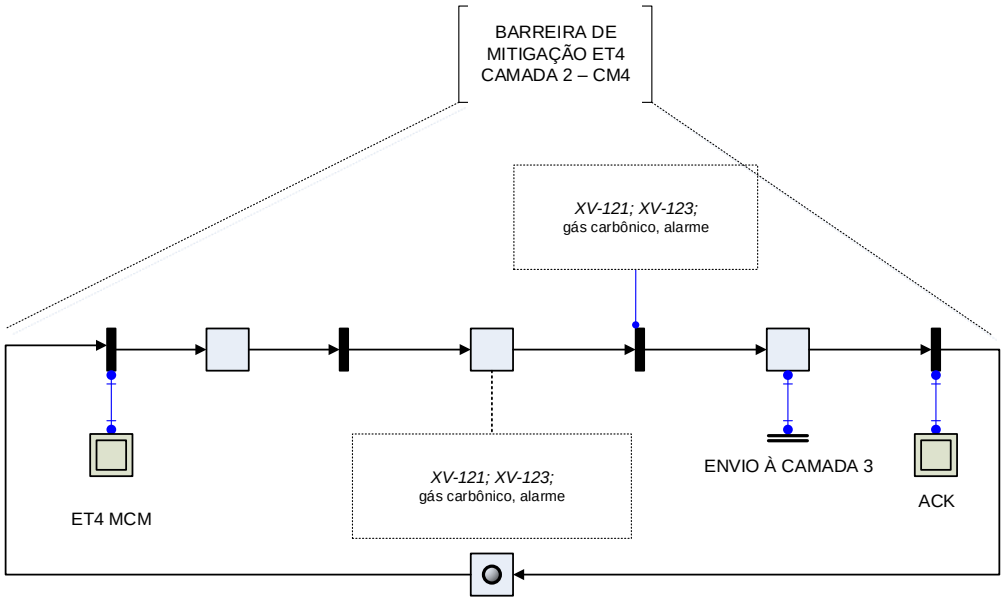
Figura 63 - E-MFG do algoritmo MCM – mitigação ET4.



Fonte: Próprio Autor

O algoritmo da mitigação, controlador de mitigação 4, camada 2, é representado na Figura 64

Figura 64 - E-MFG do algoritmo do CM4, camada 2

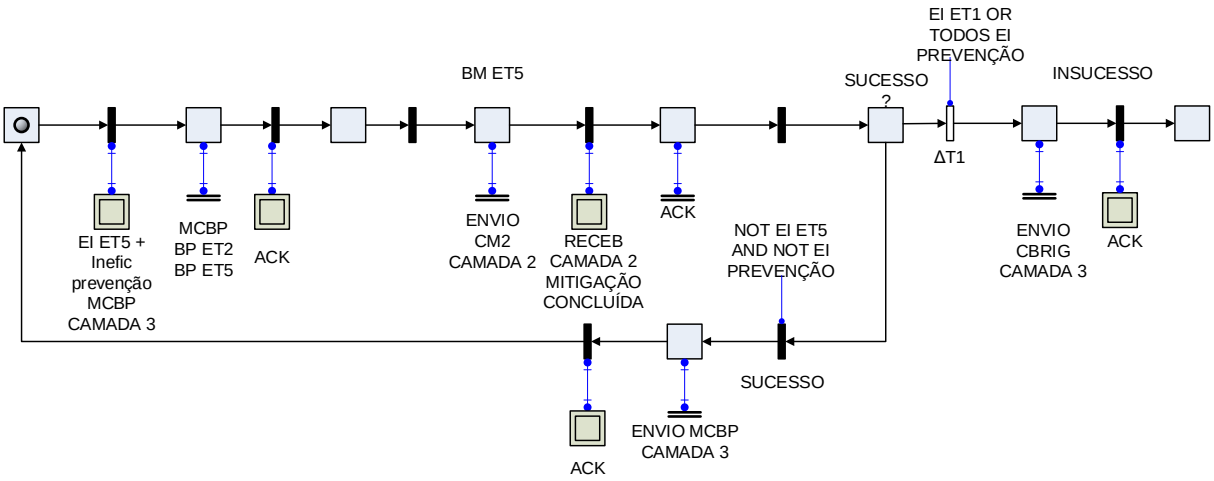


Fonte: Próprio Autor

e) Barreira de mitigação ao evento topo 5 – BM ET5

O modelo E-MFG do algoritmo de controle da camada 3, MCM, do refinamento do modelo PFS das “ATIVIDADES DE MITIGAÇÃO ET5”, é representado por meio da Figura 65.

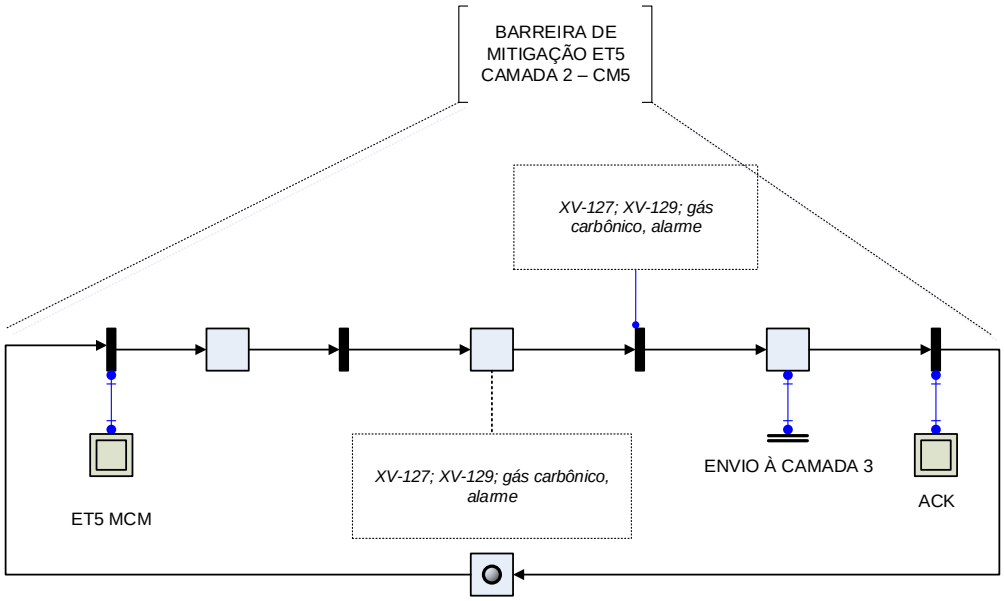
Figura 65 - E-MFG do algoritmo MCM – mitigação ET5.



Fonte: Próprio Autor

O algoritmo da mitigação, controlador de mitigação 5, camada 2, é representado na Figura 66

Figura 66 - E-MFG do algoritmo do CM5, camada 2

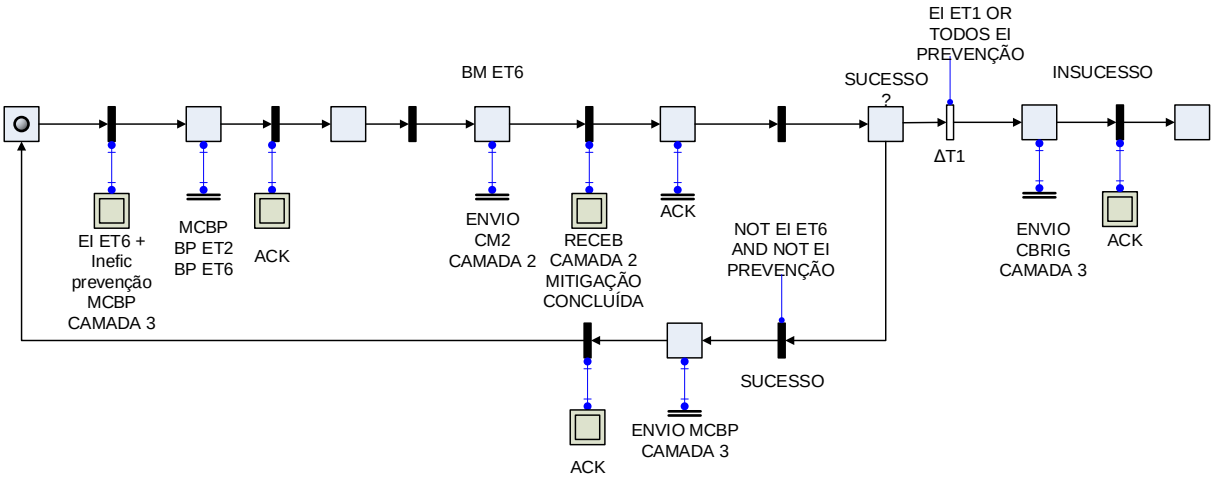


Fonte: Próprio Autor

f) Barreira de mitigação ao evento topo 6 – BM ET6

O modelo E-MFG do algoritmo de controle da camada 3, MCM, do refinamento do modelo PFS das “ATIVIDADES DE MITIGAÇÃO ET6”, é representado por meio da Figura 67.

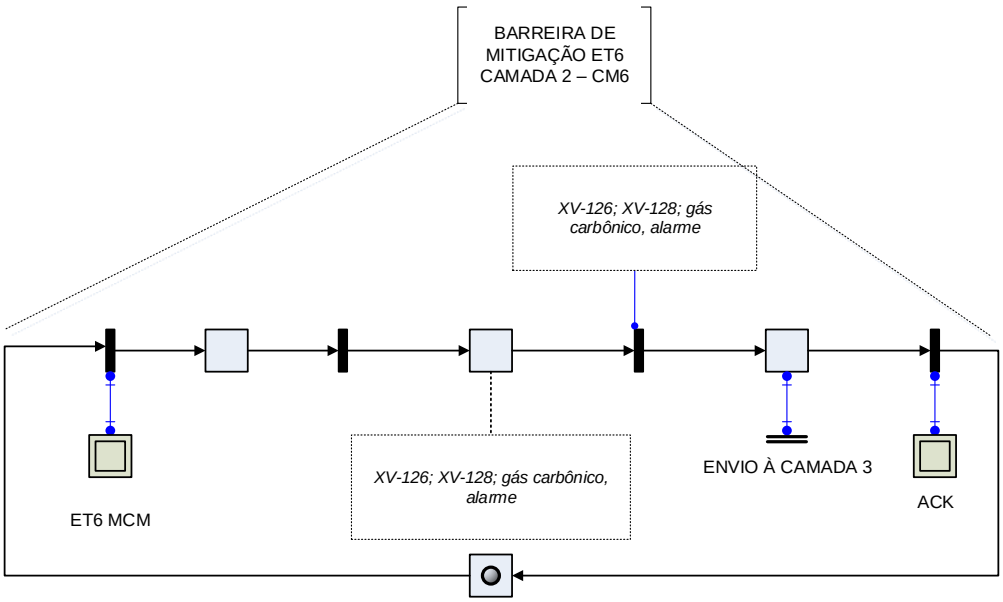
Figura 67 - E-MFG do algoritmo MCM – mitigação ET6.



Fonte: Próprio Autor

O algoritmo da mitigação, controlador de mitigação 6, camada 2, é representado na Figura 68.

