REINALDO SQUILLANTE JÚNIOR

Controle relacionado à segurança nas indústrias de processos: uma abordagem integrada de modelos de acidentes, defesa em profundidade e diagnosticabilidade segura

São Paulo
2017

REINALDO SQUILLANTE JÚNIOR

Controle relacionado à segurança nas indústrias de processos: uma abordagem integrada de modelos de acidentes, defesa em profundidade e diagnosticabilidade segura

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

São Paulo
2017

REINALDO SQUILLANTE JÚNIOR

Controle relacionado à segurança nas indústrias de processos: uma abordagem integrada de modelos de acidentes, defesa em profundidade e diagnosticabilidade segura

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

2017

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

São Paulo, 19 de Julho de 2017.

Assinatura do autor: _____

Assinatura do orientador: _____

Catalogação-na-publicação

Squillante Júnior, Reinaldo
Controle relacionado à segurança nas indústrias de processos: uma abordagem integrada de modelos de acidentes, defesa em profundidade e diagnosticabilidade segura / R. Squillante Júnior -- versão corr. -- São Paulo, 2017.
277p.

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

1.Indústrias de Processos 2.Controle relacionado à segurança funcional 3.Modelo de acidente 4.Defesa em profundidade 5.Diagnosticabilidade segura I.Universidade de São Paulo. Escola Politécnica. Departamento de Engenharia Mecatrônica e de Sistemas Mecânicos II.t.

DEDICATÓRIA

Aos meus pais Reinaldo (i.m) e Eva.

À minha esposa Sandra

Ao meu filho Stefano

AGRADECIMENTOS

Agradeço primeiramente a Deus pela graça da vida, pela saúde física, mental e espiritual e pela sabedoria que me foi dada. Diante das dificuldades que me apareceram durante o desenvolvimento deste trabalho, sempre orei a Deus clamando por auxilio e sabedoria, crendo que Ele esteve e está sempre ao meu lado. Foi Ele que me colocou neste grupo de pesquisa, foi Ele também que me fez conhecer pessoas tão importantes que me orientaram e me auxiliaram de forma direta ou indireta, no desenvolvimento deste trabalho. Muito obrigado meu Deus.

À minha esposa e companheira Sandra, com amor, admiração e gratidão por sua compreensão, me incentivando e apoiando desde o Mestrado, permitindo que eu prosseguisse com o Doutorado. Pela paciência em suportar a minha ausência em vários momentos ao longo destes anos, cabendo a ela, a responsabilidade no cuidado do nosso filho Stefano, o maior presente de Deus.

Ao meu orientador Prof. Dr. Diolino José dos Santos Filho, pela constante orientação, pela confiança depositada em meu trabalho e em minha pessoa, pelo apoio incondicional, por inúmeras e valiosas contribuições e pelo direcionamento e acompanhamento deste trabalho. Não poderia deixar de registrar também, meu profundo agradecimento pela amizade criada. Sempre me apoiou e me ajudou nos momentos mais difíceis da minha vida. O Prof. Dr. Diolino contribuiu não só para minha formação acadêmica como pesquisador, mas também para a minha vida pessoal e espiritual.

Ao Prof. Dr. Paulo Eigi Miyagi pela valiosas contribuições, auxílios e pela confiança depositada em mim, desde quando iniciei o meu Mestrado no ano de 2009. O Prof. Dr. Paulo foi um dos membros que participou da minha banca de arguição do Mestrado, tendo permitido que eu ingressasse na Escola Politécnica da USP, uma instituição de ensino e pesquisa de excelência, no Departamento de Engenharia Mecatrônica e de Sistemas Mecânicos.

Ao Prof. Dr. Fabrício Junqueira, por sua amizade, incentivos, apoio e contribuições acadêmicas desde o meu Mestrado.

Ao Prof. Dr. Newton Maruyama e ao Prof. Dr. Lucas Antonio Moscato pelas valiosas contribuições nas publicações de artigos científicos.

Ao Prof. Dr. Luis Alberto Martinez Riascos pelas valiosas contribuições na publicação de artigos, no exame de qualificação e na defesa do no meu Mestrado. Também pelas valiosas sugestões no exame de qualificação do Doutorado.

Aos eternos amigos do Laboratório de Sistemas de Automação (LSA) pelas sugestões e contribuições, em especial ao Marcosiris Pessoa, Caio Fattori, José Isidro Garcia, Osvaldo Asato, André Cavalheiro, Jeferson Afonso Lopes de Souza, Rodrigo Ferrarezi, Robson Marinho, Edson Watanabe, Mauricio Blos, Edinei Legaspe, entre outros pelo apoio e pela amizade.

A Escola Politécnica da USP, em especial ao Departamento de Engenharia Mecatrônica e de Sistemas Mecânicos, que institucionalmente viabilizaram este trabalho.

A todos os professores e funcionários do Departamento de Engenharia Mecatrônica e de Sistemas Mecânicos que foram responsáveis por me fornecerem suporte acadêmico.

As secretárias Regianne e Marisa do PPGEM pelo apoio administrativo e acadêmico.

Finalizo agradecendo à FAPESP e ao CNPq pelo apoio financeiro.

“Porque o Senhor dá a sabedoria,
e da Sua boca vem a inteligência
e o entendimento”
(Provérbios 2:6).

RESUMO

A questão da segurança funcional das indústrias de processos vem recebendo uma atenção crescente pela comunidade científica mundial, uma vez que se observa a possibilidade de ocorrências de acidentes e as consequências indesejadas que estes acidentes têm provocado. Essas indústrias podem ser consideradas como parte de uma classe de sistemas denominados Sistemas Críticos, que são caracterizados pela possibilidade de ocorrência de falhas críticas, que resultam em acidentes com perdas de vidas humanas, danos ao meio ambiente e perdas financeiras envolvendo custos significativos de equipamentos e propriedades.

Estes fatos justificam a necessidade de uma nova abordagem no que se refere ao *design* de processos, *design* de controle de processos, análise e controle de riscos e avaliação de riscos. Um dos desafios pertinentes à segurança funcional está associado a como vincular os cenários de acidentes aos requisitos para projetos de sistemas de controle relacionados à segurança das indústrias de processos de forma sistemática. Por sua vez, a possibilidade de ocorrência de eventos críticos e/ou eventos indesejados não observados ou ocultos, como fatores relevantes associados à evolução da sequência de eventos que culmina na ocorrência de um acidente. Neste contexto, o desafio está em aprimorar a eficácia destes sistemas de controle, que envolve o desenvolvimento de uma solução capaz de supervisionar o processo de evolução de falhas críticas, a fim de se garantir um nível de segurança funcional adequado e que esteja em conformidade com as normas internacionais aplicáveis IEC 61508 e IEC 61511. Portanto, estas considerações trazem novos requisitos para o projeto de sistemas de controle desta natureza, capaz de englobar modelos de acidentes e processos de evolução de falhas críticas.

Uma solução é a consideração das abordagens de prevenção e mitigação de falhas críticas de forma integrada e interativa. Além disso é necessário abordar novas técnicas e conceitos para que se possa desenvolver um sistema de controle capaz de rastrear e atuar nos processos de evolução de falhas desta natureza. Uma possibilidade consiste em considerar o princípio de defesa em profundidade aliado à propriedade de diagnosticabilidade segura. O atendimento a este novo conjunto de requisitos não é trivial e se faz necessário integrar diferentes formalismos para o desenvolvimento de soluções adequadas. Portanto, este trabalho apresenta uma

metodologia para o projeto de um sistema de controle baseado no conceito de segurança funcional para indústrias de processos, e que propõe: (i) uma arquitetura de controle para prevenção e mitigação de falhas críticas, (ii) extensão da classificação de barreiras de segurança focando na automação via sistemas instrumentados de segurança (SIS) (iii) *framework* para a síntese de sistemas de controle relacionados à segurança baseado em modelos de acidentes e que contempla os seguintes métodos: (a) elaboração do HAZOP, (b) construção de modelos de acidentes, (c) integração dos modelos de acidentes com o HAZOP e (d) geração dos algoritmos de defesa para a prevenção e mitigação de falhas críticas, a partir de técnicas de modelagem usando extensões da rede de Petri: *Production Flow Schema* (PFS) e *Mark Flow Graph* (MFG). A metodologia proposta foi verificada, a partir de exemplos de aplicação investigados na literatura.

Palavras-chave: Indústrias de Processos. Controle relacionado à segurança funcional. Defesa em profundidade. Diagnosticabilidade Segura. Modelo de acidente.

ABSTRACT

The issue of the functional safety of process industries has been receiving increasing attention from the world scientific community, since it has stated the possibility of occurrences of the accidents and the related undesired consequences. These industries can be considered as part of a system class called critical systems, which are characterized by the occurrence of critical faults, which can result in accidents involving loss of life, damage to the environment, and financial losses involving equipment and property.

These facts justify the need for a new approach that addresses: process design, process control design, risk analysis and control, and risk assessment. One of the challenges related to functional safety is associated with how to integrate accident scenarios to the requirements for the design of safety-related control systems of the process industries in a systematic way. Furthermore, there is the possibility of the occurrence of the unobserved or hidden undesired and / or critical events, as relevant factors associated to the evolution of the sequence of the events that corroborates in the occurrence of an accident. In this context, the challenge is to improve the effectiveness of these control systems, which involves the development of a solution capable of supervising the process of evolution of the critical and / or undesired events, in order to guarantee an adequate level of functional safety, and that complies with the applicable international standards IEC 61508 and IEC 61511. Therefore, these considerations bring new requirements for the design of control systems of this nature, capable of encompassing the accident models and the critical fault evolution processes. One solution is to consider critical fault prevention and mitigation approaches in an integrated and interactive way. In addition, it is necessary to addresses new techniques and concepts in order to develop a control system capable of tracking and acting in the evolution processes of faults of this nature. One possibility is to consider the principle of defense-in-depth coupled with the property of safe diagnosability. The fulfillment of this new set of requirements is not trivial and it is necessary to integrate different formalisms for the development of adequate solutions. Therefore, this work presents a methodology for the design of a safety-related control systems based on the concept of functional safety for the process industries, which proposes: (i) a control architecture for the prevention and

mitigation of the critical faults, (ii) an extension of the classification of the safety barriers focusing on automation via safety instrumented system (SIS), (iii) a framework for the synthesis of the safety-related control systems based on accident models and which includes the following methods: (a) elaboration of the HAZOP study, (b) construction of the accident models, (c) integration of the accident models with the HAZOP study, and (d) generation of the defense algorithms for the prevention and mitigation of the critical faults, via modeling techniques using extensions of the Petri net: Production Flow Schema (PFS) and Mark Flow Graph (MFG). The proposed methodology was verified, from application examples investigated in the literature.

Keywords: Process Industries. Functional safety-related control. Defense-in-depth. Safe diagnosability. Accident model.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

AF	Árvore de Falhas
AE	Árvore de Eventos
BDT	Banco de Dados de Treinamento
BDT_{AF}	Banco de Dados de Treinamento da Árvore de Falhas
BDT_{AE}	Banco de Dados de Treinamento da Árvore de Eventos
BM	Barreira de Mitigação
BP	Barreira de Prevenção
EC	Evento Crítico
EEP	Equipamento Eletrônico Programável
IE	Evento Iniciador
EM	*Expectation Maximization*
ET	Evento Topo
GAO	Grafo Acíclico Orientado
HAZOP	*Hazard and Operability Study*
HC	Hidrocarboneto
IEC	*International Electrotechnical Commission*
IHM	Interface Homem Máquina
IM	Imputação Múltipla
ISOM	Isomerização
IU	Imputação Única
LogReg	*Logistic regression*
k-out-of-n	“k” detectores de um sistema de “n” detectores
MAR	*Missing at Random*
MCAR	*Missing Completely at Random*
MCMC	*Markov Chain Monte Carlo*
MFG	*Mark Flow Graph*
MICE	*Multivariate Imputation by Chained Equation*
NMAR	*Missing Not at Random*

OE	*Outcome event* (Consequência indesejada)
P&ID	*Process and Instrumentation Diagram*
PFS	*Production Flow Schema*
PMM	*Predictive Mean Matching*
SCBP	Sistema de Controle Básico do Processo
SCr	Sistema Crítico
SCSP	Sistema de Controle relacionado à segurança para indústrias de processos
SED	Sistema a Eventos Discretos
SIS	Sistema Instrumentado de Segurança
TS_{FT}	*Training set of Fault Tree*
TS_{ET}	*Training set of Event Tree*
UE	*Undesired Event* (Evento indesejado)
VBA	*Visual Basic Application*

LISTA DE SÍMBOLOS

Imputação de dados

$\mathbf{Y}_{ij}$	variável da matriz de dados multivariada *p*-dimensional
Θ	vetor de parâmetros desconhecido
P	probabilidade
$\mathbf{Y}_{obs}$	conjunto finito de dados observados de **Y**
$\mathbf{Y}_{aus}$	conjunto finito de dados ausentes/faltantes (*missing*) de **Y**
$\mathbf{R}_i$	variável indicadora que fornece uma distribuição de probabilidade de falta completa de dados em um banco de dados.

Rede Bayesiana

RdB	rede bayesiana
P	probabilidade
S	estrutura ou GAO da RdB
GAO	grafo acíclico orientado
Θ	conjunto finito de parâmetros numéricos da rede Bayesiana
X	conjunto finito de variáveis aleatórias ou `nós` da rede Bayesiana
X_i	`nó` da rede bayesiana, representado por um círculo
F	conjunto finito de `arcos` orientados na rede Bayesiana
$Pa(X_i)$	`nó` pai de X_i da rede bayesiana, representado por um círculo
$P(X_i \mid Pa(X_i))$	probabilidade de X_i ocorrer dado que $Pa(X_i)$ ocorreu
Tr	árvore que maximiza o logaritmo da máxima verossimilhança dos dados

Rede de Petri

RdP	rede de Petri
L	conjunto finito de `lugares` da rede de Petri
T	conjunto finito de `transições` da rede de Petri
M	conjunto de `marcas` nos `lugares` da rede de Petri
M0	conjunto de `marcas iniciais` nos `lugares` da rede de Petri

SUMÁRIO

1 INTRODUÇÃO

Sistemas Críticos (SCr) são aqueles em que a ocorrência de determinadas falhas, podem resultar em acidentes com perdas de vidas humanas, danos ao meio ambiente e perdas financeiras significativas envolvendo custos de equipamentos e propriedades(KNIGHT, 2002). Por esta razão, estas falhas são denominadas falhas críticas(SQUILLANTE JR, 2011) e são caracterizadas por conduzirem esses sistemas às consequências definidas como inaceitáveis[1]. Exemplos de SCr incluem: sistemas de transportes de massa, sistemas de aviação, sistemas de usinas nucleares, sistemas de indústrias químicas e petroquímicas, sistema de equipamentos médicos, etc.(KNIGHT, 2002). As indústrias de processos[2], que estão inseridas nesta classe de sistemas, são o foco deste trabalho.

A questão da segurança[3] de um SCr – no que se refere às indústrias de processos, vem recebendo uma atenção crescente pela comunidade científica mundial. As razões principais são as ocorrências de acidentes e as consequências indesejadas que estes acidentes têm provocado (FLOREA e DOBRESCU, 2011). Acidente é a ocorrência de um evento ou de uma sequência de eventos, que causa(m) consequências indesejadas(FERDOUS, KHAN, *et al.*, 2013)(BAKOLAS e SALEH, 2011). A possível ocorrência destes eventos indesejáveis, durante a evolução dinâmica dos processos que ocorrem nesses sistemas, é motivada pela presença dos seguintes fatores: (i) ser humano, isto é, falha na operação humana; (ii) falha nos dispositivos; (iii) falha derivada da complexidade computacional dos algoritmos de controle lógico e sequencial; (iv) acidentes patogênicos e (v) evolução da falha crítica devido a ausência ou quebra de defesas ou violação dos requisitos de segurança.(SQUILLANTE JR, SANTOS FO, *et al.*, 2013)(SQUILLANTE JR, SANTOS FO, *et al.*, 2015).

---

[1] Entende-se por consequência inaceitável, aquela que coloca o sistema numa situação de risco incompatível com o nível de risco aceitável imposto por normas de segurança que devem ser observadas (IEC 61511, 2003).

[2] De acordo com o *Institute of Industrial & Systems Engineers* (IISE), as indústrias de processos são aquelas indústrias onde os processos de produção primários são tanto contínuos quanto em bateladas de tal forma que os materiais são indistinguíveis (Institute of Industrial & Systems Engineers, 2016).

[3] De acordo com a norma IEC 61508 - parte 4, segurança implica na ausência de riscos inaceitáveis. No presente trabalho, considera-se que um sistema em que o conceito de segurança é aplicado, resulta em uma classe de sistemas denominada sistemas seguros.