Figura 68 - E-MFG do algoritmo do CM6, camada 2



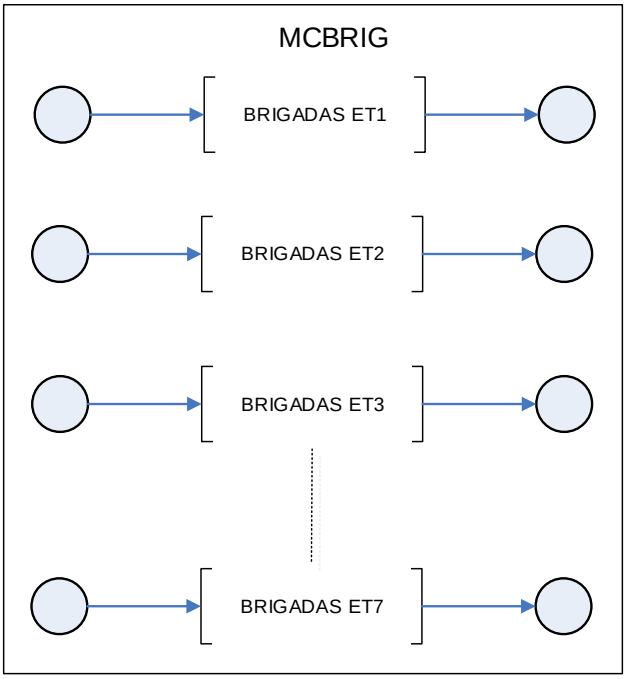
Fonte: Próprio Autor

Verifica-se, com base nos resultados, que a implementação dos algoritmos de mitigação das camadas 2 e 3 é praticamente uma transcrição direta dos resultados do estudo Hazop, que por sua vez considera os aspectos de interação entre as falhas críticas.

4.1.2.3Algoritmos de controle do MCB

O conjunto de atividades PFS de brigadas associadas ao insucesso da mitigação de cada evento topo no módulo MCBRIG é representado na Figura 69

Figura 69 – Modelo PFS das brigadas, MCBRIG



Fonte: Próprio Autor

Conforme mencionado na etapa de síntese do algoritmo, o MCBRIG deverá ter um conjunto de regras de prioridades em função da avaliação do potencial do dano de cada evento topo, e irá enviar, caso ocorram simultaneidades, qual(is) o evento(s) topo terá(ão) prioridades para as brigadas, em função da troca de informações entre os módulos.

4.2 DISCUSSÃO DOS RESULTADOS

O exemplo de aplicação apresentou um processo caracterizado por complexidade e criticidade, na medida em que o fluido de trabalho é altamente inflamável, sendo utilizado para alimentar as próprias instalações geradoras de energia elétrica e também por alimentar os equipamentos que realizam o trabalho de compressão do gás, após processos de filtragens. A planta já possuía um SIS de prevenção e mitigação, porém com uma arquitetura de controle centralizada.

Diante da complexidade inerente aos algoritmos da arquitetura utilizada, a planta / processo apresentava perdas econômicas significativas por conta do elevado número de paradas espúrias. O algoritmo resultante, em função do elevado risco de funcionamento do processo, promovia o *shutdown* de todo o processo quando o evento inicializador de alguma falha crítica fosse confirmado.

A reanálise de risco, com base no conceito de múltiplas linhas de defesa (defesa em profundidade) identificou um número maior de eventos topo e os possíveis caminhos críticos até suas ocorrências. Com base no conceito de barreiras reativas, foram inseridas as respectivas barreiras de segurança de prevenção e as respectivas SIFs de prevenção foram determinadas por meio do estudo Hazop. As estruturas de árvores de falhas resultantes evidenciaram a interação entre falhas críticas.

A nova arquitetura proposta mostrou-se adequada para a síntese formal dos algoritmos de controle, considerando-se a modularidade entre camadas e intra camadas de controle.

O resultado foi a quebra da complexidade na síntese dos algoritmos de controle, que passam a executar as interações evidenciadas nas estruturas de árvores de falhas. A análise a montante e a jusante foi facilmente tratada para os casos de degeneração completa de subsistemas.

Por fim, a proposta das barreiras semi-reativas, como reforço às SIFs de mitigação, permite uma melhor interação entre as barreiras técnicas reativas e os recursos humano-operacionais das brigadas, obrigatórias por imposição legal.

5. CONCLUSÕES

O trabalho propõe um método referenciado por normas de segurança para a identificação dos diversos eventos topo em uma planta / processo crítico, e os diversos cenários que antecedem suas ocorrências respectivas ocorrências.

A partir da definição dos cenários críticos de cada evento topo, são implementadas as barreiras de segurança reativas de prevenção e mitigação, considerando-se seus respectivos eventos inicializadores e as lógicas booleanas dos possíveis cenários críticos. A interação entre falhas críticas é evidenciada.

Arquiteturas de controle até então utilizadas para a síntese do algoritmo de controle de segurança não suportam o problema da explosão combinatória de possíveis interações entre os diversos processos de prevenção e mitigação, capazes de ocorrerem em um sistema crítico, ou seja, a complexidade de interação entre falhas não poderia ser tratada com êxito.

Nesse sentido, arquitetura proposta possui um diferencial, que é o fato das camadas de controle 2 e 3 possuírem semânticas distintas. Desta forma, o sistema supervisório contido na camada 3 possui a capacidade de realizar a alocação de processos de prevenção e/ou mitigação de acordo com o estado global do sistema crítico, observada por este supervisor.

A partir deste paradigma torna-se possível controlar a complexidade inerente aos sistemas críticos em que é possível existir a interação entre falhas críticas, considerando, também a possibilidade de atuação preventiva englobando a colaboração entre determinados processos de prevenção e de mitigação de acordo com a pertinência de cada cenário.

Com base nos resultados obtidos por meio do exemplo de aplicação, verificou-se não só a solução à questão da interação entre falhas críticas, mas a facilidade na implementação dos algoritmos de controle de cada módulo.

Em função do exposto, pode-se afirmar que o objetivo foi contemplado com êxito.

Outra importante contribuição a ser mencionada foi a proposta de uma nova classificação das barreiras de segurança, que permite a interface para o controle de barreiras de naturezas distintas.

5.1 TRABALHOS FUTUROS

Em conformidade com a norma N-2782 (NTP Petrobrás), as técnicas de análises de riscos recomendadas e obrigatórias dependem da atual fase do ciclo de vida útil da instalação.

Por conta da complexidade da planta / processo, alguns subsistemas / componentes certamente não estão na mesma fase de seu ciclo de vida útil, ainda que operacionais.

Consequentemente, as técnicas de análises de riscos podem resultar em árvores de falhas que podem ter estruturas diferentes em função da vida operacional, o que demandará barreiras de prevenção “latentes”, que devem ser inseridas e performadas em função da idade útil.

Multiplicando-se o conceito de múltiplas linhas de defesa (defesa em profundidade), pode-se chegar não só a subsistemas, mas a componentes críticos.

Em outras palavras, para cada estrutura de árvore de falhas da prevenção, os cenários críticos podem ramificar-se para outras estruturas de árvores de falhas, suportado pela arquitetura de controle proposta.

Legislações cada vez mais restritivas a critérios de sustentabilidade, meio ambiente e proteção à vida exigirá um número maior de camadas de proteção para a redução do risco inerente.

Considerando-se a arquitetura proposta e a nova classificação de barreiras semi-reativas de segurança, propõe-se a interação entre as barreiras reativas de prevenção e barreiras semi-reativas também para a prevenção.

Propõe-se a aplicação da sistemática ao contexto da I4.0, em que pode haver múltiplas camadas de controle (não só limitada a três), além da conectividade das barreiras semi-reativas a tecnologias de suporte às equipes humano-operacionais, incluindo-se as assistências remotas.

REFERÊNCIAS

ABNT ISO/IEC 31010. Gestão de riscos - Técnicas para o processo de avaliação de riscos. **ABNT**, Rio de Janeiro, BR, 2012.

ABNT NBR 14276. **Brigada de incêndio - Requisitos**. ABNT. Rio de Janeiro, p. 32. 2006.

ABNT NBR 15219. **Plano de emergência contra incêndio - Requisitos**. ABNT. Rio de Janeiro, p. 17. 2019.

ABNT NBR 5462. **Confiabilidade e Mantenabilidade**. ABNT. Rio de Janeiro, p. 37. 1994.

ARNALDOS, J. et al. Hazard and operability (HAZOP) analysis. A literature review. **Journal of Hazardous Materials - Elsevier**, n. 173, p. 19-32, 2009.

BADREDINE, A. et al. **A new multi objectives approach to implement preventive and protective barriers in bow tie diagrams**. Journal of Loss Prevention Process Ind. [S.l.]: [s.n.]. 2014. p. 238-253.

BAKOLAS, E.; SALEH, J. H. Augmenting defense-in-depth with the concepts of observability and diagnosability from Control Theory and Discrete Event Systems. **Reliability Engineering and System Safety**, Georgia, USA, 2011. 184-193.

BASILIO, J.C.; CARVALHO, L.K.; MOREIRA, M.V. Diagnose de falhas em sistemas a eventos discretos modelados por autômatos finitos. **Revista Controle & Automação**, v. 21, n. 5, p. 510-533, 2010.

BELL, R. Introducton to IEC 61508. **In Proceedings of ACS Workshop on Tools and Standards**, Sydney, Austrália, 2005.

BIERMANS, K.; VANSINA, P. **PLANOP: a method for performing loss of containment analysis**. Industrial Safety Administration, Department for the Supervision of Chemical Risks, Federal Public Service Employment, Labour and Social Dialogue. Belgium. 2005.

BOBBIO, A. **Comparison of methodologies for the safety and dependability assessment of an industrial programmable logic controller**. European Safety Dependability Conf. (ESREL). [S.l.]: N. Piccinini and E. Zio. 2001. p. 411-418.

BRAUER, W.; REISIG, W. Carl Adam Petri and Petri nets. **Informatik-Spektrum**, Heidelberg, v. 29, n. 5, p. 369-381, out. 2006.

BUCELLI, M. et al. **Assessment of safety barriers for the prevention of cascading events in oil and gas offshore installations operating in harsh environment.** Ocean Enginnering. Berlim: Elsevier. 2018. p. 171-185.

CACCIABUE, P. C. Human error risk management for engineering systems: a methodology for design, safety assessment, accident investigation and training. **Reliability Engineering and System Safety**, v. 83, p. 229-240, 2004.

CAMERON, L.; LARSEN-FREEMAN, D. Complex systems and applied linguistics. **International Journal of Applied Linguistics**, v. 17, p. 226-239, 2007.

CAO, X. R. A comparison of the dynamics of continuous and discrete event systems. **Proceedings of IEEE**, 77, 1989. 7-13.

CARVALHO, L. K. **Diagnose Robusta de Sistemas a Eventos Discretos**. Universidade Federal do Rio de Janeiro. Rio de Janeiro, p. 1-159. 2011. (tese de doutorado).

CAVALHEIRO, A. C. M. Sistema de controle para diagnóstico e tratamento de falhas em dispositivos de assistência ventricular. **Tese para obtenção do título de Doutor em Engenharia, Escola Politécnica da Universidade de São Paulo**, São Paulo, 2013. 213 p.

CCPS. **Layers of protection analysis:** simpfified process risk assessment. American Institute of Chemical Engineers. Nova York: [s.n.]. 2003.

CHEN, C.; DAI, J. Design and high-level synthesis of hybrid controller. **IEEE International Conference of Networking, Sensing and Control**, Taipei, Taiwan, 2004.

CHIEN, C. F.; CHEN, S. L.; LIN, Y. S. Using Bayesian network for fault location on distribution feeder. **IEEE Trans. Power Deliv.**, 17, n. 3, 2002. 785-793.

COCKSHOTT, J. E. Probability bow-ties: a transparent risk management tool. **Process Safety Environment Protection**, 2005. 307-316.

COOPER, G. F.; HERSKOVITS, E. A Bayesian method for the induction of probabilistic networks from data. **Machine Learning**, 9, 1992. 309-347.

CRUZ-CAMPA, H. J.; CRUZ-GOMES, M. J. Determine SIS and SIL using HAZOPS. **Wiley Interscience**, fev. 2009. Disponivel em: <www.interscience.wiley.com>.

CRUZ-CAMPA, H. J.; CRUZ-GOMEZ, M. J. Determine SIS and SIL using HAZOPS. **Process Safety Progress**, 29, n. 1, 2009. 22-31.

CURY, J. E. R. Teoria de controle supervisório de sistemas a eventos discretos. **V Simpósio Brasileiro de Automação Inteligente**, Canela - RS, 2001. 68.

DEI-SVALDI, D.; VAUTRIN, J. P. Les automates programmables. Nouvelles Technologies, nouveaux risques, príncipes de sécurité à appliquer. **Cashiers de notes documentaires**, 1989. 467-473.

DIANOUS, V.; FIEVEZ, C. ARAMIS ptoject: a more explicit demonstration of risk control through the use of bow-tie diagrams and the evaluation of safety barrier performance. **Hazard Mather**, 2006. 220-223.

DIMAIO, F. et al. Accounting for safety barriers degradation in the risk assessment of oil and gas systems by multistrate Bayesian networks. **Reliability Engineering & System Safety**, 216, 2021. 107943.

DING, L. et al. Quantitative fire risk assessment of cotton storage and a criticality analysis of risk control startegies. **FAM - Fire and materials an international journal**, 44, n. 2, 2020. 165-179.

DOE, G. **Implementation Guide for use with DOE Order. Accident Investigations**. [S.l.]. 1997.

DUTUIT, Y. et al. Probabilistic assessments in relationship with safety integrity levels by using Fault Trees. **Reliability Engineering and System Safety**, v. 93, n. 12, p. 1867-1876, 2008.

DUTUIT, Y.; RAUZY, A.; SIGNORE, J. A snapshot of methods and tools to assess safety integrity levels of high-integrity protection systems. **IMechE**, 222, 2008.

EXIDA. **The Exida 61508 Certification Program - FAQ**. [S.l.]. 2007.

FANG, L.; ZONGZHI WU, L. W. A. J. L. **Design and Development of Safety Instrumented System**. Proceedings of the IEEE International Conference on Automation and Logistics. Qingdao: [s.n.]. 2008. p. 2685 - 2690.

FERRAREZI, R. C. et al. **Formal Verification of Safety control system based on Ghenesys Net**. 18th International Conference on Circuits, Systems, Communications and Computeres - CSCC 2014. [S.l.]: [s.n.]. 2014a.

GOBLE, W. M.; CHEDDIE, H. **Safety Instrumented Systems Verification:** Practical Probabilistic Calculations. 1st. ed. Research Triangle Park: ISA - The Instrumentation, Systems and Automation Society, 2005.

HADDON, W. Energy damage and the ten countermeasure strategies. **The Journal of the Human Factors and Ergonomics Society**, 1990. 355-366.

HELMAN, H.; ANDREY, P. R. P. **Análise de Falhas - Aplicação dos métodos de FMEA e FTA**. Fundação Cristiano Otoni. Belo Horizonte. 1995.

HOLLNAGEL, E. Risk + barriers = safety? **Safety Science**, Sophia Antipolis, France, v. 46, p. 221-229, jun. 2007.

HOSSEINNIA DAVATGAR, B.; PALTRINIERI, N.; BUBBICO, R. Safety barriers management: risk-based approach for the oil and gas sector. **Journal of Marine Science and Engineering**, 9, n. 7, 2021. 722.

HSE. **Guidance for the topic assessment of the major accident hazard aspect of safety cases (GASCET)**. Health and SAfety Executive. Reino Unido. 2006a.

IEC. **IEC 61511 - Safety instrumented systems for the process industry sector**. International Electrotechnical Commission. Geneva. 2003.

IEC. **IEC 61131 Programmable Controllers - part 3: Programming Languages.** IEC - International Eletrotechnical Comission. [S.l.]. 2003a.

IEC 60812. **IEC 60812 - Analysis techniques for system reliability - procedures for failure modes and effects analysis (FMEA)**. IEC - International Electrotechnical Commission. Geneva, Switzerland. 2006.

IEC 61025. **IEC 61025 - Fault Tree Analysis (FTA)**. IEC - International Electrotechical Comission. Geneva, Switzerland. 2008.

IEC 61882. **IEC 61882 - Hazard and operability studies (Hazop) - application guide.** IEC - International Electrotechnical Comission. London, UK, p. 58. 2001. (ISBN 0 580 37625 7).

IEC 62502. **Analysis techniques for dependability - Event Tree Analysis**. IEC. Geneva, Suíca, p. 34. 2010.

IEC: 61508. **IEC 61508 - Functional safety of electrical/electronic/programmable electronic safety related systems**. International Electrotechnical Commission. Geneva. 2010.

IEC: 61508 PARTE IV. **IEC 61508 parte IV - Functional safety of electrical/electronic/programmable electronic safety-related systems**. International Electrotechnical Commission. Geneva. 2010.

IEC: 61511. **IEC 61511 - Safety Instrumented Systems for the process industry sector**. International Electrotechnical Commission. Geneva. 2003.

ISA S-5.1-1984. **ISA-S5.1 — Instrumentation Symbols and Identification**. Instrument Society of America. Research Triangle Park. 2009.

JENSEN, K. **Coloured Petri Nets:** Basic Concepts, Analysis Methods and Practical Use. [S.l.]: Springer-Verlag, v. 1, 1992.

KAMTEKAR, D. M. **Implementation of Functional Safety in a robotic manufacturing cell using IEC 61508 Standard and Siemens Technology**. Rochester Institute of Technology. New York. 2009.

KNIGHT, J. C. Safety Critical Systems: Challenges and Directions. **Proceedings of the 24rd International Conference on Software Engineering**, Orlando, Florida, USA, p. 547-550, Maio 2002. ISSN 1-58113-472-X.

LUNDTEIGEN, M. A.; RAUSAND, M. Architectural constraints in IEC 61508: Do they have the intended effect? **Reliability Engineering and System Safety**, v. 94, n. 2, p. 520-525, 2009.

MATSUSAKI, C. T. M. Modelagem de sistemas de controle distribuídos e colaborativos de sistemas produtivos. **Tese (Doutorado), Escola Politécnica da USP**, São Paulo, 2004. 154 p.

MAZZOLINI, ; BRUSAFERRI, ; CARPANZANO, E. **An Integrated Framework for Model-based Design and Verification of discrete Automation Solutions**. Proceedings 2011 9th IEEE International Conference on Industrial Informatics. Milan: [s.n.]. 2011. p. 545-550.

MISURI, A.; LANDUCCI, G.; COZZANI, V. Assessment of safety barrier performance in Natech scenarios. **Reliability Enginnering & System Safety**, 193, 2020. 106597.

MISURI, A.; LANDUCCI, G.; COZZANI, V. Assessemnt of safety barrier performance in the mitigation of domino scenarios caused by Natech events. **Reliability Engineering & System Safety**, 205, 2021a. 107278.

MISURI, A.; LANDUCCI, G.; COZZANI, V. Assessment of risk modification due to safety barrier performance degradation in Natech events. **Reliability Engineering & System Safety**, 212, 2021b. 107634.

MIYAGI, P. E. **Controle Programável - Fundamentos do Controle de Sistemas a Eventos Discretos**. São Paulo: Editora Edgard Blücher Ltda, 1996.

MODARRES, M. **Risk Analysis in Engineering - Techniques, Tools and Trends**. 1. ed. Florida: CRC Press, 2006.

MODARRES, M.; KAMINSKIY, M.; KRIVTSOV, V. **Reliability Engineering and Risk Analysis:** A Practical Guide. 2. ed. New York: CRC Press, 2009.

N-2782, N. **Critérios para a aplicação de técnicas de avaliação de riscos**. CONTEC - Petrobrás. Rio de Janeiro. 2015.

NAKAMOTO, F. Y. Projeto de sistemas modulares de controle para sistemas produtivos. **Tese para obtenção do título de Doutor em Engenharia, Escola Politécnica da USP**, São Paulo, 2008. 176 p.

OVIDI, F. et al. Agent-based model and simulation of mitigated domio scenarios in chemical tank farms. **Reliability Engineering & System Safety**, 209, 2021. 107476.

PAOLI, A.; LAFORTUNE, S. **Safe diagnosability for fault-tolerant supervision of discrete event systems**. Automatica 41(8). [S.l.]: [s.n.]. 2005. p. 1335-1347.

PARK, B. et al. Risk Assessment Method Combining Independent Protection Layer (IPL) of Layer of Protection Analysis (LOPA) and RISKCURVES software: case study of hydriogen refueling ststions in urban areas. **Energies - Advances in Hydrogen Safety**, 14, n. 13, 2021.

RAUSAND, M. **Risk Assessment:** theory, methods, and applications. 1. ed. [S.l.]: John Wiley Professional, 2011.

REASON, J. **Managing the risks of organizational accidents**. Vermont. Ashgate. 1997.

ROUSH, M. **What Every ENgineer Should Know About Risk Analysis**. 1. ed. [S.l.]: Marcel Decker, 2000.

ROUVROYE, J. L.; VAN DEN BLIEK, E. G. Comparing safety analysis techniques. **Reliability Engineering and System Safety**, v. 75, n. 3, p. 289-294, 2002.

SALEH, J. H. et al. Highligths from the literature on accident causation and system safety: Review of major ideas, recent contributions, and challenges. **Reliability Engineering and System Safety**, Georgia, USA, 2010. 1105-1116.

SANTOS FILHO, D. J. **Aspectos do Projeto de Sistemas Produtivos**. Tese de Livre Docência - Escola Politécnica da Universidade de São Paulo. São Paulo. 2000.

SCHUYLER, J. **Risk and Decision Analysis in Projects**. 2. ed. [S.l.]: Project Management Institute, 2001.

SEVERINO, A. J. **Metodologia do Trabalho Científico**. 23. ed. São Paulo: Cortez Editora, 2007.

SILVA CARNEIRO, F. C. **Avaliação de riscos: Aplicação a um processo de construção**. Universidade de Aveiro. Aveiro, Portugal, p. 1-98. 2011.

SKLET, S. Safety Barriers: definition, classification and performance. **Journal of Loss Prevention in the Process Industries**, Norway, 2006. 494-506.

SOBRAL, J.; SOARES, G. Assessment of the adequacy of safety barriers to hazards. **Safety Science**, Berlim, 114, 2019. 40-48.

SOUZA, J. A. L. D. **Desenvolvimento De Sistemas De Controle Para Mitigação De Falhas Críticas Em Sistemas Produtivos**. Dissertação de Mestrado - Escola Politécnica da Universidade de São Paulo. São Paulo. 2014.

SOUZA, J.A.L et al. Safety active barriers considering different scenarios of faults in modern production systems. **Doctoral Conference on COmputing, Electrical and Industrial Systems**, n. Springer, p. 156-164, 2017.

SQUILLANTE JR. **Controle relacionado à segurança nas indústrias de processos: uma abordagem integrada de modelos de acidentes, defesa em profundidade e diagnosticabilidade segura**. Escola Politécnica da Universidade de São Paulo. São Paulo, p. 276. 2017.

SQUILLANTE JR, R. **Diagnóstico e Tratamento de Falhas Críticas em Sistemas Instrumentados de Segurança**. Dissertação de Mestrado - Escola Politécnica da Universidade de São Paulo. São Paulo. 2011.

SQUILLANTE, R. et al. A framework for synthesis of safety-related control design to avoid critical faults and pathogenic accidents in the process industries. **Safety Science**, Berlim, 2021. 24.

SUN, H. et al. Resilience-based approach to safety barrier performance assessment im proess facilities. **Journal of Loss Prevention in the Process Industries.**, 73, 2021. 104599.

SVENSON, O. The Accident Evolution and Barrier Function (AEB) Model Applied to Incicent Analysis in the Precessing Industries. **Risk Analysis**, v. 11, n. 3, p. 499-507, Setembro 1991.

TAKAYAMA, M. A. S. **Análise de Falhas aplicada ao planejamento estratégico da manutenção.** Universidade Federal de Juiz de Fora. Juiz de Fora, MG. 2008.