O fator humano envolvido nas fases de projeto, instalação, operação, manutenção e gestão, deve ser considerado como parte integrante dos processos de um SCr. Sob o ponto de vista de segurança funcional[4], discute-se que durante o projeto de plantas industriais, assim como, durante os processos de avaliação de riscos dessas plantas, é impossível conceber uma planta que seja totalmente livre de erros humanos(CACCIABUE, 2004). Ainda de acordo com (REASON, 1997), o erro humano tem um papel fundamental na ocorrência de acidentes em SCr, tais como, casos devidamente documentados em relatórios de investigação de acidentes na aviação, nos sistemas ferroviários ou nas instalações nucleares, e isso pode ser estendido também para as indústrias de processos.

A possibilidade de ocorrência de falha nos dispositivos está associada à probabilidade dos dispositivos de detecção (sensores) e atuação (atuadores), não executarem suas funções sob demanda dos processos, comprometendo a segurança dos processos (ROUVROYE e VAN DEN BLIEK, 2002).

Por sua vez, as falhas derivadas da complexidade computacional dos algoritmos de controle lógico e sequencial, são cada vez mais relevantes, em virtude do grau de comprometimento dos equipamentos com a integridade física dos operadores e com o meio ambiente no qual os equipamentos estão inseridos (MAZZOLINI, BRUSAFERRI e CARPANZANO, 2011).

Outra questão fundamental pertinente à segurança funcional de SCr está associada a acidentes patogênicos[5]. Vários relatórios de investigação de acidentes, apontam para eventos indesejáveis não observados ou ocultos, como fatores relevantes associados à evolução de eventos que caracteriza a ocorrência de um acidente(SALEH, MARAIS, *et al.*, 2010)(SQUILLANTE JR, SANTOS FO, *et al.*, 2015). Ainda de acordo com SALEH, MARAIS, et al (2010), acidentes tipicamente resultam da ausência ou brecha de defesas ou violação dos requisitos de segurança.

---

[4] A segurança funcional é parte da segurança global relacionada ao processo e ao sistema de controle básico do processo (SCBP), os quais dependem do funcionamento correto de sistemas instrumentados de segurança e de outras camadas de proteção (IEC 61511, 2003).

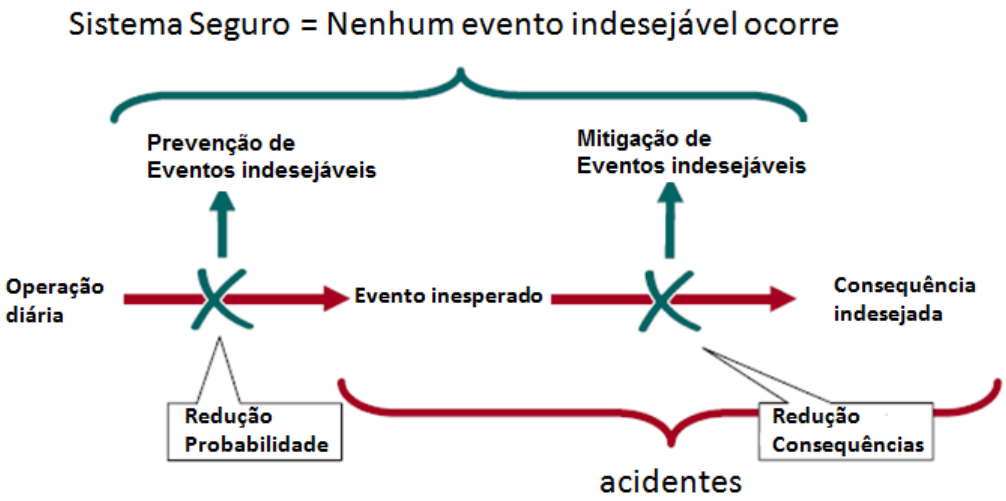
[5] Quando alguns possíveis estados críticos de SCr em operação, não são adequadamente observados por operadores e/ou sistemas de controle, podem conduzir esses sistemas a estados críticos ocultos e latentes, que aliados a outros fatores, podem precipitar em acidentes patogênicos (BAKOLAS e SALEH, 2011).

Neste cenário, assume-se que não é possível prever todos os eventos e estados críticos que violem os requisitos de segurança funcional destes sistemas. De qualquer modo, tais eventos podem provocar riscos que, dependendo de sua severidade, poderão: (i) comprometer a vida das pessoas, (ii) comprometer o meio ambiente, e/ou (iii) provocar perdas significativas com custos de equipamentos e instalações.

Desta forma, para garantir um nível de segurança funcional adequado em SCr, medidas apropriadas devem ser implementadas explorando melhor tanto a potencialidade das habilidades humanas, como o potencial de recursos de automação[6] para a prevenção de erros humanos, e para a mitigação das consequências de tais erros ou falhas (CACCIABUE, 2004). A prevenção tem como objetivo, diminuir a probabilidade de ocorrência de um determinado evento indesejável, enquanto que na mitigação, os esforços são realizados no sentido de reduzir as consequências desse evento (CARVALHO, 2011).

Adicionalmente, com relação às abordagens de prevenção e mitigação, Hollnagel (2007) argumenta que prevenir é melhor que mitigar. O autor acrescenta, que uma vez que na prática é impossível prevenir completamente todos os eventos indesejáveis (ex: eliminar completamente os riscos), as duas abordagens devem ser integradas conforme ilustrado na Figura 1

Figura 1 - Segurança por meio da prevenção e mitigação



Fonte: adaptado de (HOLLNAGEL, 2007)

[6] Tecnologia por meio da qual um processo ou procedimento é realizado sem assistência humana. Na prática isso envolve a utilização de um programa de instruções combinado a um sistema de controle que executa as instruções (GROOVER, 2011).

Sob o ponto de vista de métodos para garantir um nível de segurança funcional aceitável em SCr, este trabalho enfoca um método capaz de alinhar o princípio de defesa em profundidade(SKLET, 2006) com à propriedade de diagnosticabilidade segura (PAOLI e LAFORTUNE, 2005) (BAKOLAS e SALEH, 2011), para que sejam consideradas a identificação e avaliação de riscos no projeto de sistemas de controle relacionados à segurança de um SCr.

Um sistema a eventos discretos (SEDs) é dito ter a propriedade de diagnosticabilidade segura se ele for diagnosticável (SAMPATH, SENGUPTA, *et al.*, 1995), isto é, a detecção de uma falha ocorre com atraso limitado, antes da execução de uma sequência de eventos proibitivos que violam os requisitos de segurança(PAOLI e LAFORTUNE, 2005) (BAKOLAS e SALEH, 2011). Esta propriedade nos remete a considerar nos projetos de sistemas de controle relacionados à segurança, modelos de acidentes, ou seja, a descrição de cenários que consideram a sequência de eventos indesejáveis, que precederam à ocorrência de uma consequência indesejada, assim como, a diagnosticabilidade de cada um destes eventos.

O princípio de defesa em profundidade incorpora a idéia de múltiplas linhas de defesa e barreiras de segurança ao longo do cenário de acidente; e este princípio evita a dependência de assegurar a segurança por meio de um elemento simples(SKLET, 2006)(SALEH, MARAIS, *et al.*, 2010)(BAKOLAS e SALEH, 2011). Este princípio nos permite considerar nos projetos de sistemas de controle relacionados à segurança, algoritmos de defesa[7], endereçando as barreiras de segurança.

Neste contexto, quando se considera que o objetivo é contemplar os aspectos relacionados à segurança de um SCr, faz-se necessário detectar e tratar eventos indesejados. Estas considerações são justificadas, pois sempre existe a probabilidade destes eventos ocorrerem nestes sistemas (SCr como uma classe de SEDs). Estes eventos devem ser corretamente detectados, diagnosticados e tratados por sistemas de controle relacionados à segurança. Desta forma tem-se ainda que considerar que a monitoração, decisão e tomada de ação exclusivamente

[7] O termo “algoritmos de defesa” neste trabalho, refere-se aos algoritmos de diagnóstico e tratamento de cada evento iniciador, crítico e/ou indesejado de uma sequência concatenada de eventos que representa um cenário crítico. Estes algoritmos implementam as funções de segurança de cada barreira de prevenção e mitigação.

realizadas pelo homem (ex: operador), principalmente sob condições de estresse, pode colocar em risco a própria vida e de outras pessoas, o meio ambiente, os equipamentos e instalações.

Sob o ponto de vista de automação orientada à segurança das indústrias de processos, os sistemas instrumentados de segurança (SIS), de acordo com especialistas, é uma solução tecnológica para a implementação de sistemas de controle relacionados à segurança. O SIS é baseado em sistemas eletrônicos programáveis (SEP), sensores e atuadores de segurança. Algumas normas tais como a IEC 61508(IEC 61508, 2010) e a IEC 61511 (IEC 61511, 2003), entre outras, provêm diretrizes para diferentes atividades relacionadas ao ciclo de vida de projeto de SIS, tais como: identificação e avaliação de riscos, projeto, instalação, operação, manutenção, testes, entre outros (FANG e ZONGZHI WU, 2008)(LUNDTEIGEN e RAUSAND, 2009).

A fim de se tratar de projetos de sistemas de controle relacionados à segurança funcional, com foco nas indústrias de processos, foram pesquisadas propostas de arquiteturas de controle e de métodos para desenvolvimentos de projetos desta natureza.

Pfeffer e Urbas (2015) propõem cinco arquiteturas diferentes de SIS, endereçado à modularização das mesmas e que são praticadas por engenheiros de segurança funcional nas indústrias de processos. As arquiteturas apresentadas foram validadas, tendo como requisitos, as falhas aleatórias de hardware, reutilização e flexibilidade.

Embora esta proposta seja uma contribuição sob o ponto de vista da implementação de arquiteturas redundantes[8] e que são robustas às falhas de componentes; a mesma não endereça arquiteturas lógicas de sistemas de controle relacionados à segurança funcional, endereçando as funcionalidades de prevenção e mitigação de eventos críticos e que seja aderente às normas internacionais IEC 61508 e IEC 61511 que endereçam segurança funcional nas indústrias de processos.

[8] Redundância é a duplicação (ou mais) de componentes particulares de um sistema, com o objetivo de aumentar a confiabilidade geral do sistema. A redundância em efeito procura: (1) limitar o impacto de um único componente com baixa confiabilidade sobre a confiabilidade geral do sistema; (2) melhorar a confiabilidade de um componente crítico no sistema. (HOEPFER, SALEH e MARAIS, 2009).

Zhang e Jiang (2008) fazem uma revisão bibliográfica de sistemas de controle tolerantes a falhas e reconfiguráveis. As abordagens existentes foram classificadas com base em diferentes critérios, tais como, metodologias e aplicações. Um total de 376 referências foi pesquisado na literatura, com datas de 1971 até 2007, de modo que, as principais contribuições foram compiladas a fim de fornecer um panorama histórico de desenvolvimentos na área.

Sob o ponto de vista de segurança funcional de SCr, e segundo a norma IEC 61511(IEC 61511, 2003), as abordagens apresentadas no trabalho de Zhang e Jiang (2008), não são suficientes para garantir a segurança funcional das indústrias de processos. Entretanto, podem ser empregadas para o projeto de sistemas de controle básico do processo (SCBP). Adicionalmente, outros trabalhos análogos foram desenvolvidos (MORALES, MELO e MIYAGI, 2007) (RIASCOS, 2002) (RU e HADJICOSTIS, 2008).

Squillante (2011) apresenta em seu trabalho, uma arquitetura hierárquica de um SIS endereçando apenas o módulo funcional de prevenção, além do SCBP que realiza as funções de controle básico do processo – aderentes à norma IEC 61508 e IEC 61511. Adicionalmente foi proposto um método para o desenvolvimento de programas de controle, considerando o diagnóstico e tratamento de falhas críticas em SIS. O método considera a prevenção de falhas críticas, e utiliza a teoria de redes bayesianas e de controle relacionado à SEDs para diagnóstico e tratamento desta classe de falhas.

O método proposto por Squillante (2011) considera um estudo de HAZOP (do termo inglês *Hazard and Operability Studies*) realizado por uma equipe de especialistas com conhecimento multidisciplinar; e então aplica um formalismo para o desenvolvimento do projeto de SIS relacionado à prevenção de falhas críticas.

Os modelos de diagnóstico propostos por Squillante (2011) são derivados de uma descrição da relação causa x efeito, e não consideram o sequenciamento dos eventos, ou seja, são estabelecidas as condições que conduzem à falha crítica e se estabelece um modelo baseado em lógica combinatória; sem considerar o comportamento dinâmico de eventos que descrevessem a evolução da respectiva falha.

Souza (2014) propõe um método para desenvolvimento de sistemas de controle de mitigação de falhas críticas para os SCr, utilizando a abordagem de controle antecipativo e lógica *fuzzy*.

Embora os métodos propostos por Squillante (2011) e Souza J.A.L (2014), contribuam para a síntese de um SIS em SCr, eles não estão em consonância com as normas de segurança funcional aplicáveis, e ao conceito de sistema seguro proposto por Hollnagel (2007), pois consideram abordagens independentes de prevenção ou mitigação e não as duas abordagens integradas.

Adicionalmente, (FERRAREZI, SANTOS FO, *et al.*, 2014a)(FERRAREZI, SANTOS FO, *et al.*, 2014b) propõem um ambiente unificado para modelagem e posterior verificação da dinâmica de sistemas usando a técnica *model-checking* aplicada aos modelos dos programas de controle para SIS. A abordagem é orientada a modelos ou *Model-based Design*. O ambiente considera as peculiaridades de um SIS nos contextos específicos das camadas de prevenção e mitigação de falhas críticas, bem como, as possíveis interações que possam existir entre essas camadas, que não poderiam ser identificadas em uma abordagem não unificada. A proposta trata apenas da verificação formal (*model-checking*) de algoritmos de controle, mas entende-se que pode ser aplicada nas abordagens de prevenção e mitigação de falhas críticas.

Neste contexto, embora se observe que existam avanços nesta área, há uma carência de estudos que integrem as propostas em um único arcabouço, e que envolvam um novo paradigma de sistema de controle relacionado à segurança que considere as abordagens de prevenção e mitigação de falhas críticas. Entende-se que é necessário caracterizar melhor as sequências de eventos relacionados com a ocorrência de uma falha, e explorar isso para o projeto de um sistema de controle distribuído para atuar durante a evolução dos eventos que culminam com a ocorrência das falhas.

Neste sentido, outras fontes de informação também contribuem para identificar novos requisitos para a descrição de processos de degeneração e mitigação dos SCr relacionados às indústrias de processos. Com base nas fontes pesquisadas, o conceito de modelos de acidentes, que é comumente empregado em processos de investigação de causas de acidentes, mostra-se adequado à descrição de processos de evolução de eventos precedentes à ocorrência de acidentes (NIVOLIANITOU,

LEOPOULOS e KONSTANTINIDOU, 2004)(DUIJM, 2009) (RATHNAYAKA, KHAN e AMYOTTE, 2011)(BADREDDINE e BEN AMOR, 2013).

Neste contexto, surge a questão:

- ✓ Como vincular os cenários de acidentes aos requisitos para projetos de sistemas de controle relacionados à segurança de um SCr, assegurando a eficácia destes sistemas de controle, via caracterização do processo de encadeamento de eventos críticos?

O desafio passa a ser especificar um processo dinâmico que represente a lógica e a sequência de ocorrência de eventos críticos, que resultam em falhas críticas num SCr.

Por sua vez, a partir do momento em que se utiliza o conceito de modelagem de acidentes via abordagem probabilística considerando bancos de dados, como ferramenta para síntese de SIS, observa-se que a maioria dos bancos de dados nas indústrias de processos são incompletos, e infelizmente, este é um problema inevitável(LAKSHMINARAYAN, HARP e SAMAD, 1999). Frequentemente estes bancos de dados apresentam dois tipos de variáveis: (i) as que possuem dados faltantes (do termo inglês *missing*), cujos dados são algumas vezes “observados” e gravados no banco de dados, e algumas vezes “não observados” e não gravados no banco de dados; e (ii) as ocultas (do termo inglês *hidden*), cujos dados nunca foram observados e gravados no banco de dados(SINGH, 1998). Métodos propostos para modelagem de cenários de acidentes a partir de bancos de dados com variáveis ocultas, requerem o conhecimento humano. Esta abordagem é razoável, em alguns poucos domínios onde se tem pleno conhecimento das relações entre as variáveis. Por outro lado, esta abordagem é claramente inviável na maioria dos domínios da vida real(FRIEDMAN, 1997).

Neste contexto, este trabalho considera a modelagem de cenários de acidentes, considerando bancos de dados que apresentam variáveis com dados faltantes, endereçando a descrição do processo de evolução de eventos críticos “observados” e “parcialmente observados”.