TSUNEMI, K. et al. Quantitative risk assessment of the interior of a hydrogen refueling station considering safety barrier systems. **Internationsl Journal of Hydrogen Energy**, 44, 2019. 23522-23531.

VILLEMEUR, A. **Reliability, Availability, Maintainability and Safety Assessment**. 1. ed. [S.l.]: John Wiley & Sons, v. 1 e 2, 1992.

WANG, X. et al. Fault Detection and Diagnosis Based on Time Petri Net. **Proceedings of 8th International COnference on Eletronic Measurement and Instruments**, Beijing, China, 2008.

YOE, C. E. **Principles of Risk Analysis**. [S.l.]: Taylor & Francis, v. 1, 2012.

YUAN, S. et al. Safety barriers in the chemical process industries: A state-of-the-art-review on their classification, assessment, and management. **Safety Science**, Berlim, 2022. 16.

ZHANG, Y.; JIANG, J. Bibliographical review on reconfigurable fault-tolerant control systems. **Annual Reviews in Control 32**, p. 229-252, 2008.

ZHU, C.; QI, M.; JIANG, J. Quantifying human error probability in independent protection layers for a batch reactor system using dynamic simulations. **Process Safety and Environment Protection**, 133, 2020. 243-258.

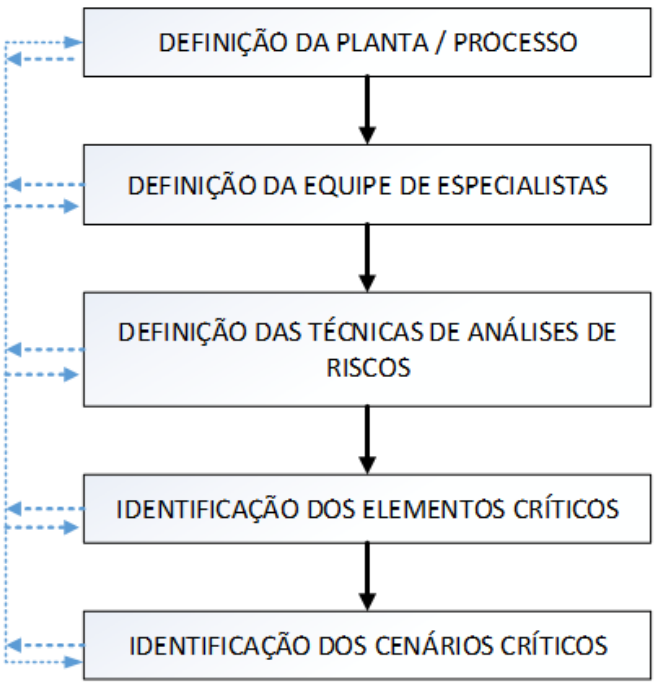
APÊNDICE A – CENÁRIOS CRÍTICOS E BARREIRAS DE SEGURANÇA REATIVAS DE UMA PLANTA / PROCESSO

Apêndice A1. Método para definição dos cenários críticos

Nesta etapa é definido o método para definição dos cenários críticos a partir da definição da planta / processo, documentação, equipe multidisciplinar de especialistas e as técnicas de análises de riscos recomendadas e obrigatórias, definidas nas normas de segurança vigentes, em função da severidade do efeito de ocorrência do evento topo e a atual fase do ciclo de vida da planta / processo.

A Figura 70 apresenta as etapas para a implementação do método. O detalhamento de cada etapa é feito nas seções subsequentes.

Figura 70 - Método para definição dos cenários críticos



Fonte: Próprio Autor

1. Definição da planta / processo

O primeiro passo para a definição dos cenários críticos consiste na definição da planta / processo que fará parte do objeto de controle, além da documentação necessária e suficiente para sua completa descrição, tanto do ponto de vista dos equipamentos / subsistemas que a compõe, além dos fluxos de processos, das malhas de controle e dos parâmetros das variáveis de processo envolvidas com as respectivas tolerâncias máximas e mínimas. O *checklist* da documentação necessária pode ser:

- ✓ Atual fase do ciclo de vida da planta / processo;
- ✓ Definição das funções primárias e secundárias de cada elemento / subsistema;
- ✓ Parâmetros nominais de operação, limites operacionais, manuais técnicos;
- ✓ Modos de falha associados;
- ✓ Históricos de falhas e consequências da ocorrência da falha;
- ✓ Fluxos de processo;
- ✓ Diagramas P&ID – *process and instrumentation diagram* (norma ISA S-5.1-1984, 2009);
- ✓ Malhas de controle;
- ✓ Valores nominais e intervalos permitidos para as variáveis de processo;
- ✓ Exemplos de instalações semelhantes;
- ✓ etc

A documentação deve ser suficiente para que a equipe multidisciplinar tenha subsídios para a tomada de decisões em relação às ações de controle de segurança para a prevenção e mitigação de falhas críticas.

2. Definição da equipe de especialistas

De posse da documentação da planta / processo e da documentação necessária e suficiente para a plena compreensão do objeto de controle, o próximo passo consiste na definição da equipe multidisciplinar que terá a função de aplicar um determinado conjunto de técnicas de análises de riscos para a análise qualitativa e quantitativa do risco inerente ao funcionamento da planta / processo.

Em função da complexidade das instalações, profissionais de diferentes áreas do conhecimento devem estabelecer a sinergia necessária para a melhor avaliação do risco da instalação, e propor medidas para a sucessiva redução do risco inerente e não aceitável, para uma operação de risco aceitável.

São exemplos de profissionais que compõe a equipe: engenheiros mecânicos, engenheiros mecatrônicos / elétricos, engenheiros de produção, líderes e operadores, brigadistas, engenheiros de segurança, representantes técnicos dos fabricantes dos equipamentos etc.

3. Definição das técnicas de análises de riscos

Realizadas as etapas anteriores, de posse da documentação necessária e da definição da equipe multidisciplinar especialista no processo, o próximo passo consiste na definição das técnicas de análises de riscos que servirão de ferramenta para a definição dos elementos críticos do processo, isto é, aqueles que, sob estado de falha, podem resultar em sérios danos à população, ao meio ambiente e às próprias instalações.

Considerando-se as normas relacionadas à segurança utilizadas neste trabalho, dependendo da atual fase do ciclo de vida da instalação, da severidade x frequência de ocorrência da falha e da matriz de tolerabilidade de riscos, algumas técnicas são obrigatórias e outras recomendadas para a análise de risco da planta / processo (N-2782, Petrobrás) (Tabela 3.1).

A IEC 61508 (IEC-61508, parte I) recomenda as técnicas *what-if, Hazop*, FMEA, Árvore de Falhas e Árvore de Eventos, dentre outras, para a determinação dos

elementos críticos. A N-2782 (NTP, Petrobrás) recomenda as técnicas de análises de riscos em função da atual fase do ciclo de vida da planta / processo.

Tal variedade de técnicas de análises de riscos é necessária pois nenhuma técnica, aplicada isoladamente, é capaz de avaliar completamente o risco de uma planta / processo (MODARRES, KAMINSKIY e KRIVTSOV, 2009).

4. Identificação dos elementos críticos

De posse das técnicas de análises de riscos mais apropriadas para aquele subsistema / componente, os especialistas em cada ramo de conhecimento apresentam, após a aplicação das técnicas de análises de riscos recomendadas, uma lista dos componentes críticos e a equipe, de forma multidisciplinar, irá avaliar e definir quais os componentes críticos da instalação.

Após a definição dos elementos críticos, o próximo passo consiste na possibilidade de instrumentação para a detecção de ocorrência de falha, seja no próprio componente / subsistema, ou por meio de desvios de variáveis de processo.

De maneira geral, o estudo *Hazop* (IEC 61882, 2003) têm se mostrado bastante eficiente para a definição dos desvios de variáveis de processo, e propor as medidas de prevenção de ocorrência da falha e, caso sejam ineficazes, as respectivas medidas para a mitigação de seus efeitos.

5. Identificação dos cenários críticos

Identificados os elementos críticos da planta / processo, o próximo passo consiste na determinação de cenários de ocorrência da falha crítica, ou seja, quais os possíveis eventos inicializadores que podem ter relação de causa-efeito com a ocorrência do evento topo. Em outras palavras, falhas ocorridas em componentes / subsistemas que aparentemente não representem risco elevado, mas que, em estado de falha, podem resultar na ocorrência na falha daquele componente crítico.

Após a identificação dos elementos críticos, a norma HSE – *Health and Safety Executive* (HSE, 2006a) recomenda as técnicas *What-If, Hazop* e FMEA para a

identificação dos cenários críticos. Já para os cenários de risco elevado com alta complexidade, há o destaque para os diagramas de *bow-tie.*

Já a norma N-2782 (NTP, Petrobrás) recomenda as técnicas FTA (árvore de Falhas) e ETA (árvore de eventos) para a seleção de cenários com estimativa de frequência. A união dos resultados das técnicas de árvore de falhas e árvore de eventos compõe justamente a estrutura de um diagrama *bow-tie*.

De posse dos elementos críticos e das técnicas recomendadas, a equipe multidisciplinar, com base no conhecimento do processo, irá definir os caminhos críticos que antecedem a falha crítica (árvore de falhas) e os possíveis cenários após a sua ocorrência (árvore de eventos).

Uma outra possibilidade de obtenção dos cenários críticos é por meio de algoritmos de aprendizagem Bayesiana.

Apêndice A2. Método para definição das barreiras de segurança

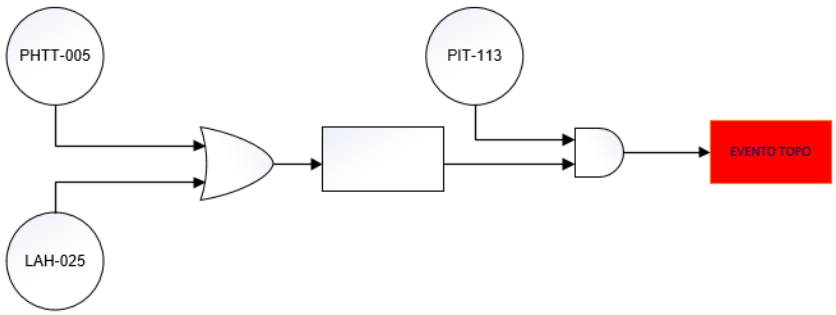
Nesta etapa é definida a nomenclatura das barreiras de segurança de prevenção e mitigação para cada evento topo e a inserção das barreiras para as estruturas de árvores de falhas e árvores de eventos.

É proposto um método para a elaboração do estudo *Hazop* (IEC: 61882, 2003) para a definição das funções instrumentadas de segurança de prevenção e mitigação.

1. Inserção das barreiras de segurança de prevenção e mitigação

Considere, como exemplo, a Árvore de Falhas da Figura 71.

Figura 71 - Exemplo de estrutura de árvore de falhas



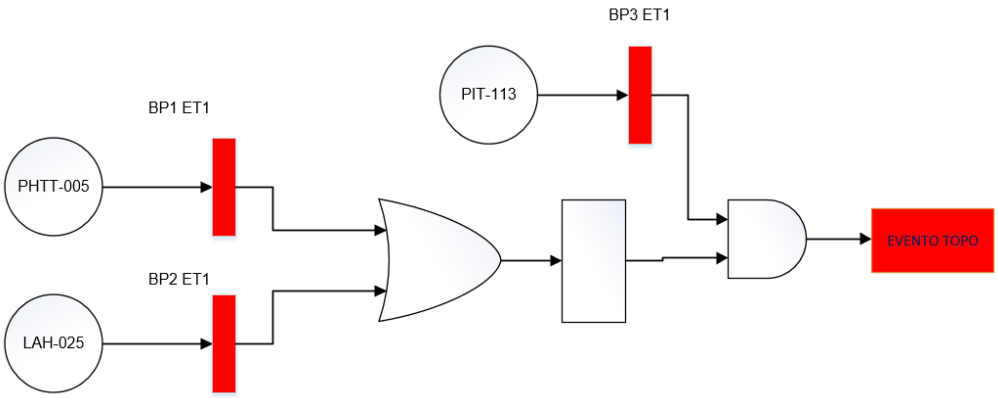
Fonte: Próprio Autor

Partindo-se dos respectivos eventos inicializadores, para que o evento topo não ocorra, as respectivas barreiras de segurança devem ser alocadas para que as equações das combinações lógicas não sejam satisfeitas. O presente trabalho propõe a seguinte nomenclatura para as barreiras:

- BPx ETy : Barreira de prevenção “x” do evento topo y ;
- BMx ETy: Barreira de mitigação “x” do evento topo y.