1.1 OBJETIVO

O objetivo deste trabalho é propor uma metodologia para o projeto de um SCSP, isto é, de um sistema de controle baseado no conceito de segurança funcional para as indústrias de processo, de acordo com a norma IEC 61511 e que estabelece: (i) uma arquitetura de sistema de controle para prevenção e mitigação de falhas críticas de forma integrada, e (ii) um *framework* para a síntese de sistemas de controle desta natureza, baseado em modelos de acidentes, de modo que se possa intervir no processo de evolução de falhas críticas a partir da ocorrência de eventos críticos "observados" e que suporta eventos "parcialmente observados".

De forma específica, são consideradas as seguintes metas:

A. Em relação à arquitetura de controle:

(i) integração das abordagens de prevenção e mitigação de eventos críticos; em consonância com as normas IEC (IEC 61508, 2010) IEC (IEC 61511, 2003) e (HOLLNAGEL, 2007);

(ii) atende ao princípio de defesa em profundidade; e

(iii) atende a propriedade de diagnosticabilidade segura;

B. Em relação às medidas para garantir um nível de segurança funcional aceitável nas indústrias de processos, baseado no conceito de SIS:

(i) reclassificação do sistema de barreiras de segurança.

C. Em relação ao framework para a síntese de sistemas de controle de segurança:

(i) descrição de processos de evolução de eventos críticos, a partir da modelagem de acidentes via abordagem probabilística, considerando inclusive os casos de bancos de dados incompletos;

(ii) integração dos modelos de acidentes com as técnicas clássicas de identificação e análise de riscos (ex: HAZOP); e

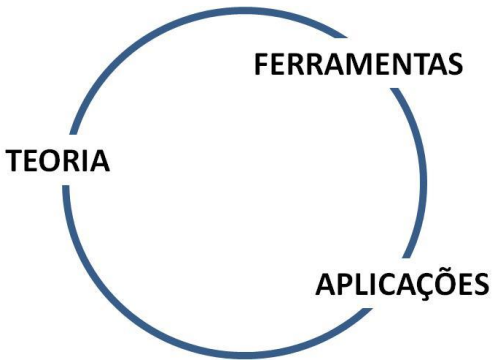
(iii) modelagem dos algoritmos de defesa de prevenção e mitigação de falhas críticas, a partir de formalismos da teoria de controle de SEDs e aderentes ao conceito de SIS.

Finalmente, para analisar os resultados alcançados e validar a metodologia proposta, dois exemplos de aplicação de SCr relacionados às indústrias de processos investigados na literatura foram considerados.

1.2 MÉTODO DE PESQUISA

O ciclo de vida do projeto de pesquisa deste trabalho baseou-se método apresentado por (JENSEN, 1992); onde são abordados de forma cíclica e repetitiva (Figura 2), três aspectos: (i) aspectos associados às teorias, (ii) ferramentas e (iii) aplicações. Para solucionar os problemas identificados nas aplicações, estudam-se os aspectos teóricos relacionados, propondo uma revisão das abordagens, modificações e aperfeiçoamentos das mesmas. Por meio do desenvolvimento de novas ferramentas, ou a partir de ferramentas existentes, aplicam-se as modificações e aperfeiçoamentos nos aspectos teóricos aos problemas das aplicações, a fim de validar as novas abordagens propostas.

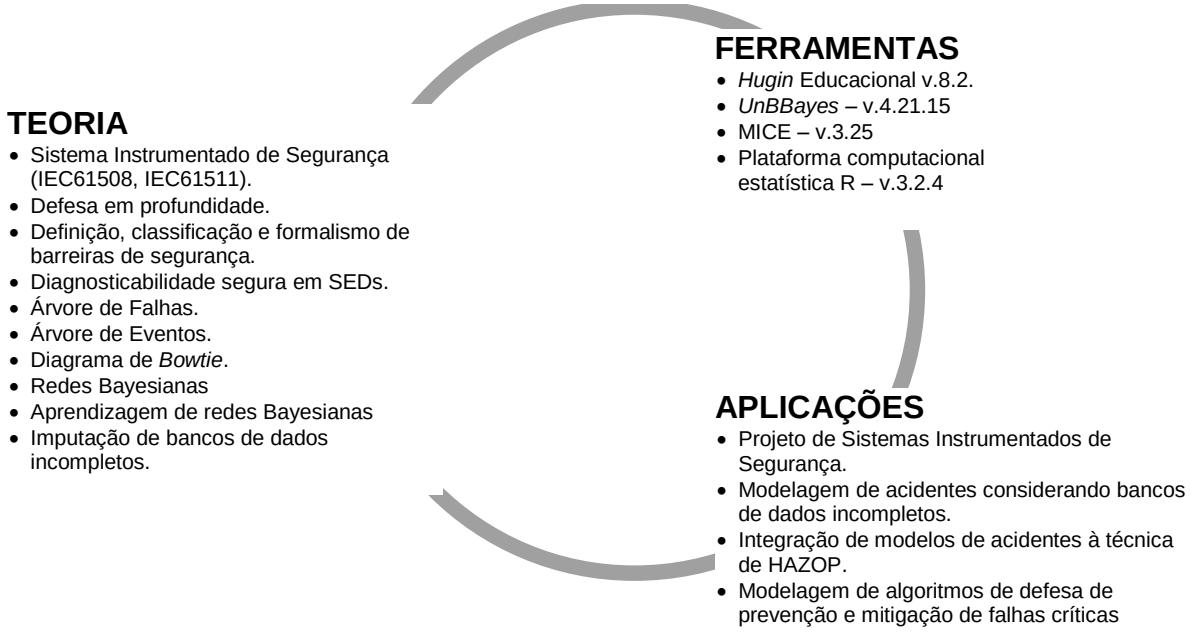
Figura 2 – Ciclo para desenvolvimento da pesquisa



Fonte: (JENSEN, 1992)

É uma abordagem de engenharia que, neste trabalho, considera os aspectos formais associados à definição de modelos, os métodos de análises aplicáveis via ferramentas computacionais existentes e as aplicações em processos industriais – baseadas em exemplos de aplicação obtidos da literatura – como motor de desenvolvimento e concepção de novos paradigmas. Os três aspectos identificados em (JENSEN, 1992) evoluem simultaneamente, condicionando-se mutuamente. Os desenvolvimentos em cada um dos aspectos identificados se beneficiam das sinergias resultantes das atividades em cada um dos outros dois aspectos. A Figura 3 sintetiza os aspectos do presente trabalho.

Figura 3 – Ciclo para o desenvolvimento desta pesquisa



Fonte: próprio autor

1.3 ORGANIZAÇÃO DO TEXTO

O Capítulo 2 descreve a revisão da literatura iniciando com o conceito de defesa em profundidade, assim como, das estratégias de implementação deste conceito e formalismos para projetos de sistemas de controle relacionados à segurança. Em seguida, a propriedade de diagnosticabilidade segura também é apresentada, como característica intrínseca a ser incorporada às estratégias de projeto e implementação destes mesmos sistemas de controle. Uma introdução aos modelos de acidentes é feita e uma comparação de técnicas para a modelagem de acidentes é apresentada. As técnicas de imputação de dados também são introduzidas, como meio para se tratar de bancos de dados com dados faltantes (*missing data*), assim como, a ferramenta computacional e um algoritmo de imputação de dados faltantes são apresentados. Finalmente, a rede bayesiana e sua formalização são apresentadas e aplicações em sistemas relacionados à segurança são discutidas. Também são discutidas técnicas de aprendizagem de modelos baseados em redes bayesianas e sua pertinência à modelagem de diagramas de *bowtie*.

O Capítulo 3 apresenta uma metodologia para o desenvolvimento de SCSP que envolve: (i) uma arquitetura lógica que endereça as funções de segurança para

prevenção e mitigação de eventos críticos observáveis e parcialmente observáveis aplicando a propriedade de diagnosticabilidade segura e o princípio de defesa em profundidade, (ii) uma reclassificação de sistemas de barreiras de segurança considerando o uso de SIS e que é aderente à arquitetura lógica proposta, e (iii) um *framework* para a síntese de SCSP.

No Capítulo 4 o *framework* para a síntese de SCSP é aplicado em um exemplo – obtido da literatura - para a validação do mesmo. Os resultados obtidos com a aplicação do *framework* são discutidos.

O Capítulo 5 apresenta as principais conclusões e contribuições deste trabalho.

O Anexo A apresenta a metodologia PFS/MFG. O Apêndice A apresenta um procedimento para a geração de bancos de dados de treinamentos contendo dados ausentes/faltantes. O Apêndice B apresenta o algoritmo de geração de dados faltantes em bancos de dados. O Apêndice C apresenta uma síntese do estudo de geração de modelos de acidentes, a partir de bancos de dados incompletos ou com dados faltantes, via técnicas de imputação de dados e aprendizagem bayesiana. O Apêndice D mostra a aplicação do *framework* para a síntese do SCSP para um segundo exemplo de aplicação. Finalmente, os Apêndices E e F apresentam as Tabelas de HAZOP para o primeiro e segundo exemplos de aplicação, respectivamente.

2. REVISÃO DA LITERATURA

Este capítulo aborda aspectos teóricos, técnicas e ferramentas que constituíram o arcabouço para o desenvolvimento da metodologia para o projeto de um sistema de controle baseado no conceito de segurança funcional para as indústrias de processos. Inicialmente, na seção 2.1 é apresentado o princípio de defesa em profundidade que tem sido utilizado para a concepção de projetos relacionados à segurança. Nas seções 2.2 e 2.3 são abordados fundamentos de barreiras de segurança, sua classificação e formalização para aplicação em cenários de acidentes. Na seção 2.4 é apresentada a propriedade de diagnosticabilidade segura que quando associada ao princípio de defesa em profundidade, podem ser exploradas para aumentar a eficácia de sistemas de controle orientados à segurança das indústrias de processos. A seção 2.5 começa com uma definição de modelos de cenários de acidentes, e depois apresenta uma comparação de técnicas formais para a modelagem de cenários de acidentes. No final, a técnica de *bowtie* é discutida, assim como, o formalismo necessário para a sua construção. Na seção 2.6, técnicas de imputação de dados são apresentadas, como uma solução estatística para bancos de dados incompletos ou com dados faltantes. A seção 2.7 apresenta inicialmente a teoria de rede bayesiana, sua formalização, aplicações em sistemas relacionados à segurança, e são apresentadas e discutidas técnicas de aprendizagem dessas redes. Na seção 2.8 é apresentada a Rede de Petri e sua extensão denominada *Production Flow Schema* (PFS) utilizada para modelagem de atividades que sejam dirigidas por eventos em indústrias de processos. Finalmente na seção 2.9 é apresentada a síntese deste capítulo.

2.1 DEFESA EM PROFUNDIDADE

Defesa em profundidade (do termo em inglês *Defense-in-depth*) é um princípio fundamental para que um SCr atinja e mantenha um estado de segurança (SALEH, MARAIS, *et al.*, 2010) (BAKOLAS e SALEH, 2011). Inicialmente conceituado para a indústria nuclear pela comissão reguladora nuclear dos Estados Unidos, este princípio vem sendo a base para tomada de decisões baseada no conhecimento de riscos(SALEH, MARAIS, *et al.*, 2010). Este princípio é também reconhecido sob

outros nomes (ex: camadas de proteção, do termo em inglês *layers of protection*) na indústria química (SUMMERS, 2003).

O princípio de defesa em profundidade constitui a base para a discussão de barreiras de segurança. Sklet (2006), descreve o princípio de defesa em profundidade da seguinte maneira:

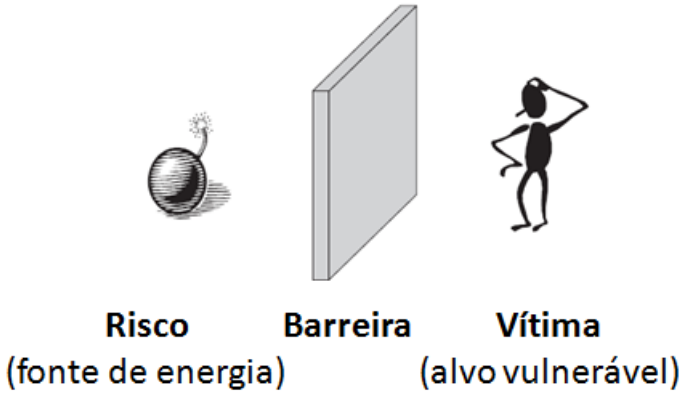
> Para compensar falhas mecânicas e erros humanos, a defesa em profundidade é implementada com base nos níveis de proteção, de modo que, sucessivas barreiras previnem a liberação de material radioativo para o meio ambiente. O princípio inclui a proteção das barreiras para evitar danos à planta (processo) 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 (SKLET, 2006).

O conceito de barreira de segurança é baseado em dois modelos de acidentes: (i) modelo de energia e (ii) modelo de processo.

O princípio básico do modelo de energia é separar os riscos (fontes de energia) das vítimas, por meio das barreiras de segurança (Figura 4)(HADDON, 1990)(SQUILLANTE JR, SANTOS FO, *et al.*, 2015).

O modelo de processo divide a sequência de situações que levam a um acidente em diferentes estágios, para auxiliar o projetista a compreender como o SCr é deteriorado gradualmente a partir de um estado normal até atingir o estado em que o acidente ocorre (KJELLÉN, 2000). Neste sentido, os fatores que previnem a transição de estados em um processo de acidente, podem ser considerados como barreiras de segurança. A Figura 5 mostra as barreiras de segurança conjugadas a um acidente (evolução do processo).

Figura 4 – Modelo de energia



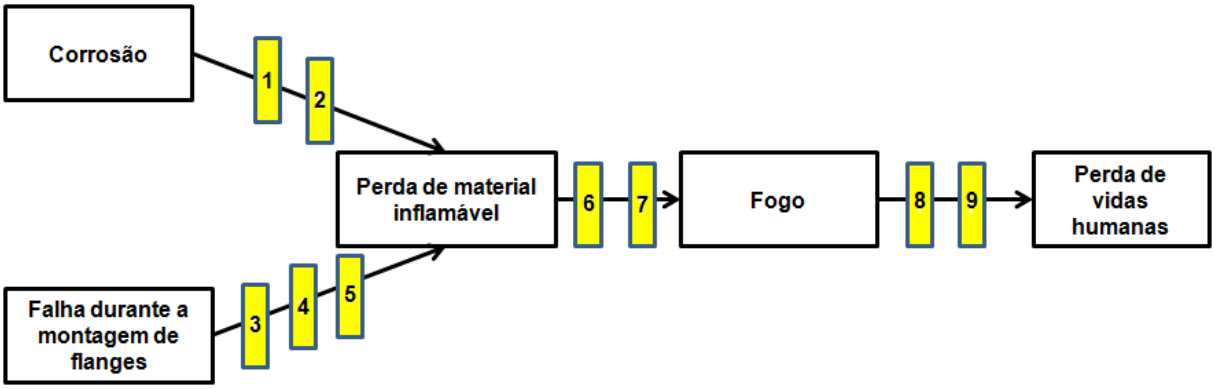
Fonte: baseada em (HADDON, 1990)

O princípio de defesa em profundidade pode ser entendido por meio de um modelo de múltiplas barreiras de segurança ao longo do cenário de acidente. Desta forma, entende-se que acidentes resultam da ausência/brecha de/em barreiras ou então da violação das restrições de segurança vinculadas às barreiras(SALEH, MARAIS, *et al.*, 2010).

A implementação da defesa em profundidade é assim realizada por diversas e sucessivas barreiras de segurança destinadas a: (i) prevenir a ocorrência de eventos críticos, (ii) prevenir que o cenário de acidente evolua, se as barreiras de segurança falharem em suas funções, e (iii) mitigar ou conter as consequências provocadas pelos acidentes, em caso de brecha ou ausência das barreiras de prevenção.

Na Figura 5, os retângulos amarelos correspondem às barreiras de segurança. É importante a distinção entre as barreiras responsáveis pela prevenção e pela mitigação durante a sequência de eventos ou cenário do acidente. Também é importante identificar os fatores de riscos que podem influenciar no desempenho destas barreiras. Na Figura 5, as barreiras 3, 4 e 5 são responsáveis pelo controle da montagem da tubulação e flanges, assim como, controle de testes de vazamento das tubulações realizados por empresas terceirizadas. As barreiras 1 e 2 são responsáveis por prevenir o vazamento de material inflamável (ex: gás hidrocarboneto) na atmosfera devido à corrosão na tubulação. As barreiras 6 e 7 são responsáveis pela prevenção de incêndios, por meio de degeneração do SCr, e finalmente, as barreiras 8 e 9 são responsáveis pela mitigação dos danos provocados pelo incêndio, a partir da ativação do sistema de dilúvio e sinalização de caminhos de evacuação do pessoal.