Para a estrutura de árvore de falhas da Figura 71, o conjunto de barreiras de prevenção para o evento topo, considerando evento topo 1 ou ET1, é representado na Figura 72.

Figura 72 - Conjunto de barreiras de prevenção para o evento topo



Fonte: Próprio Autor

Nota-se, a partir da estrutura da árvore de falhas, que há dois sequenciamentos ou caminhos críticos até a ocorrência do evento topo.

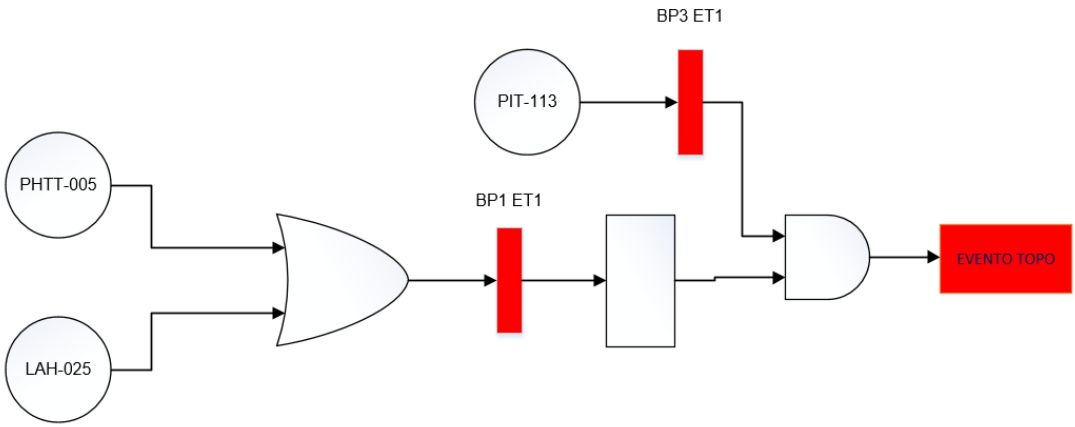
Para a ocorrência da falha identificada como “PIT-113”, podemos ter as seguintes situações:

i) A barreira de prevenção “BP1 ET1” possui evento inicializador “PHTT-005”, e possui uma função de segurança de prevenção **distinta** da “BP2 ET1”, com respectivo evento inicializador “LAH-025”. Para tal caso, tem-se a representação do conjunto de barreiras da Figura 72[15].

[15] A representação da barreira de segurança não desconfigura a lógica da árvore de falhas. Representa uma barreira de prevenção (ou mitigação), implementada por meio do conceito de SIS para a prevenção / mitigação do evento topo ou falha crítica.

ii) A barreira de prevenção “BP1 ET1” possui evento inicializador “PHTT-005”, e possui **mesma** função de segurança de prevenção da “BP2 ET1”, com respectivo evento inicializador “LAH-025”. Para tais casos, uma das barreiras é suprimida, e dependerá de critérios de cotação e lógica “ou” de seus eventos inicializadores. O conjunto de barreiras é representado na Figura 73.

Figura 73 - Representação de barreiras de mesmas atividades de prevenção



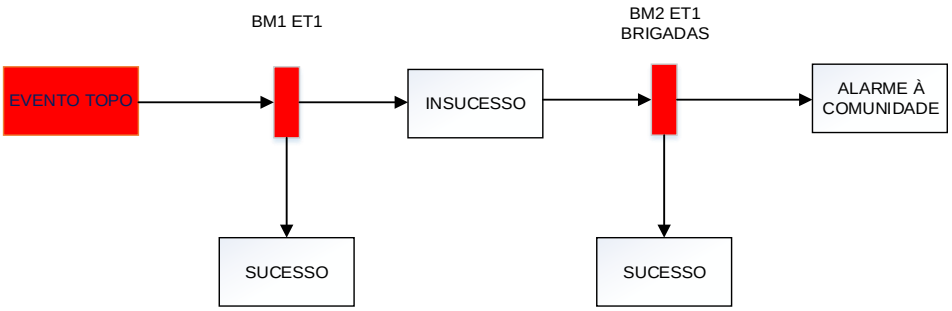
Fonte: Próprio Autor

Para a inserção das barreiras de segurança de mitigação, considera-se que a estrutura da árvore de eventos proposta no trabalho compreende dois níveis de barreiras de mitigação, uma barreira composta por funções instrumentadas de mitigação e, no caso de insucesso, a interação com barreiras não técnicas, representadas pelas equipes de brigadas.

Para um evento topo, a estrutura de árvore de eventos, com as respectivas barreiras de mitigação[16], é representada na Figura 74.

[16] O trabalho considerou que após a ocorrência da falha crítica, todas as SIFs de prevençãoe mitigação, associadas a um dado evento topo. Ao insucesso das barreiras de segurança instrumentadas, são implementadas as respectivas barreiras das brigadas.

Figura 74 - Estrutura de árvore de eventos após a ocorrência do evento topo



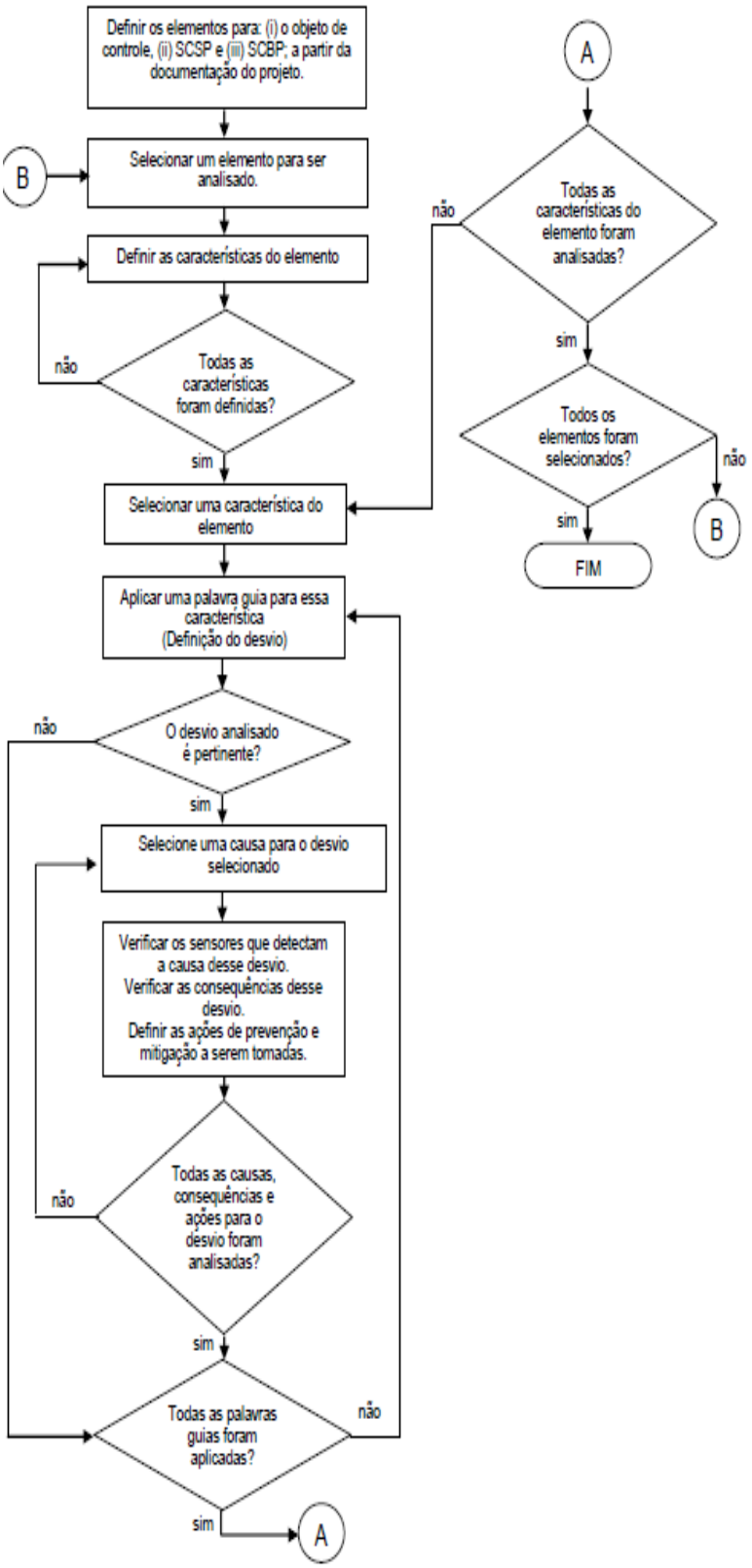
Fonte: Próprio Autor

Para casos em que a estrutura da árvore de eventos contemple um número maior de barreiras técnicas de mitigação com as respectivas SIFs de mitigação, o método continua válido, e a inserção / nomenclatura das barreiras segue conforme exemplo das estruturas das árvores de falhas.

2. Estudo Hazop para as SIFs

Definidas as barreiras de prevenção para cada estrutura de árvore de falhas e árvore de eventos, o próximo passo consiste na aplicação do estudo *Hazop* (IEC 61882, 2003) para a definição das SIFs de prevenção e mitigação de falhas críticas. O algoritmo para preenchimento da tabela *Hazop* é apresentado na Figura 75. A Tabela 11 representa o modelo para o preenchimento dos resultados para cada barreira.

Figura 75 - Algoritmo para preenchimento da tabela *HAZOP*.



Fonte: Adaptado de (CAVALHEIRO, 2013)

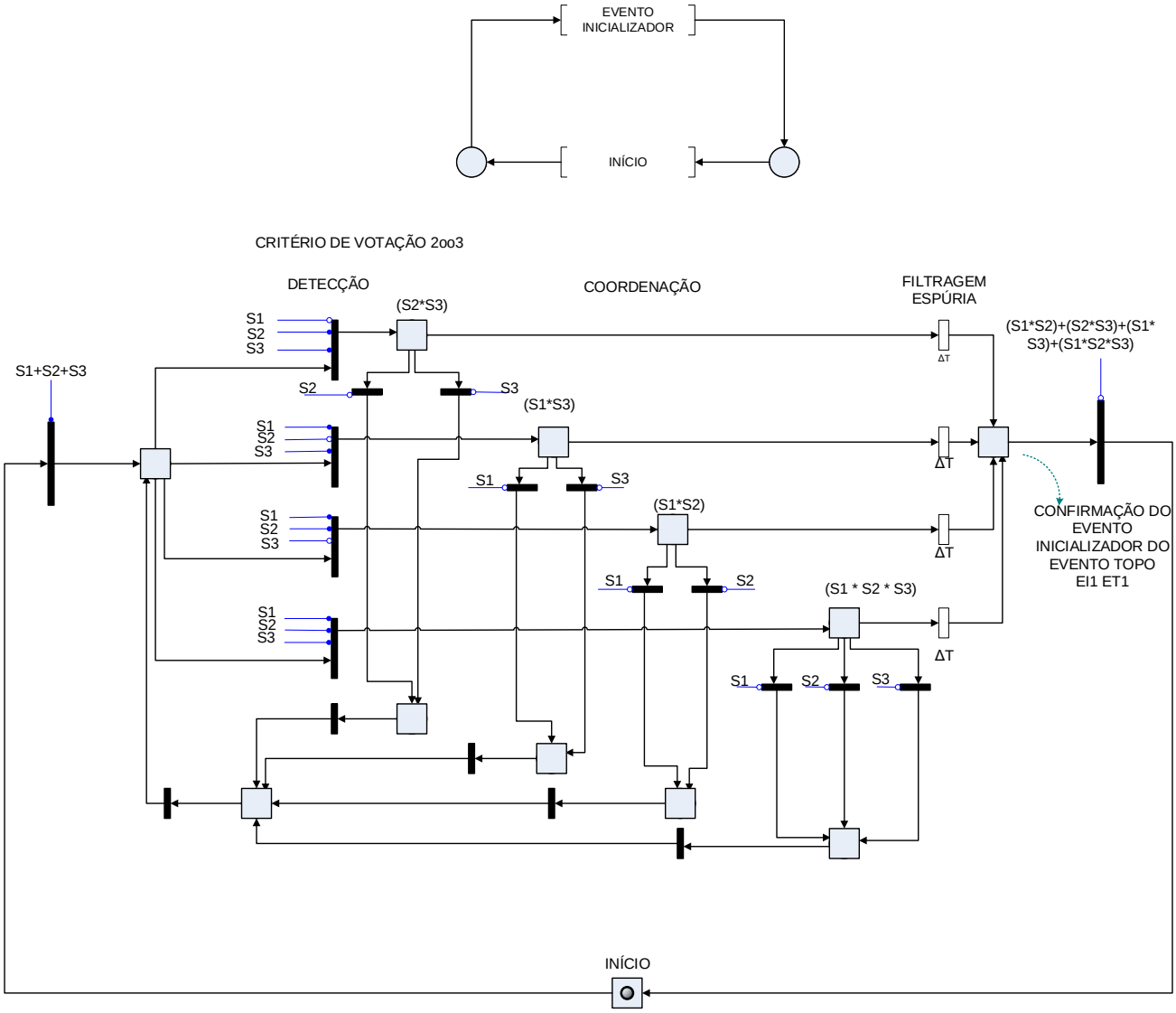
Tabela 11 - Tabela típica para a elaboração do *HAZOP*

Título **Número do Documento** **Responsáveis pelo estudo** **Sistema / parte do sistema**				**Número da revisão**			**Número da folha** **Data da reunião**	
Barreira	**Elemento**	**Evento crítico / desvio**	**Possíveis causas**	**Consequências**	**Ação**	**Equipamento**	**Sensores**	**Atuadores**
BP 1 ET1								
BP2 ET1								

Fonte Adaptado da (IEC 61882, 2001):

APÊNDICE B – Modelo E-MFG de detecção, coordenação e filtragem espúria de eventos inicializadores

Figura 76 – Modelo E-MFG para detecção, filtragem e confirmação da ocorrência de falha, com critério de votação 2oo3.



ANEXO A –FERRAMENTAS DE MODELAGEM

Como suporte às ferramentas de modelagem de SED utilizadas no trabalho, são apresentados os anexos subsequentes.

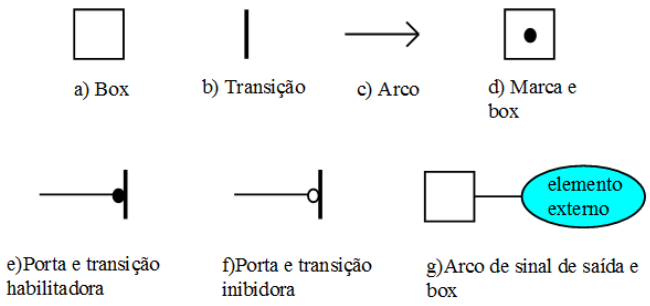
Anexo A.1 Mark Flow Graph – MFG

Conforme (MIYAGI, 1996), o MFG é um grafo bipartido que representa as características fundamentais necessárias para a representação de sistemas sequenciais complexos. O MFG é derivado das redes de Petri do tipo condição/evento e, desta forma, pressupõe que para ocorrer um determinado evento seja necessária a obediência de determinadas condições, estabelecendo-se a relação causal existente entre condição e evento para a evolução dinâmica do sistema. Por sua vez, no modelo MFG equivalente de um sistema, as transições correspondem aos eventos e os ‘boxes’ correspondem às condições e, portanto, o grafo é composto a partir da conexão de transições e’ boxes’ alternadamente, através de arcos orientados. O MFG é composto pelos seguintes elementos estruturais:

- Box: o Box corresponde a uma condição, sendo equivalente ao lugar de uma RdP C/E.
- Transição: a transição corresponde a um evento que causa uma mudança de estado do sistema.
- Arco orientado: a relação entre um ‘box’ e uma transição é representado por um arco orientado que conecta estes dois elementos.
- Marca: a manutenção de uma condição é representada pela existência de uma marca no ‘box’ correspondente.
- Porta habilitadora: desempenha a função de habilitar a ocorrência dos eventos correspondentes às transições a que estão conectadas.
- Porta inibidora: desempenha a função de inibir a ocorrência dos eventos correspondentes às transições a que estão conectadas.
- Arco de sinal de saída: corresponde a um arco que se origina de um ‘box’ e envia a informação deste ‘box’ para um elemento externo.

A representação gráfica dos elementos do MFG pode ser observada na Figura 77.

Figura 77 - Representação gráfica dos elementos MFG.



Fonte: Adaptado de (MIYAGI, 1996).

O Arco de sinal de saída é o único elemento do MFG que não foi representado em redes de Petri é sua importância se dá no fato de ser capaz de representar o mapeamento de um elemento externo no modelo. Tal poder de representação garante ao MFG a propriedade matemática de ser um modelo interpretado.

Conforme (MIYAGI, 1996), o estado de um sistema pode ser representado pelo arranjo das marcas no grafo MFG e, dessa forma, o comportamento dinâmico do sistema é representado pela alteração dos estados causada pela ocorrência de eventos, esses que correspondem às transições. Uma transição no MFG está habilitada para o disparo se:

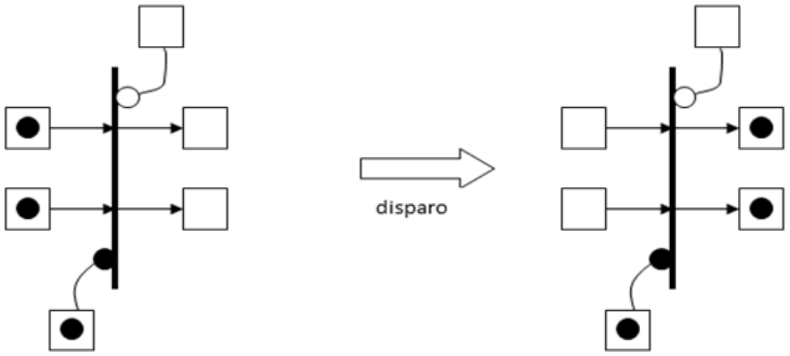
- Não existe ‘box’ do lado de saída com marcas.
- Não existe ‘box’ do lado de entrada sem marcas.
- Não existe arco habilitador interno desativado.
- Não existe arco inibidor interno ativado.

Uma transição habilitada pode ser disparada se:

- Não existe arco habilitador externo desativado.
- Não existe arco inibidor externo ativado.

A Figura 78 a seguir ilustra-se o disparo de uma transição.

Figura 78 - Disparo de uma transição no MFG.



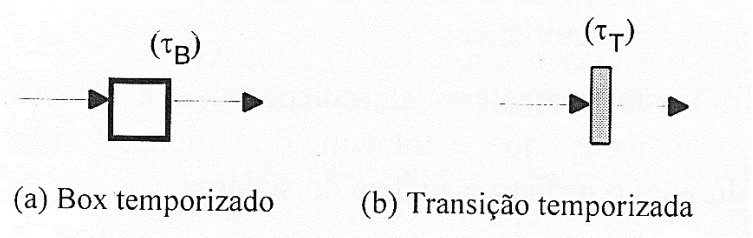
Fonte: Adaptado de (MIYAGI, 1996)

Em sistemas reais o tempo é um elemento importante e não pode ser omitido. Dessa forma os seguintes elementos devem ser introduzidos:

- 'Box' temporizado é usado para representar o tempo de duração de processos e retém a marca durante um intervalo de tempo pré-definido (τ_B)
- A transição temporizada atrasa o seu disparo de um intervalo de tempo pré-definido (τ_T), medido a partir do instante em que está se torna habilitada e pode ser disparada.

Na Figura 79 podem ser visualizadas as representações gráficas do 'box' e da transição temporizada.

Figura 79 - Elementos temporizados.



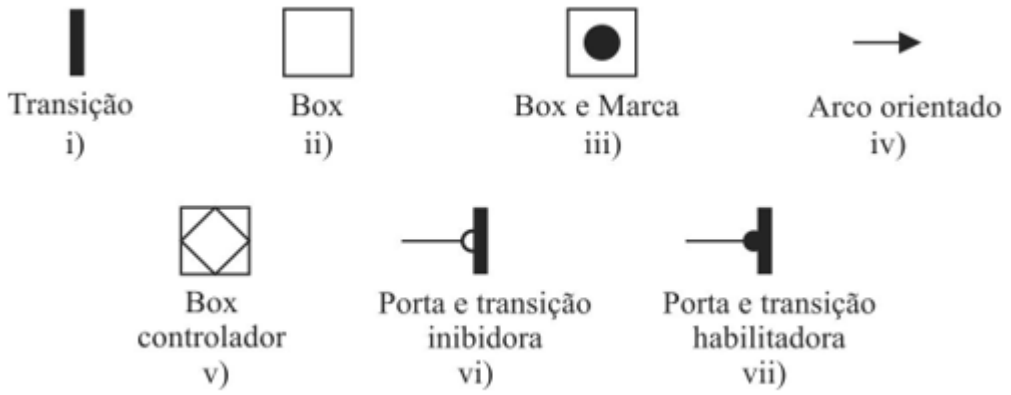
Fonte: Adaptado de (MIYAGI, 1996)

Anexo A.2 Enhanced Mark Flow Graph – E-MFG

A ferramenta de modelagem E-MFG inclui as marcas individuais e os elementos estruturais do MFG, e permite a manipulação de marcas com atributos sem, no entanto, fugir do modelo de rede elementar convencional. Possui capacidade de modelar e controlar as alterações de informações das marcas e seleção das tarefas associadas aos boxes (SANTOS FILHO, 2000).

O E-MFG é composto basicamente dos elementos estruturais do MFG, conforme apresentado na Figura 80:

Figura 80 – Elementos básicos do E-MFG

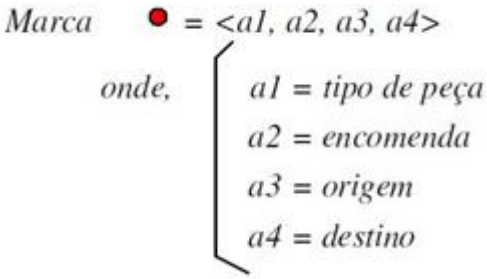


Fonte: (MIYAGI, 1996)

Os elementos estruturais básicos constituem um caso particular em que não há marcas individuais e não há regras adicionais associadas às transições. No E-MFG as marcas individuais são acompanhadas de um vetor de atributos (garante a individualidade da marca) e que pode estar associada a diversas informações referentes ao produto, processo e ao controle (NAKAMOTO, 2008).

A Figura 81 ilustra um exemplo atributos de marcas.