Figura 5 – Modelo de processo de um acidente e as barreiras de segurança



1. Monitoração da corrosão	2. Inspeção para identificar corrosão
3. Controle da montagem para identificação de falhas	4. Inspeção dos serviços realizados por empresas terceirizadas, a fim de evitar falhas
5. Teste de vazamento	6. Degeneração do processo para reduzir a magnitude da liberação de material inflamável
7. Desconexão de todas as possíveis fontes de ignição	8. Ativação do sistema de dilúvio para extinção do fogo
9. Caminhos de evacuação do pessoal	

Fonte: baseada em (SKLET, 2006)

O princípio de defesa em profundidade tem sido e continua sendo um meio efetivo para lidar com incertezas em equipamentos, desvios de processo e erros humanos (SALEH, MARAIS, *et al.*, 2010).

2.2 FUNDAMENTOS DE BARREIRAS DE SEGURANÇA

O princípio de defesa em profundidade e as normas de segurança funcional das indústrias de processos, tais como a (IEC 61508, 2010) e (IEC 61511, 2003), entre outras, demonstram a importância de barreiras de segurança em ordem para prevenir e/ou reduzir riscos de acidentes(SKLET, 2006).

2.2.1 Definição

O trabalho de Sklet (2006) propõe definições formais para três termos fundamentais a seguir:

a. Barreiras de segurança - são meios físicos e/ou não físicos planejados para prevenir, controlar, ou mitigar eventos indesejados ou acidentes. Os meios podem ser desde uma unidade técnica ou ação humana até um sistema sócio-técnico complexo. Planejar implica que no mínimo, um dos propósitos dos meios é a redução do risco. Prevenir significa reduzir a probabilidade de um evento indesejável. Controlar significa limitar a extensão e/ou duração de um evento indesejável. Mitigar significa reduzir os efeitos provocados pelo evento indesejável. Os eventos indesejáveis podem ser oriundos de falhas técnicas, erros humanos, eventos externos, ou uma combinação destas ocorrências que podem provocar riscos potenciais.
b. Função da barreira - é uma função planejada para prevenir, controlar ou mitigar eventos indesejados ou acidentes. As funções das barreiras descrevem o propósito das barreiras de segurança, ou seja, se as barreiras irão prevenir, controlar ou mitigar eventos indesejáveis ou acidentes. Se a função da barreira é realizada com sucesso, isto deve ocasionar um efeito direto e significativo na ocorrência e/ou consequências de um evento indesejável ou acidente. A função da barreira deve preferencialmente ser definida por um verbo e um substantivo (ex: “fechar válvula” e “desligar equipamento”).
c. Sistemas de barreiras - é um sistema que é projetado e implementado para realizar uma ou mais funções das barreiras. Um sistema de barreiras pode ser formado por elementos de hardware e software, atividades operacionais executadas por humanos, ou uma combinação dos mesmos. Um elemento de barreira é um componente ou subsistema de um sistema de barreiras que, por ele próprio, não é suficiente para realizar a função da barreira. Um subsistema da barreira pode compreender vários elementos redundantes da barreira. Neste caso, um elemento específico da barreira não precisa estar em funcionamento para o sistema realizar a função da barreira. Este é o caso de detectores de gás redundantes, conectados em uma configuração “*k-out-of-n*”, ou seja, se “*k*” detectores de um sistema de “*n*” detectores estiverem realizando, de forma adequada, a mesma função; então a função realizada por “*k*” detectores é a função do sistema formado por “*n*” detectores. Por exemplo, para k=2 e n=3, se dois detectores informarem nível alto de

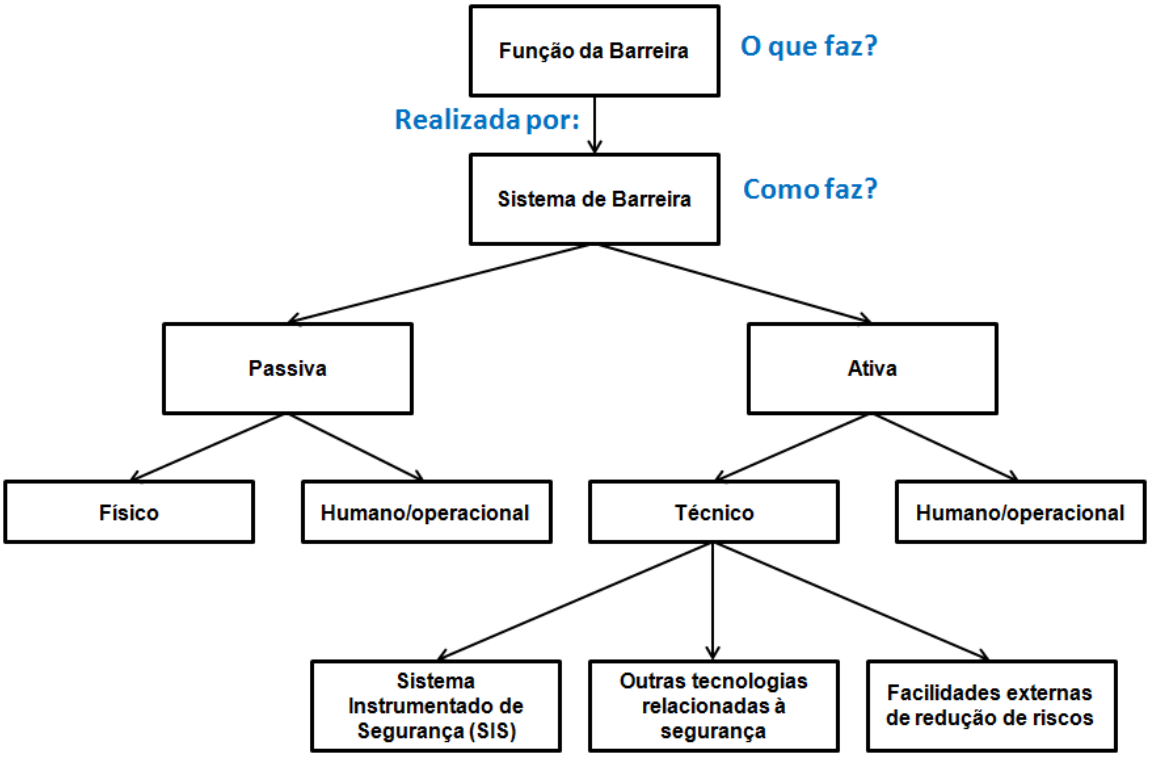
concentração de gás combustível (função de barreira), então o sistema de três detectores informam nível alto de concentração de gás combustível.

2.2.2 Classificação de barreiras de segurança

Diferentes classificações de barreiras de segurança são encontradas na literatura. Sklet (2006) apresenta em seu estudo, uma revisão bibliográfica abordando as diferentes formas de classificação de barreiras de segurança. Esta classificação pode ser baseada em (i) funções(HOLLNAGEL, 2004)(ANDERSEN, H.; CASAL, J.; DANDRIEUX, A.; DEBRAY, B.; DE DIANOUS, V.; DUIJM, N.J., 2004)(DUIJM, ANDERSEN, *et al.*, 2004), (ii) sistemas(WAHLSTROM e GUNSELL, 1998)(KECKLUND, L.J.; EDLAND, A.; WEDIN, P.; SVENSON, O., 1996) e (iii) outras abordagens para as barreiras de segurança(SCHUPP, 2004)(GROOSSENS e HOURTOLOU, 2003)(RAUSAND e HOYLAND, 2004)(HOLAND, 1997).

Sklet (2006) apresenta uma classificação de barreiras de segurança baseada em propostas similares sugeridas por (HALE, 2003) e pela norma IEC 61511(IEC, 2003). A Figura 6 ilustra a classificação.

Figura 6 – Classificação de barreiras de segurança



Fonte: (SKLET, 2006)

Com base na Figura 6, algumas observações importantes são destacadas:

- Sobre as barreiras físicas:

(i) As barreiras passivas físicas funcionam continuamente e não necessitam ser ativadas.

   i. Exemplos: paredes de contenção e paredes de proteção contra incêndio.

   ii. Elas podem também ser temporárias (ex: uma grade de obstrução temporária numa determinada área de risco onde uma atividade de trabalho está sendo executada).

(ii) As barreiras ativas técnicas são iniciadas se um risco existir.

   i. Devido aos avanços da tecnologia, outros mecanismos de controle foram incorporados como sendo sistemas de barreiras(REASON, PARKER e LAWTON, 1998).

- Sobre as barreiras humano/operacionais:

(i) As barreiras passivas podem funcionar continuamente, ou ser implementada como uma parte de soluções para evitar atividades de alto risco (ex: assegurar distâncias seguras entre a fonte de energia e a vítima – pelo princípio de (HADDON, 1990)).

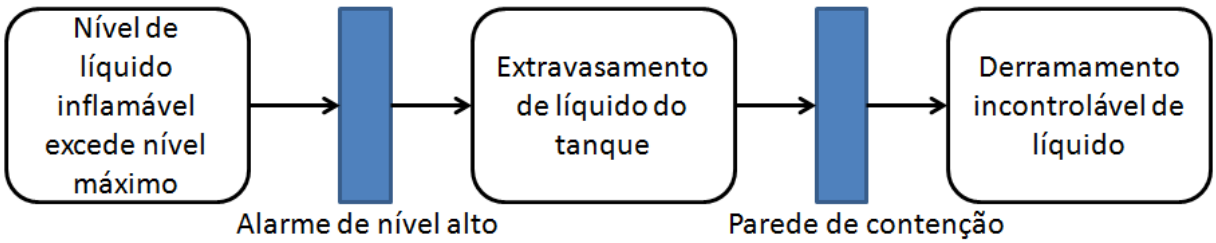
(ii) As barreiras ativas podem funcionar em modo contínuo ou sob demanda. Frequentemente, essas barreiras são uma parte dos fatores a serem consideradas (ex: autocontrole de atividades de risco ou controle de atividades de risco realizadas por empresas terceirizadas), com o propósito de prevenir falhas potenciais (ex: falhas introduzidas pelo homem).

Sklet (2006) também argumenta que as barreiras de segurança podem ser classificadas de outras maneiras, uma vez que a classificação ilustrada na Figura 6 pode não ser adequada para um determinado propósito.

2.3 DIAGRAMA DE BARREIRAS DE SEGURANÇA

O diagrama de barreiras é uma representação gráfica que mostra, como as barreiras de segurança agem no sentido de prevenir a propagação de eventos iniciais indesejados até atingir resultados indesejados ou acidente. Estes diagramas podem descrever também possíveis cenários de acidentes(DUIJM, 2009). Entende-se por cenário, a descrição da evolução de eventos indesejados desde a ocorrência de um evento inicial até se atingir um estado catastrófico ou acidente. Se uma barreira de segurança executar sua função com sucesso, a evolução de eventos indesejados é interrompida na barreira, caso contrário, ou seja, se a barreira falhar, o diagrama mostra a próxima barreira a ser executada até o acidente ocorrer; caso todas as barreiras tenham falhado na execução de suas funções (DUIJM, 2009). A Figura 7 mostra um exemplo de um diagrama de barreiras. Neste exemplo, duas barreiras são representadas: (i) alarme de nível alto de líquido inflamável e (ii) parede de contenção de líquido inflamável. Estas barreiras previnem que o líquido ultrapasse o nível alto permitido no tanque e o resultado seja o derramamento deste líquido na área industrial.

Figura 7 – Exemplo de um Diagrama de barreiras



Fonte: adaptado de (DUIJM, 2009)

Os diagramas de barreiras têm sido usados como ferramenta para análise e gestão de riscos nas indústrias de processos. Esses diagramas permitem a comunicação entre especialistas e pessoas não especialistas, pois descrevem de forma simples e clara, a descrição de medidas a serem tomadas para a prevenção e a mitigação de acidentes(DUIJM, 2009). A principal vantagem dos diagramas de barreiras de segurança é o foco nas medidas de segurança, inseridas no sistema para prevenir e mitigar acidentes. Essas medidas, representadas graficamente por barreiras de segurança, podem fornecer todas as informações necessárias para a manutenção e operacionalidade das barreiras.

2.3.1 Formalização

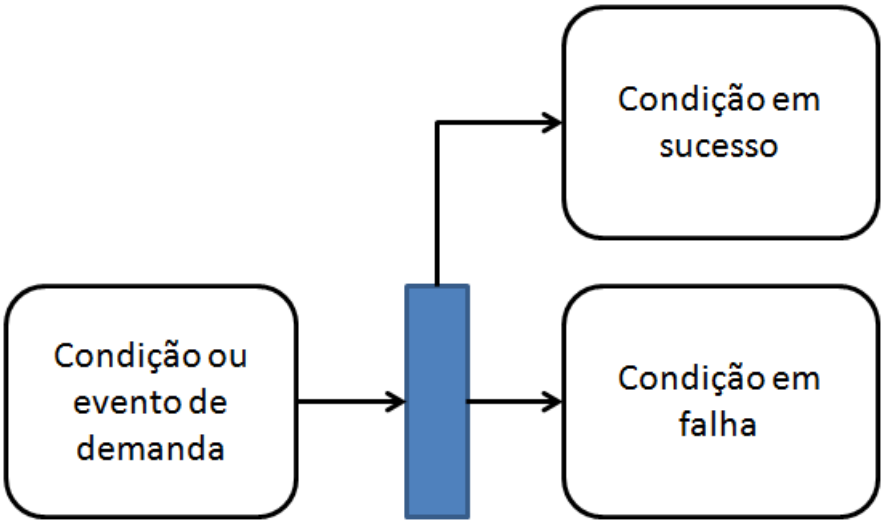
O diagrama de barreiras de segurança é um grafo (HARARY, 1969) acíclico orientado, capaz de descrever a evolução de estados a partir da ocorrência de eventos, podendo ou não ser dependentes do tempo. Por sua vez, esses grafos também permitem a avaliação da probabilidade condicional de ocorrência dos estados no diagrama, dados: (i) os estados iniciais, e (ii) as probabilidades de eficácia das barreiras(DUIJM, 2009).

Portanto, com base na teoria de grafos, as barreiras de segurança são os `nós`[9] ou `vértices` do grafo. As `arestas` entre os `nós` correspondem às condições ou estados do sistema: (i) no lado esquerdo da barreira de segurança, tal condição ou estado é responsável pela ativação da barreira (estado de demanda ou condição de demanda), enquanto que, (ii) no lado direito da barreira de segurança, tal condição ou estado ocorre quando a função de barreira falhar.

Outros estados no lado direito da barreira podem representar diferentes respostas da barreira, mas geralmente somente duas respostas são consideradas: sucesso ou falha. Por exemplo, para uma válvula de alívio de pressão, uma condição de sucesso conduz a uma liberação de material, o qual não é uma condição normal, e que, portanto, deve ser incluída no diagrama de barreira; dando origem a um cenário alternativo (ex: caminho alternativo por meio do diagrama de barreira). A notação gráfica para barreiras com dois estados ou condições no lado direito, é mostrada na Figura 8 .

[9] Termos relacionados à teoria de grafos estão sendo representados no texto com `fonte Courier New`

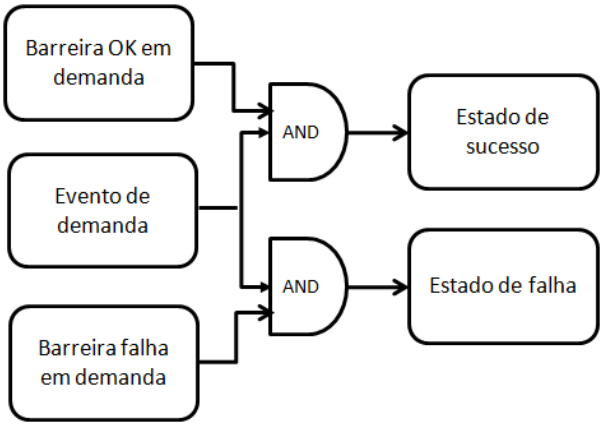
Figura 8 – Exemplo de um diagrama de barreiras com dois estados ou condições do lado direito da barreira.



Fonte: adaptado de (DUIJM, 2009).

Diagramas de barreiras de segurança usam a mesma lógica presente em modelos do tipo árvore de falhas (AF) e árvore de eventos (AE). Entretanto, as lógicas e eventos básicos relacionados ao funcionamento de cada barreira são encapsulados em um único elemento para diminuir a complexidade do grafo, resultando em diagramas mais simples e que facilitam a compreensão. A Figura 9 mostra um diagrama de barreiras representado como uma AF. A barreira de segurança é representada por uma porta lógica *AND* (ex: a condição ou estado de falha é atingida quando a demanda ocorre e a barreira falha). Nota-se que a representação na forma de AF não permite mostrar uma condição ou estado de sucesso sem introduzir uma nova condição de entrada (barreira OK em demanda) e uma nova porta lógica *AND*.

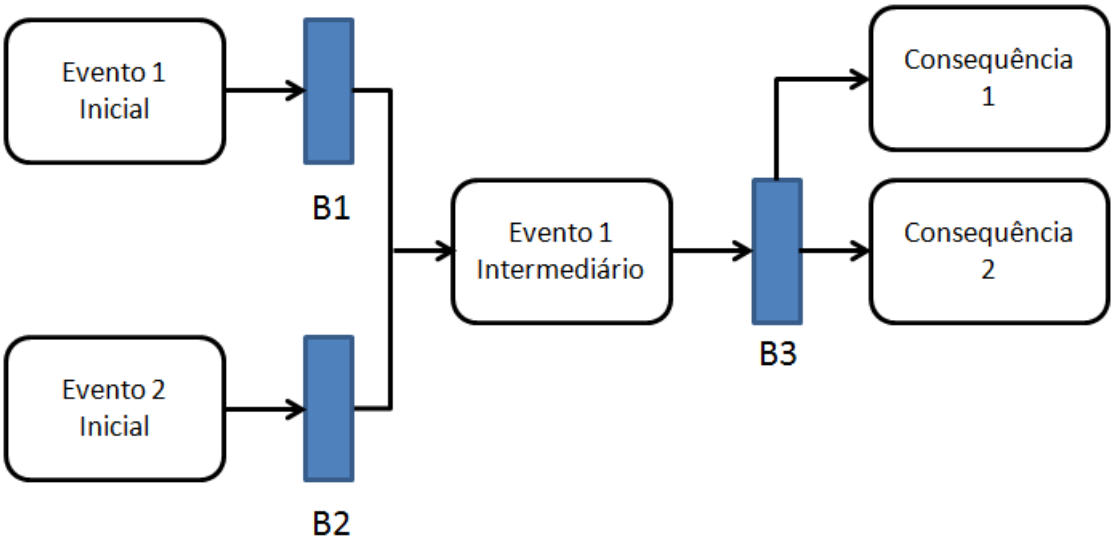
Figura 9 – Diagrama de barreira representado como uma AF com portas AND.



Fonte: adaptado de (DUIJM, 2009).

Um diagrama de barreiras genérico é ilustrado na Figura 10. A leitura do diagrama é feita da esquerda (cenário inicial com o(s) evento(s) inicial(is)) para a direita (cenário final com o(s) resultado(s) indesejado(s) ou consequência(s)).

Figura 10 – Diagrama de barreira convergente



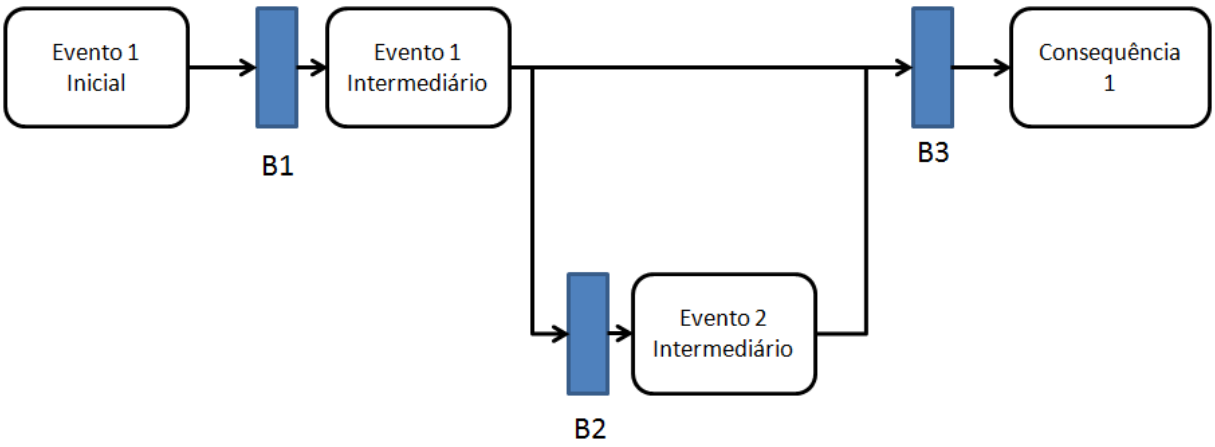
Fonte: adaptado de (DUIJM, 2009).

2.3.2 Regras para a construção dos diagramas

Os diagramas de barreiras de segurança inicialmente eram construídos manualmente e baseados em regras intuitivas. Com o desenvolvimento de ferramentas de software para auxiliar projetistas na construção e gestão de barreiras de segurança, houve a necessidade de se estabelecer as regras lógicas que governam esses diagramas. A seguir, apresenta-se as regras fundamentais para elaboração de diagramas de barreiras de segurança de acordo com (DUIJM, 2009).

- **Princípio da mútua exclusão** – cada barreira de segurança responde a uma condição de demanda bem conhecida e conduz aos estados de sucesso ou falha de forma mutuamente exclusiva. Desta forma, não se considera a hipótese de projeto de barreiras neutras que não interfere no processo de segurança, ou seja, seja indiferente à sua resposta sob demanda. Consequentemente, um “curto-circuito” colocado em paralelo com uma barreira, como ilustrado na Figura 11 não é permitido, pois representaria que a barreira B2 seria neutra.

Figura 11 – Diagrama inválido de barreira de segurança com um ‘curto-circuito”



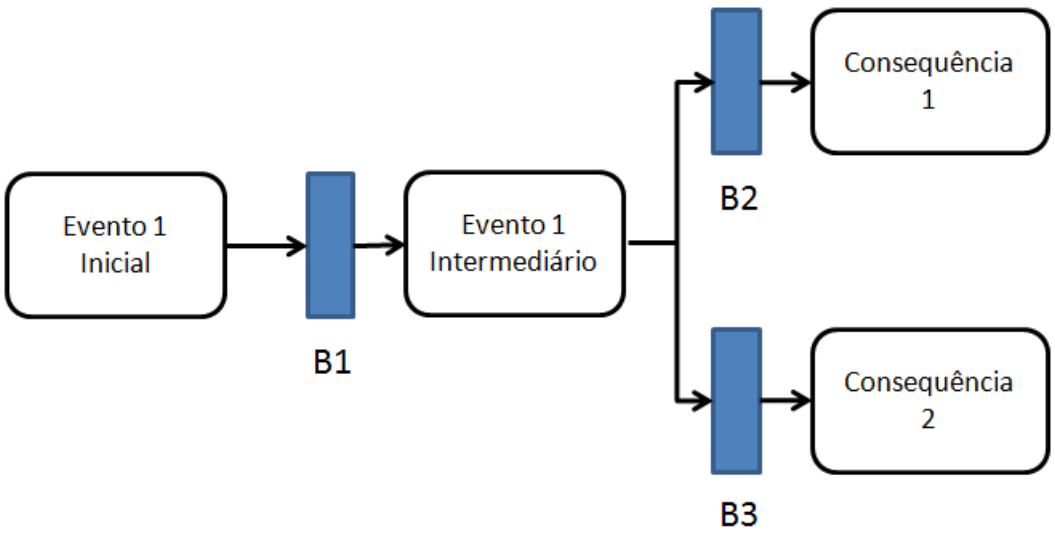
Fonte: adaptado de (DUIJM, 2009).

- **Modularização** – cada barreira é única, isto é, possui uma função determinada para desempenhar, enquanto que, os estados alcançados a partir da mesma podem ser compartilhados como consequência ou como um evento inicial em outros diagramas.
- **Compartilhamento de elementos** – os elementos que compõem uma barreira não necessitam serem únicos, ou seja, de uso exclusivo. Por exemplo: barreiras diferentes podem ter uma fonte de alimentação comum, ou então ações relativas a várias barreiras podem ser realizadas pelo mesmo operador.
- **Grafos convergentes** – são grafos onde vários nós localizados no lado antecedente são conectados a um único nó no lado consequente. Na Figura 10, por exemplo, as barreiras B1, B2 e B3 formam um grafo convergente. No diagrama convergente, as `arestas` que conectam várias barreiras do lado esquerdo com barreiras no lado direito, representam uma porta lógica *OR*, (ex: Na Figura 10, as condições de demanda para a barreira B3 aparecem quando ocorrer a condição de falha da barreira B1 “ou” ocorrer a condição de falha da barreira B2 (cenários alternativos)). Diagramas convergentes podem representar os caminhos de uma AF para uma falha crítica a partir de diferentes eventos indesejados iniciais.
- **Grafos divergentes** – existem duas situações possíveis:

- Caminhos divergentes a partir de um nó do tipo barreira. Neste caso, as `arestas` representam condições mutuamente exclusivas, conforme ilustrado pelas setas que saem de B3 na Figura 10.
- Caminhos divergentes a partir de `arestas` associadas a uma mesma condição. Neste caso, uma `aresta` que conecta uma barreira do lado esquerdo com várias barreiras do lado direito, resulta em caminhos paralelos, ou seja, se a barreira que antecede falhar, todas as barreiras consequentes serão demandadas. Na Figura 12 a barreira B1 conecta-se à ambas as barreiras B2 e B3 no lado direito, por meio de uma única condição ou evento 1 intermediário.

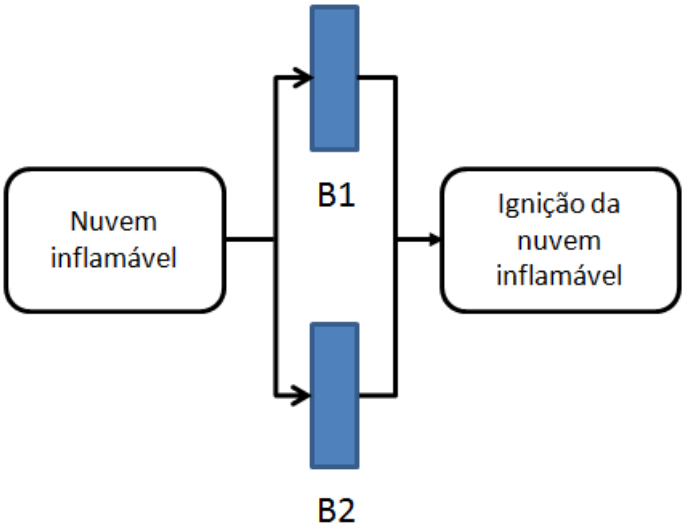
- **Barreiras simultâneas** – é quando várias barreiras agem simultaneamente contra a evolução de uma condição ou evento. Neste caso, a condição de falha de todas essas barreiras é idêntica. Por exemplo, na Figura 13 quando uma nuvem inflamável aparece, a ignição pode ser minimizada: (i) pela instalação de um equipamento a prova de explosão (barreira passiva – B1) e (ii) por meio da proibição de fumantes na área (barreira comportamental baseada em aviso passivo – B2). Observa-se que a condição de falha de ambas as barreiras é a mesma (ignição da nuvem inflamável).

Figura 12 – Exemplo de um diagrama de barreira de segurança divergente.



Fonte: adaptado de (DUIJM, 2009).

Figura 13 – Duas barreiras paralelas entre dois eventos

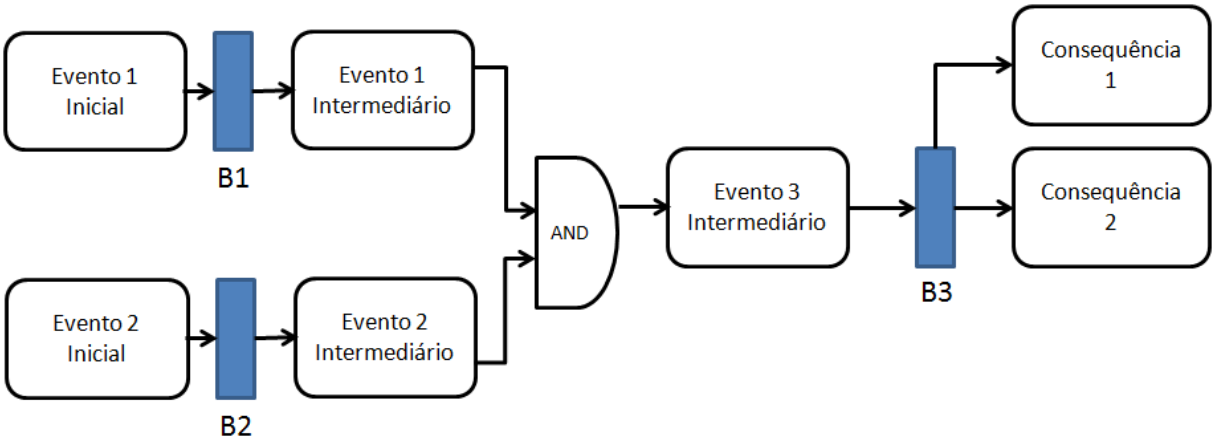


Fonte: adaptado de (DUIJM, 2009)

- **Conexão entre diagramas de barreiras** – existem procedimentos para estabelecer a conexão entre diferentes diagramas de barreiras:
    - Um diagrama de barreira contém `arestas` com o ambiente externo. As `arestas` do lado antecedente correspondem a condições ou eventos iniciais e as arestas do lado consequente corresponde às consequências que podem ser condições ou eventos de outro diagrama e vice-versa(DUIJM, 2009).
    - Não existem regras formais que orientam como iniciar ou finalizar um diagrama de barreiras, sendo possível dividir um diagrama em vários diagramas de acordo com a necessidade do projetista.
        - A dimensão mínima de um diagrama consiste de uma única barreira e suas correspondentes condições de demanda e estados em caso de falha ou sucesso.
        - Se diagramas compartilham condições ou eventos, então eles são conectados e, portanto, por meio deles é possível gerar um único diagrama de barreiras, que deve ser orientado e acíclico.
    - Desta forma, conclui-se que um diagrama de barreiras de segurança pode ser dividido em vários diagramas conectados entre si.

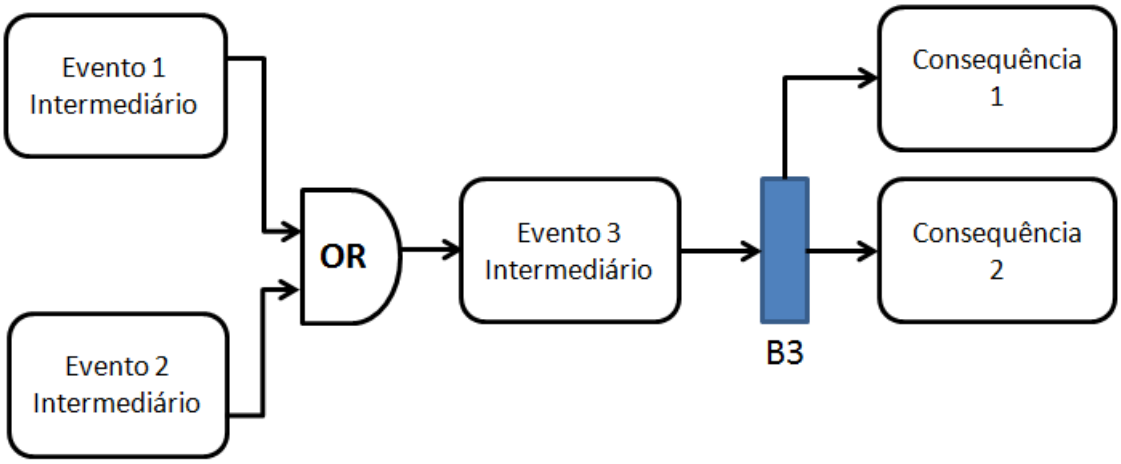
- **Operadores lógicos sobre os antecedentes** – quando há mais de uma condição antecedente sobre uma barreira, é possível aplicar os operadores da lógica de primeira ordem para estabelecer um modelo adequado de ativação das barreiras para cada caso. Por exemplo, na Figura 14 a "condição de demanda" para a barreira B3 é verdadeira, se as condições/eventos de ambas as barreiras B1 "e" B2 forem verdadeiras (requisição automática de que ambas as condições/eventos iniciais 1 e 2 devem ocorrer e ambas as barreiras B1 e B2 devem falhar). Por outro lado, existem casos onde vários eventos conduzem a uma mesma condição de perigo (ex: falha na energia "ou" falha mecânica "ou" perda de refrigeração conduzem a um aumento de temperatura no reator). Por esta razão, portas lógicas *OR* também devem ser consideradas, conforme ilustrado na Figura 15.

Figura 14 – Variação do diagrama de barreiras de segurança da Figura 10 e porta AND



Fonte: adaptado de (DUIJM, 2009).

Figura 15 – Diagrama de barreira de segurança com uma porta explícita OR



Fonte: adaptado de (DUIJM, 2009).

2.4 DIAGNOSTICABILIDADE SEGURA

A propriedade de diagnosticabilidade segura foi introduzida por Paoli e Lafortune (2005). Um sistema a eventos discretos (SEDs) é dito ter esta propriedade, se ele for diagnosticável(SAMPATH, SENGUPTA, *et al.*, 1995)(BAKOLAS e SALEH, 2011), ou seja, a detecção de uma falha ocorrer com atraso limitado, antes da execução de uma dada sequência de eventos proibitivos que violem os requisitos de segurança decorrente da ocorrência da falha.