Figura 81 – Exemplo de atributos de marca



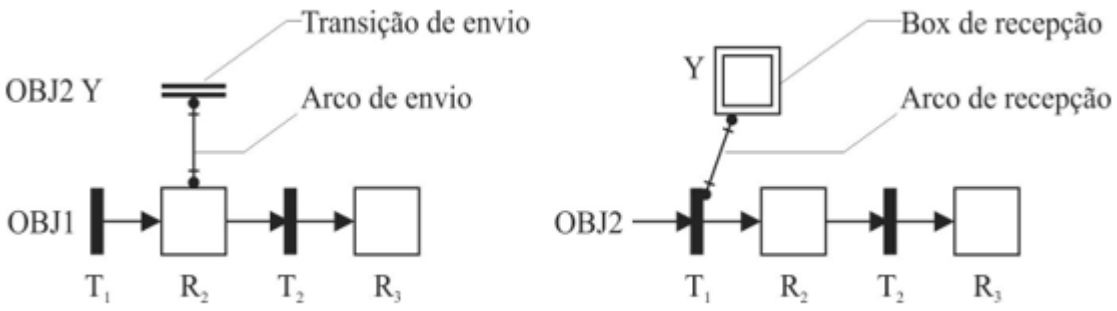
Fonte: (NAKAMOTO, 2008)

A incorporação de elementos comunicadores na técnica de modelagem E-MFG ocorreu devido a necessidade de uma modelagem que viabilizasse a colaboração entre os sistemas (MATSUSAKI, 2004). Com isso, a modelagem E-MFG com comunicadores, além de incluir os elementos da interface de transmissão e da interface de recepção, mantém a individualidade das marcas nos elementos estruturais do E-MFG (SANTOS FILHO, 2000).

A interface de transmissão envia eventuais mensagens assíncronas quando o box a ela conectada estiver marcado. A interface de recepção de mensagem recebe a mensagem e dependendo da informação recebida, realiza a ativação ou desativação da transição (MATSUSAKI, 2004).

A Figura 82 ilustra as interfaces de transmissão e recepção dos elementos comunicadores.

Figura 82 - E-MFG com as interfaces de transmissão e recepção.



Fonte: (MATSUSAKI, 2004)

Anexo A.3 Production Flow Schema - PFS

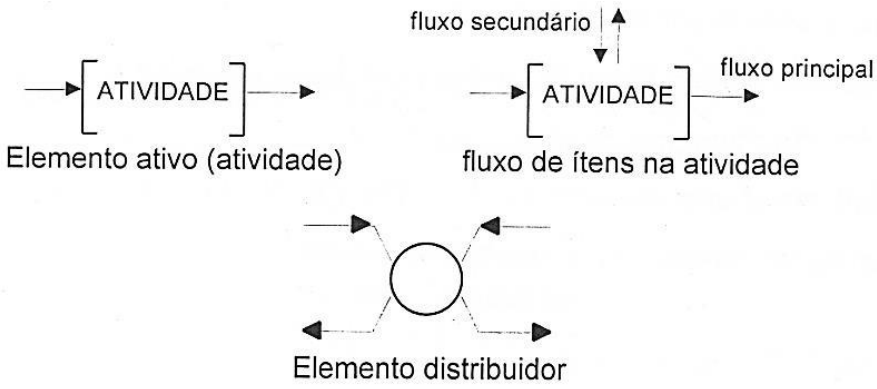
Conforme (MIYAGI, 1996), o objetivo do PFS é sistematizar e facilitar a modelagem de sistemas utilizando redes considerando-se que existem eventos de um SED que podem estar organizados de forma hierárquica. Ou seja, um evento pode conter um arranjo de eventos e estados organizados hierarquicamente. Dessa forma, em vez de representarmos o desenvolvimento em um único passo, propõe-se representar o desenvolvimento de forma hierárquica utilizando uma abordagem *top-down.*

A metodologia propõe que qualquer processo produtivo pode ser decomposto em três elementos básicos:

- Os elementos-atividade têm como função representar uma atividade que pode ser interpretada como uma ação ou conjunto de ações que causam uma transformação no estado do elemento que está sendo processado.
- O elemento-distribuidor existe para representar as situações em que nenhuma atividade está sendo executada sobre um determinado elemento, estando, portanto em um estado de espera.
- Arcos representam as relações entre os elementos anteriores e a direção do fluxo do processo. Arcos conectados à parte interna da atividade representam um fluxo secundário.

A representação gráfica dos elementos do PFS é realizada conforme a Figura 83.

Figura 83 – Elementos estruturais do PFS.



Fonte: (MIYAGI, 1996)

Anexo A.4 Metodologia PFS/MFG

A metodologia consiste em descrever inicialmente modelos PFS de mais alto nível que vão sendo refinados até que a representação de todas as atividades que se deseja modelar seja obtida. Em seguida, quando se deseja modelar a execução das atividades, representa-se os elementos PFS em MFG. De acordo com (MIYAGI, 1996), o procedimento envolve cinco passos:

i. Definição e representação dos principais processos por modelos PFS.
ii. Detalhamento dos processos em atividades ou funcionalidades desejadas do sistema em modelagem.
iii. Detalhamento das atividades ou funcionalidades em operações, com a introdução de elementos MFG.
iv. Introdução dos elementos de controle de recursos explicitando os compartilhamentos.
v. Representação dos sinais de controle, sejam esses de detecção ou atuação, com a planta. Ou seja, representa-se a relação do controle do processo modelado com os entes físicos.