Um SED é dito ser diagnosticável se um 'observador externo' puder inferir sobre o estado do SED, tendo este, alcançado um estado de perigo. Esta inferência é baseada na rastreabilidade de toda a sequência de eventos observáveis que o sistema executa(PAOLI e LAFORTUNE, 2005)(BAKOLAS e SALEH, 2011).

A observabilidade de falhas se faz de forma: (i) direta onde grandezas são coletadas diretamente de sensores e/ou (ii) indireta por meio de informações derivadas da manipulação sobre grandezas coletadas de sensores do sistema.

Sampath et. al. (1995) discutem as condições necessárias e suficientes para o diagnóstico de falhas em SEDs:

a. O(s) modelo(s) que descreve(m) o comportamento do sistema deve(m) ser 'vivo(s)', ou seja, para cada estado alcançado pelo sistema deve existir um evento que origina a transição de estados,

b. No(s) modelo(s) não deve(m) existir ciclo(s) de evento(s) não observáveis.

De acordo com (SALEH, MARAIS, *et al.*, 2010), vários relatórios de investigação de acidentes reportam a identificação de falhas 'ocultas' ou a 'não observabilidade' de falhas, durante a evolução de eventos críticos/indesejados, como fatores relevantes na ocorrência de acidentes catastróficos.

Quando o estado de um SCr não é monitorado ou disponibilizado e as técnicas de estimativa de estado não são empregadas, o SCr pode evoluir para um estado de risco e manter-se oculto do ponto de vista de observação por parte dos operadores e/ou sistemas de controle relacionados à segurança. Esta condição é referida como um acidente patogênico[10], como, por exemplo, a existência de uma falha 'oculta'

[10] Um acidente patogênio é quando uma condição latente adversa ou um estado de risco,

num elemento de um sistema de redundância. Um acidente patogênico é um elemento do vetor de estados do SCr, porém é invisível na saída do mesmo. Neste contexto, é importante que os acidentes patogênicos sejam diagnosticados, e que a informação de que um SCr evoluiu para um estado de risco seja disponibilizada para os operadores e/ou sistemas de controle relacionados à segurança, a fim de que ações sejam executadas para garantir a operação do SCr em segurança.

O princípio de defesa em profundidade tem sido criticado por alguns autores (PERROW, 1984)(ROCHLIN, LA PORTE e ROBERTS, 1998)(SALEH, MARAIS, *et al.*, 2010), em parte por contribuir para a ocorrência de falhas não observáveis. Uma vez que o princípio de defesa em profundidade é realizado por uma diversidade de barreiras de segurança, estas múltiplas linhas de defesa distribuídas ao longo da sequência de um acidente (cenário de um acidente), podem alavancar mecanismos ocultando a ocorrência de eventos, ou seja, as falhas críticas podem evoluir para um estado de perigo, de tal forma que um acidente possa estar prestes a ocorrer.

Neste contexto, Bakolas e Saleh (2011) abordam em seu trabalho, a deficiência do princípio de defesa em profundidade e propõem a propriedade de diagnosticabilidade segura como alternativa para resolver esta questão. Segundo os autores, se a propriedade de diagnosticabilidade segura não for considerada, a estratégia de prevenção e mitigação de falhas críticas baseada no princípio de defesa em profundidade, pode degenerar para uma estratégia de ‘defesa cega’, e sua eficiência pode ser degradada, ou pior, pode produzir efeitos negativos no SCr.

A propriedade de diagnosticabilidade segura requer que todos os eventos críticos que demandam as funções das barreiras de segurança sejam diagnosticados. Em termos simples, não deve existir ambiguidade na detecção e sinalização de falhas críticas quando as defesas forem violadas (ex: quando barreiras de segurança falham em suas funções) e o sistema evolui para um estado mais crítico(BAKOLAS e SALEH, 2011).

A propriedade de diagnosticabilidade segura não é proposta como uma alternativa para a estratégia de defesa em profundidade, uma vez que ela não atua sobre eventos adversos ou sequência de acidentes, que é o domínio das barreiras de segurança e do princípio de defesa em profundidade. Por outro lado, a

---

em associação com outros fatores, pode precipitar um acidente ou agravar suas consequências (BAKOLAS e SALEH, 2011).

propriedade de diagnosticabilidade segura fornece um conceito a ser considerado juntamente com o princípio de defesa em profundidade. A adoção desta propriedade aliada à defesa em profundidade pode potencializar os resultados de uma equipe envolvendo analistas de riscos, gestores de segurança, projetistas de sistemas, operadores e profissionais de manutenção; no sentido de maior eficácia na segurança de SCr e prevenção de acidentes em indústrias de processos(BAKOLAS e SALEH, 2011).

2.5 DIAGRAMA DE *BOWTIE*

Um modelo de acidente descreve a sequência de eventos e estados indesejados que precedem a ocorrência de um acidente, ou cenário de acidente(SKLET, 2004). De acordo com Badreddine e Ben Amor (2013), existem algumas técnicas para esta modelagem. Por exemplo: diagrama de barreiras de segurança (DUIJM, 2009), árvore de falhas (AF) e árvore de eventos (AE)(HENLEY e KUMAMOTO, 1981) e diagramas de *bowtie* (RUIJTER e GULDENMUND, 2016). Uma comparação entre estas técnicas pode ser encontrada em (NIVOLIANITOU, LEOPOULOS e KONSTANTINIDOU, 2004). Entre essas técnicas, os diagramas de *bowtie* têm provado ser eficientes na maioria das aplicações, tais como: (a) avaliação de riscos de acidentes(DELVOSALLE, FIEVEZ, *et al.*, 2006)(DIANOUS e FIEVEZ, 2006), (b) gestão de riscos(COCKSHOTT, 2005) e (c) implementação de barreiras de segurança(DIANOUS e FIEVEZ, 2006)(BADREDDINE e BEN AMOR, 2013).

Por outro lado, as organizações vêm se esforçando para compreender e controlar os riscos inerentes à operação de suas plantas ou processos. As tentativas em se obter uma visão global destes riscos, assim como, o gerenciamento dos mesmos, fez com que diferentes abordagens fossem desenvolvidas a fim de identificar e avaliar de forma sistemática estes riscos. O diagrama de *bowtie* é uma das abordagens que se tornou popular em SCr, como nas indústrias de petróleo e gás, aviação e mineração(RUIJTER e GULDENMUND, 2016).

2.5.1 Descrição do diagrama de *bowtie*

Diagramas de *bowtie* (do termo em inglês gravata borboleta devido a sua forma), têm sido largamente usados para a modelagem de acidentes, baseados em cada

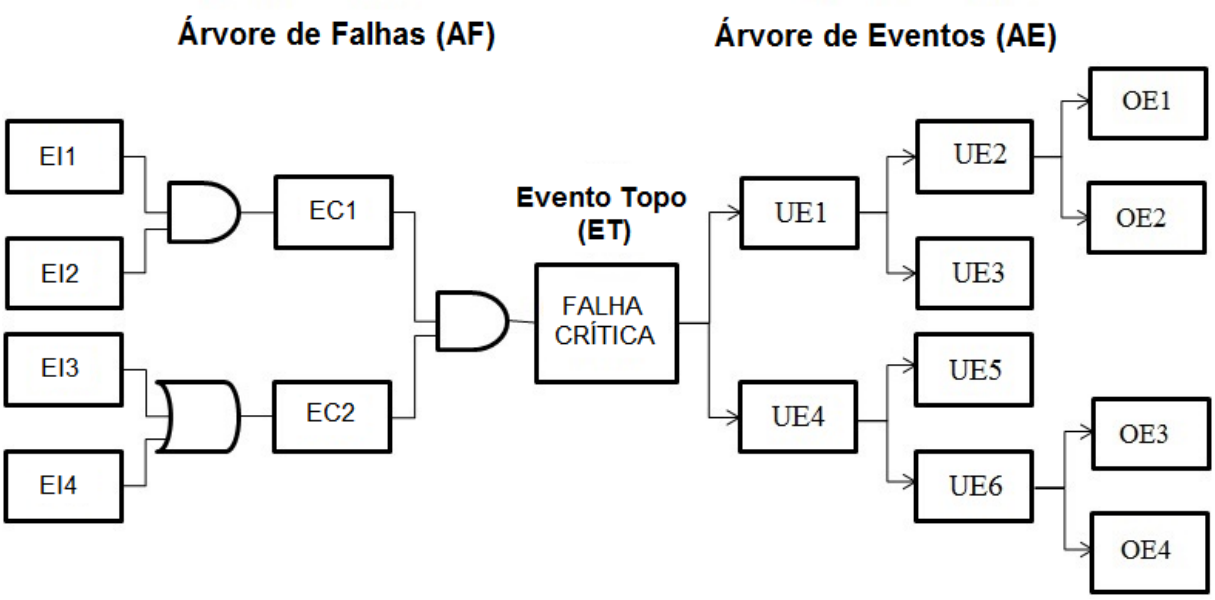
risco Ri identificado que também é chamado de evento topo (ET)(BADREDDINE e BEN AMOR, 2013) ou falha crítica neste trabalho. O diagrama de *bowtie* tem duas partes (Figura 16).

O lado esquerdo do diagrama representa a árvore de falhas (AF) que define todas as possíveis causas do ET. A AF representa graficamente o caminho das causas que conduzem à falha crítica. A falha crítica é o evento topo (ET) e as interações entre as diferentes causas são descritas por meio de portas lógicas. As causas são as razões fundamentais que resultam em falhas, mau funcionamentos, desvios de processos, ou erros humanos (FERDOUS, KHAN, *et al.*, 2013). Estas causas podem ser classificadas em dois tipos, conforme ilustra a Figura 16: (a) eventos críticos (EC), os quais são as principais causas do ET, e (b) eventos iniciadores (IE) que são as causas do EC. Além disso, embora tecnicamente as portas lógicas da AF existam, a descrição de cenários não usam propriamente a lógica booleana, e estão mais diretamente relacionadas às relações de causa e efeito entre os eventos, descrevendo o cenário completo num nível mais elevado(RUIJTER e GULDENMUND, 2016).

O lado direito do diagrama representa a árvore de eventos (AE) que define e sequencia dos possíveis eventos indesejados e consequências do ET. Os eventos pertinentes a este lado são também classificados em dois tipos, conforme ilustra a Figura 16: (a) eventos indesejados (UE), os quais são as principais consequências do ET, e (b) resultados indesejados (OE), os quais representam os resultados provenientes de uma propagação sistemática de eventos a partir do ET(FERDOUS, KHAN, *et al.*, 2013).

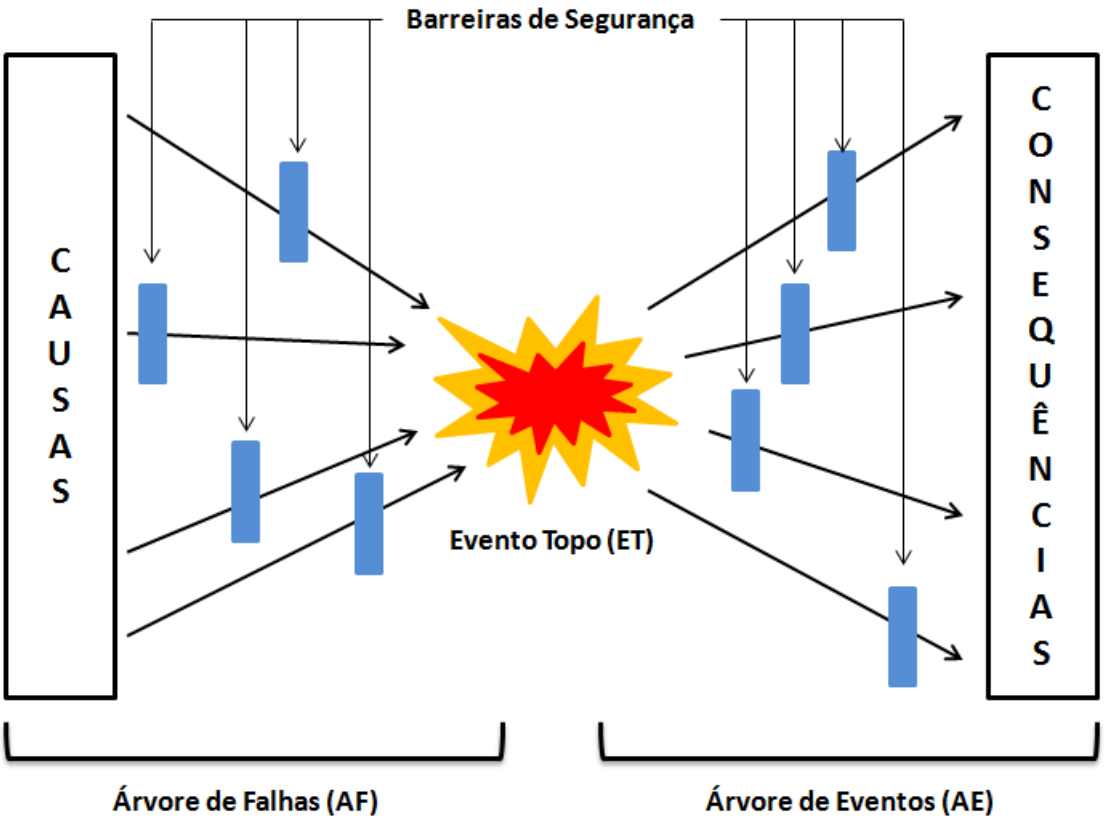
Os diagramas de *bowtie* são usados para a identificação e implementação de barreiras de segurança para a prevenção do ET e para a mitigação dos efeitos provenientes da ocorrência do ET (MARKOWSKI, MANNAN e BIGOSZEWKA, 2009)(RUIJTER e GULDENMUND, 2016). A Figura 17 ilustra a identificação das barreiras de segurança no diagrama de *bowtie*.

Figura 16 – Diagrama de *bowtie*



Fonte: adaptado de (BADREDDINE e BEN AMOR, 2013)

Figura 17 – Identificação das barreiras de segurança no diagrama de *bowtie*



Fonte: adaptado de (RUIJTER e GULDENMUND, 2016)

2.5.2 Construção dos diagramas de *bowtie*

Ruijter e Guldenmund (2016) fazem uma revisão da literatura sobre diferentes abordagens usadas para a construção do diagrama de *bowtie*. Uma das questões discutida pelos autores, é a incerteza inerente à modelagem envolvida. Os diagramas de *bowtie* são usualmente construídos baseado no conhecimento de especialistas. O resultado é que os diagramas gerados são subjetivos e podem não representar a realidade.

Dentre as abordagens que utilizam técnicas de Inteligência Artificial (IA), Badreddine e Ben Amor (2013) usam a técnica de aprendizagem de redes bayesianas para construir e validar o diagrama de *bowtie* com base em bancos de dados. Além disso, Ferdous *et al*.(2013), usam lógica fuzzy e teoria de evidência para estimar o nível de incerteza que está presente dentro da estrutura de *bowtie* e para agregar conhecimento ao diagrama a partir de múltiplos especialistas.

2.6 IMPUTAÇÃO DE DADOS

Na prática, a maioria dos bancos de dados nas indústrias de processos são incompletos e, assim, este é um problema inevitável(LAKSHMINARAYAN, HARP e SAMAD, 1999). Frequentemente estes bancos de dados apresentam dois tipos de variáveis: (i) faltantes (do termo inglês *missing*), cujos dados são algumas vezes “observados” e gravados no banco de dados, e algumas vezes “não observados” e não gravados no banco de dados; e (ii) ocultas (do termo inglês *hidden*), cujos dados nunca foram observados e gravados no banco de dados(SINGH, 1998).

Por outro lado, utilizando métodos estatísticos é possível utilizar os dados do bancos de dados para inferir conclusões sobre um determinado fenômeno. Entretanto, determinar a abordagem analítica adequada para conjuntos de dados com observações incompletas é uma questão delicada, pois a utilização de métodos inadequados pode resultar em inferências erradas sobre um determinado fenômeno(NUNES, KLUCK e FACHEL, 2009).

Para contornar esse problema, desde os anos 80 surgiram técnicas estatísticas que envolvem a imputação de dados faltantes. Essas técnicas têm por objetivo, “preencher” os dados faltantes e possibilitar a análise do conjunto de dados, agora completo. As primeiras técnicas de imputação desenvolvidas, envolviam métodos relativamente simples, tais como, substituição dos dados faltantes pela média, pela mediana, por interpolação ou até por regressão linear dos dados observados(NUNES, KLUCK e FACHEL, 2009). Todas essas técnicas permitem “preencher” os dados faltantes por meio do que se chama de imputação única (IU), ou seja, o dado ausente é preenchido uma única vez e então se utiliza o banco de dados completo para as análises. Entretanto, a incerteza associada à IU deve ser levada em conta, para que os resultados obtidos sejam válidos, pois os valores imputados não são valores de fato, observados. Para solucionar essa questão foi desenvolvida a técnica de imputação múltipla (IM)(RUBIN, 1987).

Para se utilizar os métodos de imputações descritos na literatura, é necessário considerar alguns “padrões de dados ausentes” e “mecanismos de dados ausentes” que foram definidos por (RUBIN, 1976).

Os padrões de dados ausentes se referem à forma com que os dados faltantes estão distribuídos em um conjunto de dados, porém não se explica porque os dados

são faltantes. Já os mecanismos de dados ausentes descrevem possíveis relações entre as variáveis observadas e a probabilidade de dados faltantes, informando a causa da ausência(SILVA, 2012)(ENDERS, 2010).

2.6.1 A distribuição de dados ausentes – Teoria de Rubin

Segundo a teoria de Rubin (1976), o conjunto de dados completos representados por $\mathbf{Y}_{com}$ podem ser divididos em valores observados $\mathbf{Y}_{obs}$ e valores que não foram observados $\mathbf{Y}_{aus}$, ou seja,

$$\mathbf{Y}_{com} = (\mathbf{Y}_{obs}, \mathbf{Y}_{aus})$$

Seja uma matriz de dados retangular ($n \times p$), sendo as unidades (i = 1,2,...,n), uma amostra aleatória de alguma distribuição de probabilidade multivariada p-dimensional e as unidades (j = 1,2,...,p), as variáveis desta matriz. Os valores das variáveis respostas para o i-ésimo indivíduo estão agrupadas em um vetor $\mathbf{Y}_i = (Y_{i1}, Y_{i2}, ..., Y_{ip})^T$. Considerando uma variável da matriz de dados multivariada p-dimensional, observa-se que

$$\mathbf{Y}_{i1} = \{Y_{11}, Y_{21}, ..., Y_{n1}\} = \{Y_{11}, Y_{21}, Y_{r1}, Y_{r1+1}, ..., Y_{n1}\}$$

No qual $\mathbf{Y}_{obs} = \{Y_{11}, Y_{21}, Y_{r1}\}$ corresponde aos valores que foram observados e $\mathbf{Y}_{aus} = \{Y_{r1+1}, ..., Y_{n1}\}$ referem-se aos valores ausentes da variável. Desta forma o conjunto de dados contém r valores observados e $m = n - r$ valores ausentes. Para estudar o comportamento dos dados ausentes, o autor cria uma variável indicadora **R** que fornece uma distribuição de probabilidade de falta completa, ou seja, uma distribuição de probabilidade indicando se $\mathbf{R}_i$ assume o valor 1 ou 0. Também conhecida como distribuição indicadora.

$$\mathbf{R} = \begin{cases} 1, \text{se } Y_{ij} \text{ é observado;} \\ 0, \text{se } Y_{ij} \text{ é não observado.} \end{cases}$$

Esta distribuição depende da forma com que os dados ausentes se distribuem ao longo da matriz de dados, quando o indivíduo não apresentar resultado sobre a variável em estudo ele receberá o valor 0, caso contrário será representado pelo valor 1. Tal distribuição será importante quando se pretende verificar a causa da falta de dados. Por meio dos “mecanismos de dados ausentes” pode-se verificar as relações entre os valores ausentes e a probabilidade de ausência, informando o que gerou esta ausência, os quais são descritos na subseção 2.6.3.

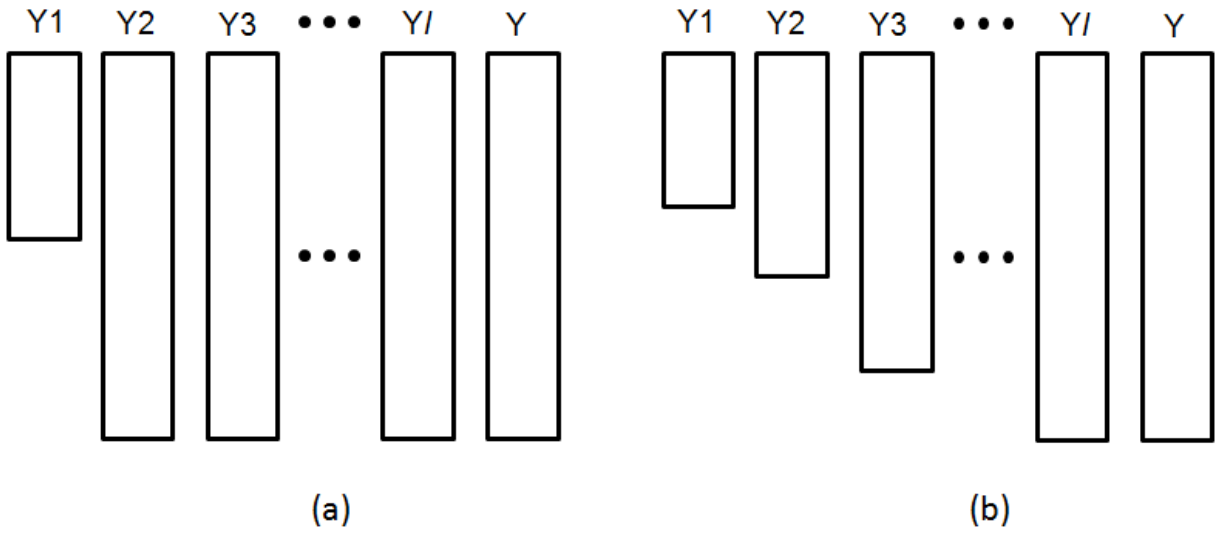
2.6.2 Padrões de dados ausentes

Muitos conjuntos de dados podem ser arranjados na forma de matriz, onde as linhas são as instâncias e as colunas são as variáveis. Com esse tipo de arranjo é possível identificar padrões de dados ausentes, como ilustrado na Figura 18. Quando ocorrem dados faltantes em somente uma das variáveis (o dado faltante pode ocorrer tanto nas variáveis preditoras como na variável resposta), configura-se o padrão univariado (Figura 18a) que é um caso especial de padrão monotônico. Quando há dados faltantes em mais do que uma variável e é possível organizar os dados conforme ilustra a Figura 18b, ou seja, as colunas podem ser arranjadas de tal forma que $\mathbf{Y}_{j+1}$ é observado para todo caso que é observado em $\mathbf{Y}_j$, temos o padrão monotônico.(RUBIN, 1987)(SCHAFER e GRAHAM, 2002)(NUNES, 2007).

A Figura 19a ilustra um padrão onde duas variáveis (por exemplo, $\mathbf{Y}_1$ e $\mathbf{Y}_2$) nunca são observadas juntas. Tais dados originam-se quando duas amostras contendo observações em $\mathbf{Y}_1$ e $\mathbf{Y}$ e $\mathbf{Y}_2$ e $\mathbf{Y}$ são unidas em um só banco de dados.

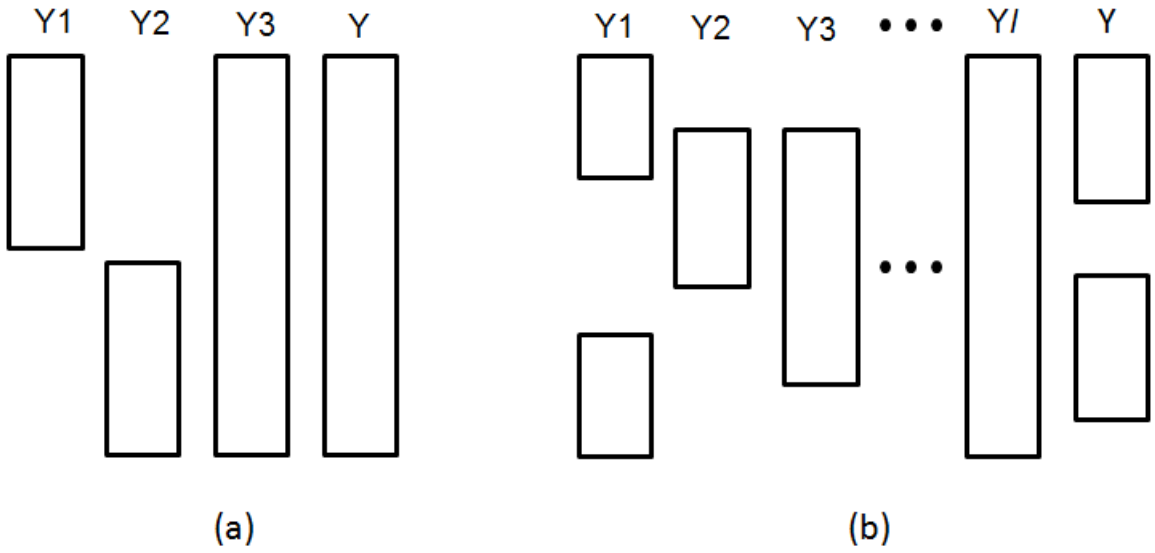
As estimativas a partir desse padrão requerem suposição (explícita ou implícita) sobre a associação condicional de $\mathbf{Y}_1$ e $\mathbf{Y}_2$, dado $\mathbf{Y}_3$ e $\mathbf{Y}$. E por fim, a Figura 19b representa um padrão geral sem estrutura, também conhecido como padrão arbitrário(RUBIN, 1987)(SCHAFER e GRAHAM, 2002)(NUNES, 2007). Estes casos da Figura 19 são padrões não monotônicos de ausência de dados.

Figura 18 – Padrão monotônico de ausência de dados



Fonte: adaptada de (NUNES, 2007)

Figura 19 – Padrão não monotônico de ausência de dados



Fonte: adaptada de (NUNES, 2007)

2.6.3 Mecanismos de dados ausentes

Diferentemente dos “padrões de dados ausentes”, os “mecanismos de dados ausentes” descrevem as relações entre os dados faltantes e a probabilidade de ausência, informando a causa da falta dos dados. Quando se tem dados ausentes em uma matriz de dados, o pesquisador ou analista deve avaliar o mecanismo que as gerou, identificá-lo e considerá-lo na análise de dados, caso contrário, as inferências estatísticas podem não ser válidas. Os mecanismos de dados faltantes citados por (RUBIN, 1987) são:

(a) Dado faltante completamente aleatório – MCAR (*Missing Completely at Random*)

A ausência ocorre de forma totalmente aleatória, isto é, a probabilidade da falta de dados sobre a variável **Y** não está relacionada com alguma outra variável medida e não tem relação com os valores de **Y**. Sua distribuição indica que existe algum parâmetro Θ importante para a probabilidade de que **R** assuma um valor 0 ou 1, porém a falta completa (**R**) não está relacionada com isto. Esta distribuição pode ser escrita como:

$$P(\mathbf{R}|,\Theta)$$

Os dados faltantes pertinentes a este mecanismo, normalmente são derivados de fatores externos, tais como falhas de dispositivos (ex: sensores), entre outros.

(b) Dado faltante aleatório – MAR (Missing at Random):

A ausência de dados ocorre de forma aleatória, isto é, a probabilidade da falta de dados sobre a variável **Y** depende das informações disponíveis na matriz de dados que contém as variáveis medidas. Em muitas situações experimentais esta ausência não é completamente aleatória. Sua distribuição indica que a probabilidade de falta completa (**R**) depende da proporção dos dados observados ($\mathbf{Y}_{obs}$), por meio de algum parâmetro Θ que relaciona **Y** e **R**, assim a distribuição pode ser escrita como:

$$P(\mathbf{R} \mid \mathbf{Y}_{obs}, \Theta)$$

(c) Dado faltante não aleatório – NMAR (Missing Not a Random):

Quando a ausência de dados depende das informações que não foram observadas ($\mathbf{Y}_{aus}$), não é mais considerada aleatória. Outro caso seria quando a ausência de dados depende da variável em si. A distribuição de dados em falta, indica a probabilidade de falta completa (**R**) assumir um valor de 0 ou 1 dependendo de $\mathbf{Y}_{obs}$ e $\mathbf{Y}_{aus}$. Esta distribuição pode ser escrita como:

$$P(\mathbf{R} \mid \mathbf{Y}_{obs}, \mathbf{Y}_{aus}, \Theta)$$

2.6.4 Procedimentos de Imputação Única

A imputação única (IU), engloba métodos relativamente simples para substituição de dados faltantes, isto é, os dados faltantes são substituídos uma única vez por métodos como: (i) Substituição por um valor de tendência central, (ii) *Hot deck*, (iii) Regressão (média predita), (iv) Estimativa de Máxima Verossimilhança (algoritmo EM) e (v) métodos de imputação única para dados longitudinais. Uma descrição detalhada destes métodos pode ser encontrada em (NUNES, 2007).

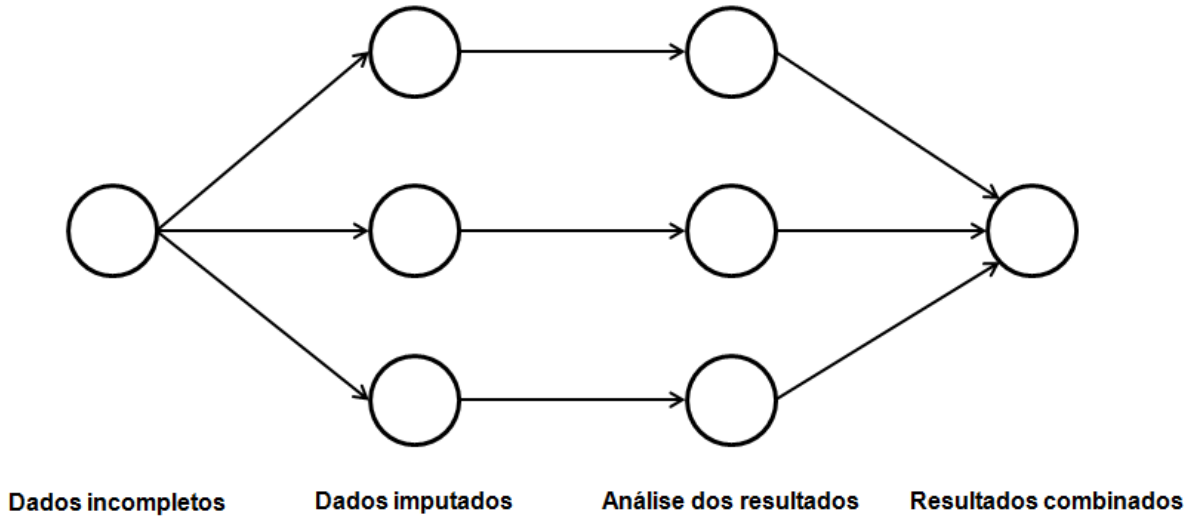
2.6.5 Imputação Múltipla

A imputação múltipla (IM) é uma técnica estatística, proposta inicialmente por (RUBIN, 1976) para resolver o problema de “não reposta” em coleta de dados estatísticos. No entanto, apenas recentemente esta técnica vem sendo mais utilizada devido ao desenvolvimento de ferramentas computacionais para implementação da mesma. Esta técnica possibilita, além da estimativa pontual dos dados faltantes, a consideração da incerteza, provocada pelo processo de imputação dos dados, na variância dos resultados estimados, corrigindo o maior problema associado à IU (RUBIN, 1987)(NUNES, 2007).

Basicamente, a IM consiste de três passos, conforme ilustra a Figura 20:

1. São obtidos **m** (em geral, **m** fica entre 3 e 10) bancos de dados completos via técnicas adequadas de imputação;
2. Separadamente, os **m** bancos de dados são analisados por um método estatístico tradicional, como se realmente fossem conjuntos completos de dados; e
3. Os **m** resultados encontrados no passo 2 são combinados de um modo simples e apropriado para se obter a chamada inferência da imputação repetida.

Figura 20 – Passos da Imputação Múltipla



Fonte: adaptada de (BUUREN e OUDSHOORN, 2011)

O primeiro passo é a parte fundamental da IM, pois as técnicas de imputação utilizadas têm que preservar a relação entre os dados faltantes (não observados) e

os dados observados, isto é, levar em conta o “mecanismo de dados ausentes” (MCAR, MAR ou NMAR) e o “padrão de dados ausentes” (monotônicos ou não monotônicos).

A partir das **m** imputações realizadas, no caso da Figura 20 são consideradas **m**=3, o segundo passo pode ser realizado, ou seja, os **m** bancos de dados são analisados por métodos tradicionais de análise. Finalmente, os **m** resultados obtidos podem ser combinados, usando-se as regras propostas por (RUBIN, 1987). Uma descrição formal e detalhada do algoritmo de IM pode ser encontrada em (HORTON e LIPSITZ, 2001).

Ainda segundo (HARREL JR, 2001) é possível serem definidas linhas gerais para a escolha entre os métodos de imputação de acordo com a proporção de dados faltantes em qualquer uma das variáveis, ou seja:

(a) Proporção ≤ 0,05 → Neste caso pode ser usada IU ou analisar somente os dados completos (abordagem baseada na desconsideração de dados faltantes).

(b) Proporção entre 0,05 e 0,15 → Imputação única pode ser usada sem problemas, entretanto, o uso da imputação múltipla é recomendado.