Anexo B: Diagramas de instrumentação parciais

Figura 84 – Linha de sucção

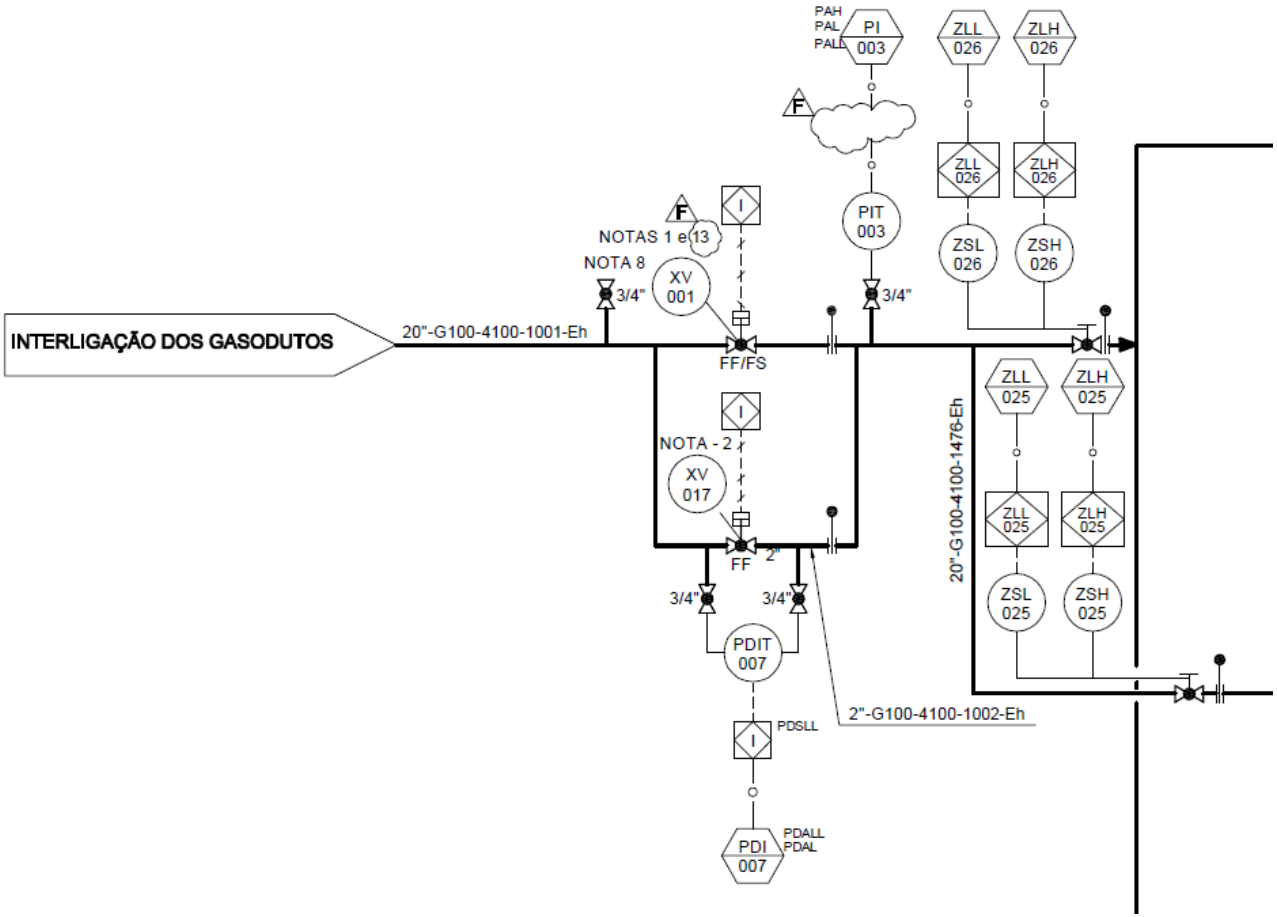


Figura 85 – Filtros coalescedores

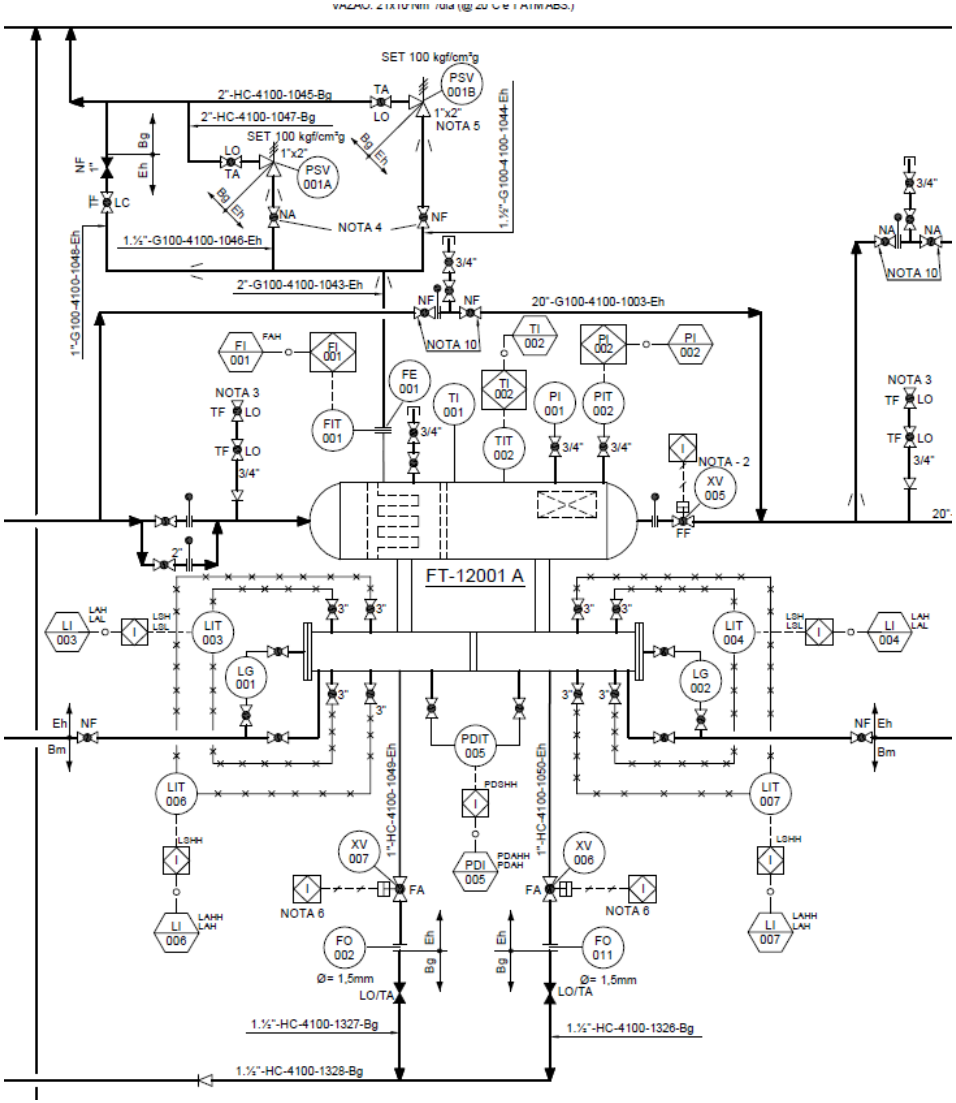


Figura 86 – Unidades compressoras

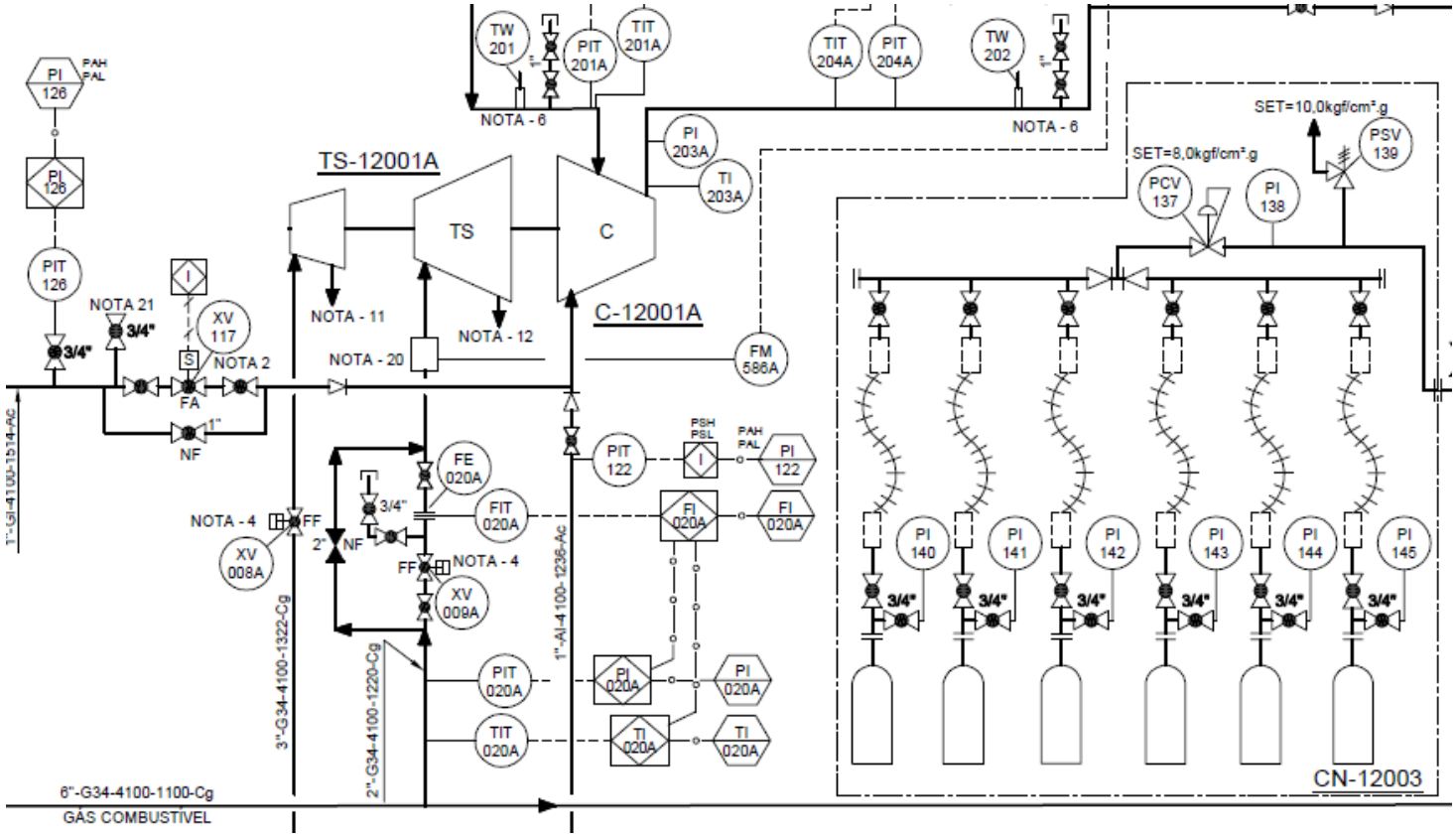


Figura 87 – Unidades resfriadoras

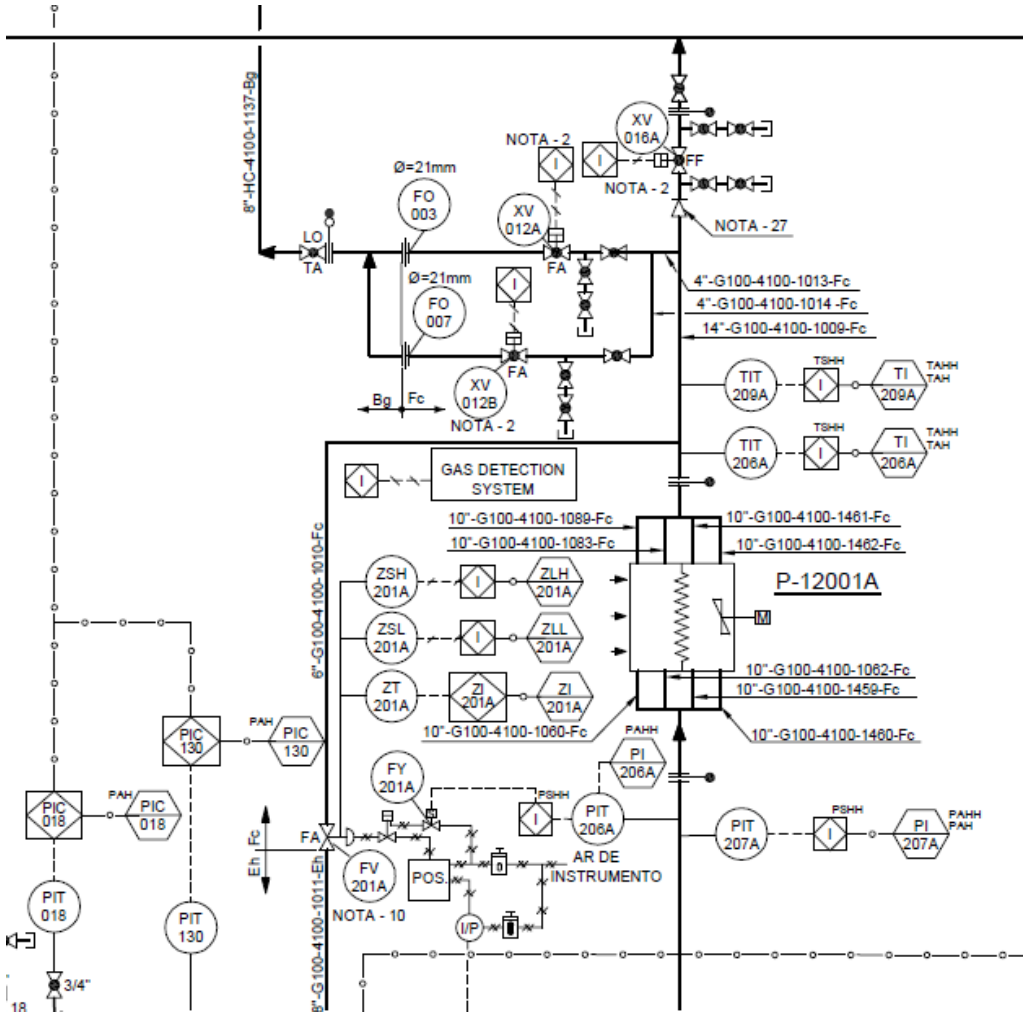


Figura 88 – Filtragem para instalações

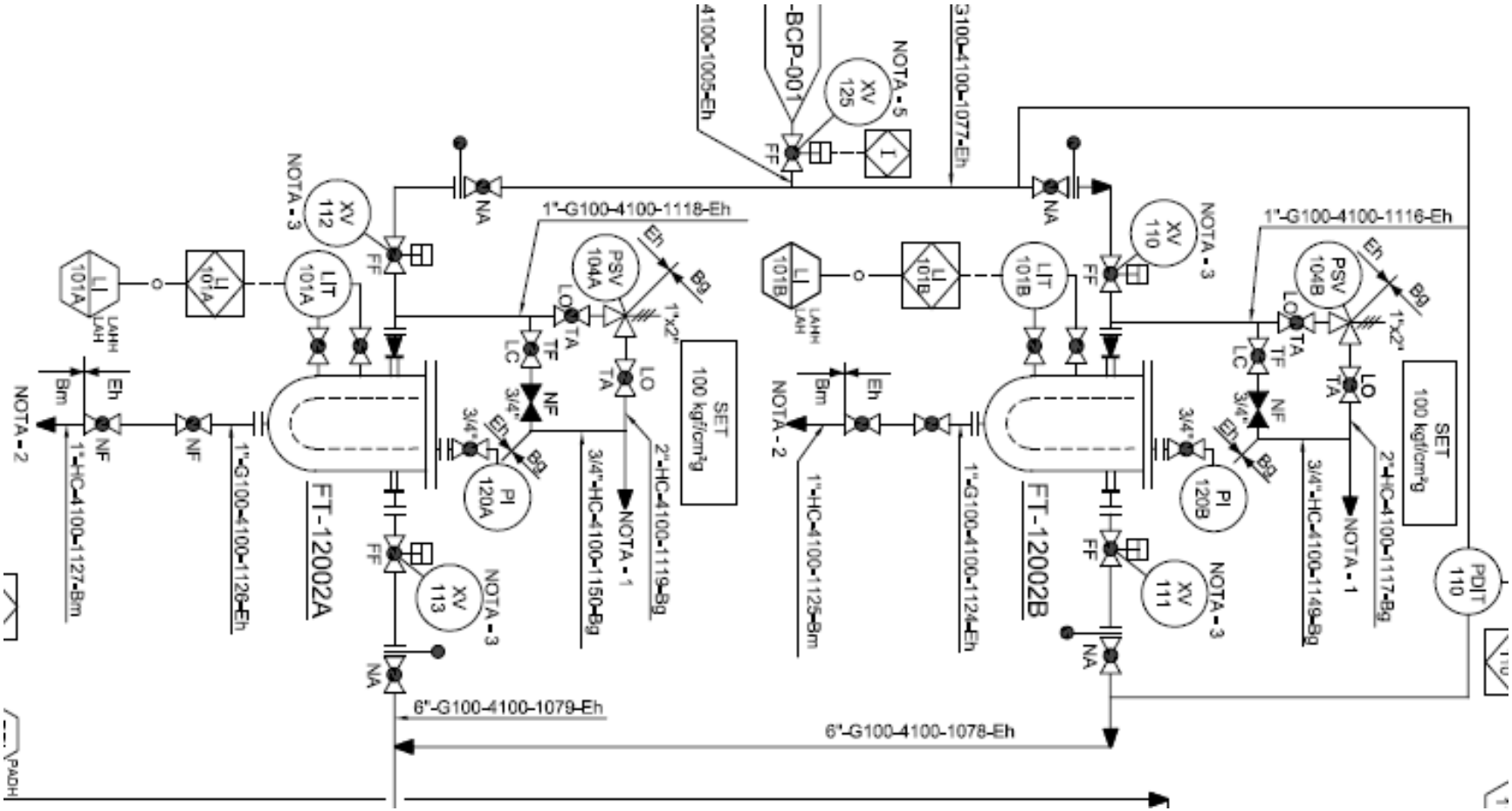


Figura 89 – Trocadores de calor