(c) Proporção ≥ 0,15 → A imputação múltipla é indicada na maior parte dos casos.

Para a implementação da técnica de imputação, alguns aplicativos têm sido citados na literatura. Dentre os mais utilizados, pode-se citar por exemplo o SAS, S-Plus, SOLAS, NORM, MPlus e MICE.

O algoritmo de imputação multivariada baseada em equações encadeadas (MICE: *multivariate imputation by chained equations*), desenvolvida por (BUUREN e OUDSHOORN, 2011), é um dos algoritmos que implementa a técnica de IM. Dentre as características deste algoritmo pode-se citar: (i) a introdução de seleção de preditores, (ii) seleção de métodos de imputação, (iii) combinação automática das imputações, (iv) preservação das relações entre os dados, e (v) preservação da incerteza sobre tais relações.

O algoritmo permite lidar com diferentes tipos de dados (ex: binário (categórico com fator = 2), não ordenado, ordenado e contínuo)(BUUREN e OUDSHOORN, 2011).

O processo de imputação múltipla de dados via MICE é feito com base em diferentes métodos. A descrição detalhada destes métodos é encontrada em (BUUREN e OUDSHOORN, 2011). Dentre os métodos citados, o *Predictive Mean Matching* (PMM) é um método de propósito geral, adequado para a maioria das distribuições probabilísticas e que apresenta bons resultados, pois suas virtudes principais são: (i) as imputações são restritas aos valores observados das variáveis envolvidas no domínio, e (ii) os dados imputados preservam uma relação de não linearidade.

Uma das grandes vantagens em se utilizar o MICE é que ele manipula dados faltantes para o padrão não monotônico, usando equações encadeadas, via método de Monte Carlo, via Cadeias de Markov (MCMC). Adicionalmente, o MICE permite: (i) selecionar um dos modelos de imputação, (ii) a transformação de variáveis, e (iii) a escolha dos preditores no modelo de imputação. O passo de imputação é executado usando a função mice( ). Para dados faltantes do tipo contínuo, MICE suporta imputação usando o método norm (regressão linear bayesiana) e o método pmm (predictive mean matching). Banco de dados com valores imputados são obtidos usando a função complete( ). Finalmente, os resultados podem ser combinados usando a função pool( ) (HORTON e LIPSITZ, 2001).

As aplicações deste algoritmo são extensas em diversos campos, como por exemplo, na medicina (ex: artrites e reumatologia, aterosclerose, sistema cardiovascular, câncer, epidemiologia, endocrinologia, doenças infecciosas, etc); na economia; pediatria; reprodução humana; ciências da gestão; segurança ocupacional; política; psicologia; sociologia e na engenharia. Uma relação detalhada das citações dos trabalhos realizados pode ser encontrada em (BUUREN e OUDSHOORN, 2011).

2.7 REDE BAYESIANA

A rede bayesiana (RdB) combina a teoria dos grafos(HARARY, 1969) e a teoria da probabilidade(CASTILHO, GUTIÉRREZ e HADI, 1997). A RdB possui dois componentes principais: (a) uma estrutura ***S***, que define o relacionamento qualitativo causal entre os nós, e (b) parâmetros numéricos **Θ**, que quantificam a relação

probabilística causal entre os nós da estrutura ***S***, conforme representado na equação (1).

$$\mathrm{RdB} = (\boldsymbol{S}, \boldsymbol{\Theta}) \quad (1)$$

2.7.1 Formalização

Uma RdB representa uma distribuição conjunta de probabilidade *P* sobre um conjunto de variáveis aleatórias $X = \{X_1, X_2, ..., X_n\}$. De acordo com (OCHOA-LUNA e ZANUSSO, 2005), uma estrutura ***S*** para *X*, codifica as assertivas de independência condicional sobre as variáveis no conjunto *X*, enquanto que, a instância de **Θ** codifica as probabilidades condicionais associadas às variáveis em *X*. Juntos, a estrutura ***S*** e os parâmetros **Θ** definem uma distribuição de probabilidades conjunta, tal que:

(i) ***S*** é um grafo acíclico orientado (GAO);

(ii) Os nós em ***S*** estão numa relação 1-1 com as variáveis em *X*;

(iii) Cada variável X_i, em *X*, denota uma variável e também o correspondente nó em ***S***;

(iv) $Pa(X_i)$ denota os nós pais de X_i, e também as variáveis correspondentes a esses pais;

(v) A distribuição de probabilidade conjunta de *X* é dada pela equação (2)

$$P(X) = \prod_{i=1}^{n} P(X_i \,|Pa(X_i)) \quad (2)$$

onde:

- $P(X)$ é a distribuição de probabilidade conjunta de $X = \{X_1, X_2, ..., X_n\}$;

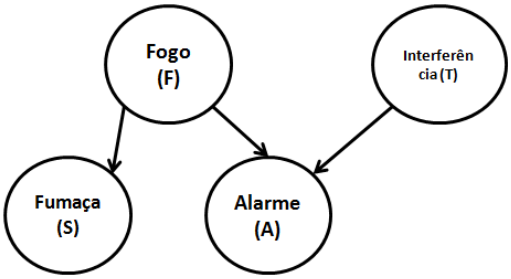
Um exemplo de RdB é ilustrado na Figura 21.

Figura 21 – Exemplo de uma rede bayesiana

Suposições		Probabilidade condicional
Fogo (F)	Fumaça (S)	Θ
verdadeiro	verdadeiro	0.90
falso	verdadeiro	0.01

Suposições			Probabilidade condicional
Fogo (F)	Interferência (T)	Alarme (A)	Θ
verdadeiro	verdadeiro	verdadeiro	0.500
verdadeiro	falso	verdadeiro	0.990
falso	verdadeiro	verdadeiro	0.850
falso	falso	verdadeiro	0.001

(a)



(b)

Fonte: adaptada de (DARWICHE, 2010)

A Figura 21b ilustra a estrutura ***S*** e estabelece a influência causal das variáveis F e T sobre as variáveis S e A. A Figura 21a ilustra o conjunto de probabilidades condicionais da variável S em relação à sua variável pai – F, assim como, o conjunto de probabilidades da variável A em relação aos seus pais F e T. Os parâmetros **Θ** correspondem a este conjunto de probabilidades condicionais.

2.7.2 Aplicações em sistemas relacionados à segurança

As RdB vêm sendo usadas como uma técnica de inferência para expressar as relações causais entre as variáveis dentro de um determinado domínio(DALY, SHEN e AITKEN, 2011)(WEBER, MEDINA-OLIVE, *et al.*, 2012)(SQUILLANTE JR, SANTOS FO, *et al.*, 2013)(BADREDDINE e BEN AMOR, 2013). As RdBs são usadas ou para predizer a probabilidade de variáveis desconhecidas, ou para atualizar a probabilidade de variáveis conhecidas, dados certos estados de outras variáveis (denominadas de evidências), via processo de propagação de probabilidade ou raciocínio. O raciocínio neste caso é baseado no teorema de *Bayes*, e esta é uma característica muito importante para análise da segurança de sistemas e gerenciamento de riscos(KHAKZAD, KHAN e AMYOTTE, 2011).

(WEBER, MEDINA-OLIVE, *et al.*, 2012) apresentam uma revisão bibliográfica de aplicações das RdBs em diferentes áreas, tais como, análise e manutenção de

riscos, os quais são qualitativamente comparados com outros métodos tradicionais, tais como: árvore de falha (AF), árvore de eventos (AE), cadeia de *Markov*, e rede de Petri.

As técnicas baseadas em AF e AE utilizadas para a construção dos diagramas de *bowtie* (modelos de acidente), resultam em estruturas estáticas. Com isto, as informações coletadas em tempo real não podem ser aplicadas ao diagrama para a atualização das probabilidades(BOBBIO, A; PORTINALE, L.; MINICHINO, M.; E.CIANCAMERLA, 2001)(KHAKZAD, KHAN e AMYOTTE, 2011). Abordagens baseadas em RdB e bancos de dados completos foram então propostas para modelagem de acidentes para superar as limitações do diagrama de *bowtie*(BADREDDINE e BEN AMOR, 2013)(RUIJTER e GULDENMUND, 2016).

Os resultados mostram que as RdBs têm se mostrado efetivas para casos onde é necessário considerar informações que são atualizadas em tempo real.

2.7.3 Aprendizagem de Redes Bayesianas

Os dois componentes de uma RdB: (i) a estrutura **S** e (ii) os parâmetros numéricos **Θ**, podem ser aprendidos indutivamente a partir de dados de um banco de dados. Primeiro deriva-se a estrutura S, com base nas informações disponíveis, e a seguir, com a estrutura conhecida, se adota um processo de aprendizagem dos parâmetros numéricos **Θ** (OCHOA LUNA, 2004).

De acordo com (FRIEDMAN, 1997), uma das motivações da aprendizagem das RdB a partir de dados de um banco de dados, é que a elicitação das RdB a partir de especialistas, pode ser um processo laborioso e de alto custo em grandes aplicações.

O problema da aprendizagem de uma RdB a partir de dados de um banco de dados pode ser definida da seguinte forma: Dado um banco de dados de treinamento $D = \{x^1, ... ,x^N\}$ de instâncias de $X = \{X_1, X_2, ..., X_n\}$, procurar por uma RdB = [**S**, **Θ**] que melhor represente *D*.

Existem alguns métodos para construção de RdBs: (a) baseada no próprio conhecimento do projetista e / ou conhecimento de outros especialistas onde se explora percepções humanas sobre influencias causais, (b) baseada em aprendizagem de estruturas **S** e parâmetros **Θ**, de maneira indutiva, a partir de um

banco de dados de treinamento (BADREDDINE e BEN AMOR, 2013)(OCHOA-LUNA e ZANUSSO, 2005)(FRIEDMAN, 1997). De fato, as duas abordagens são recomendadas para a construção de uma “boa” RdB(RIASCOS, SIMOES e MIYAGI, 2007).

Os bancos de dados para treinamento de RdB podem ser classificados em duas classes: (i) dados completos: matriz de variáveis observadas em todas as instâncias do banco de dados, e (ii) dados faltantes: matriz que contém dados faltantes para variáveis em algumas instâncias do banco de dados. De acordo com (OCHOA-LUNA e ZANUSSO, 2005), existem quatro casos de aprendizagem de RdB de forma indutiva a partir de um banco de dados de treinamento: (1) estrutura conhecida e dados completos; (2) estrutura conhecida e dados faltantes; (3) estrutura não conhecida e dados completos; e (4) estrutura não conhecida e dados faltantes.

Existem abordagens que lidam com a técnica de aprendizagem de parâmetros **Θ** e estruturas **S**, a partir de bancos de dados com dados faltantes, como por exemplo o algoritmo *Expectation Maximization* (EM) (FRIEDMAN, 1998)(FRIEDMAN, 1997)(OCHOA LUNA, 2004). Entretanto, essas abordagens apresentam um resultado satisfatório apenas quando lidam somente com a aprendizagem de parâmetros **Θ** - a partir de um banco de dados incompleto e quando se conhece a estrutura **S**; tornando o processo de aprendizagem de parâmetros **Θ** relativamente simples. Por outro lado, a aprendizagem de estrutura **S** de uma RdB é um assunto, em geral, complexo e ainda não está bem resolvido(OCHOA LUNA, 2004). Adicionalmente, (ZHANG, 2003) argumenta que as abordagens que lidam com a aprendizagem de RdB a partir de dados faltantes, podem apresentar também complicações computacionais, sendo complexa a sua implementação, assim como, a acurácia das inferências pode ser prejudicada devido a presença de dados faltantes(ZHANG, 2003).

Por sua vez, grafos com estrutura de árvore possuem a mesma semântica das árvores de falha (AF) e de eventos (AE). Nas AF os `arcos` relacionam as variáveis de um domínio (causas) com a variável raiz (ET); enquanto que, nas AE, os `arcos` são orientados da variável raiz (ET) para as demais variáveis do domínio (efeitos) (BADREDDINE e BEN AMOR, 2013).

O problema da aprendizagem de estrutura de RdB na forma de árvore, foi inicialmente proposto por (CHOW e LIU, 1968). Ainda de acordo com Badreddine e

Ben Amor (2013), as AF e AE, e consequentemente os diagramas de *bowtie*, podem ser formuladas como: dada uma distribuição conjunta na forma de árvore T_d e um banco de dados de treinamento BDT de N observações (ex: BDT = $\{x_1, x_2, ..., x_N\}$, onde x_i é a i-ésima observação relativa a todas as variáveis em BDT), busca-se por uma árvore *Tr* que maximiza o logaritmo da verossimilhança dos dados de acordo com a equação (3).

$$Tr = \arg\max \sum_{i=1}^{N} \log T_d(x_i) \qquad (3)$$

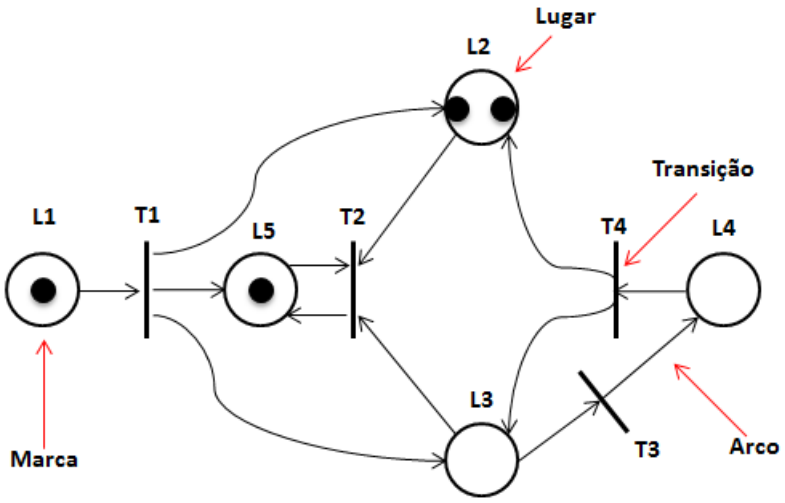
Existem atualmente ferramentas computacionais para modelagem de grafos probabilísticos tais como as RdBs. Por exemplo, a ferramenta Hugin® permite a fusão do conhecimento humano com a aprendizagem por indução a partir de dados de um domínio. Dentre as capacidades e recursos desta ferramenta, pode-se elencar: (i) aprendizagem da estrutura **S** via algoritmo de *Chow e LiuTree* entre outros algoritmos; (ii) estimativa de parâmetros **Θ**, no caso de utilização de bancos de dados com dados faltantes; e (iii) adaptação de parâmetros **Θ** das RdBs. As funcionalidades desta ferramenta podem ser encontradas em (MADSEN, LANG, *et al.*, 2003). Uma versão de demonstração gratuita (*Hugin® Lite*) pode ser baixada em *http://www.hugin.com*.

2.8 REDE DE PETRI

A Rede de Petri (RdP) é uma técnica de modelagem gráfica e matemática desenvolvida por Carl Adam Petri em sua tese de doutorado "*Kommunikation mit Automaten"* na Universidade de Darmstad, na antiga Alemanha Ocidental em 1962(BRAUER e REISIG, 2006). Desde então, ela tem sido utilizada para a modelagem e análise de sistemas concorrentes, assíncronos, distribuídos e paralelos(MURATA, 1989)(CARDOSO e VALETTE, 1997). A RdP também tem sido usada na modelagem e análise de diferentes tipos de aplicações, tais como: protocolos distribuídos(KANESHIRO, 2008), aplicações industriais(ZURAWSKI e ZHOU , 1994), diagnóstico e tratamento de falhas (RIASCOS, 2002)(MORALES, MELO e MIYAGI, 2007)(SQUILLANTE JR, 2011), entre outras. A RdP é de compreensão relativamente fácil e simples devido a sua representação gráfica, se comparada a outras técnicas de modelagens de sistemas a eventos discretos (SEDs). Outro diferencial desta técnica é a possibilidade de conversão dos modelos para programas de controladores lógicos programáveis.

Um modelo em RdP é um grafo composto de `lugares` representados por círculos, `transições` representadas por barras, `arcos orientados` interligando os componentes anteriores e `marcas` que são utilizadas para definir o estado de uma RdP. Um modelo em RdP é considerado como grafo orientado e bipartido (Figura 22), pois existe a restrição de que os `arcos` só interligam elementos de natureza diferente (MURATA, 1989)(PETERSON, 1981).

Figura 22 – Representação de uma Rede de Petri



Fonte: (PETERSON, 1981)

2.8.1 Production Flow Schema

De acordo com (MIYAGI, 2007), *Production Flow Schema* (PFS) é uma técnica desenvolvida para sistematizar e facilitar a modelagem de estratégias de controle de SEDs. O PFS é uma extensão da RdP canal-agência(REISIG, 1985) para sistemas produtivos discretos, sendo possível aplicá-la também para atividades que sejam dirigidas por eventos e que ocorrem nas indústrias de processos.

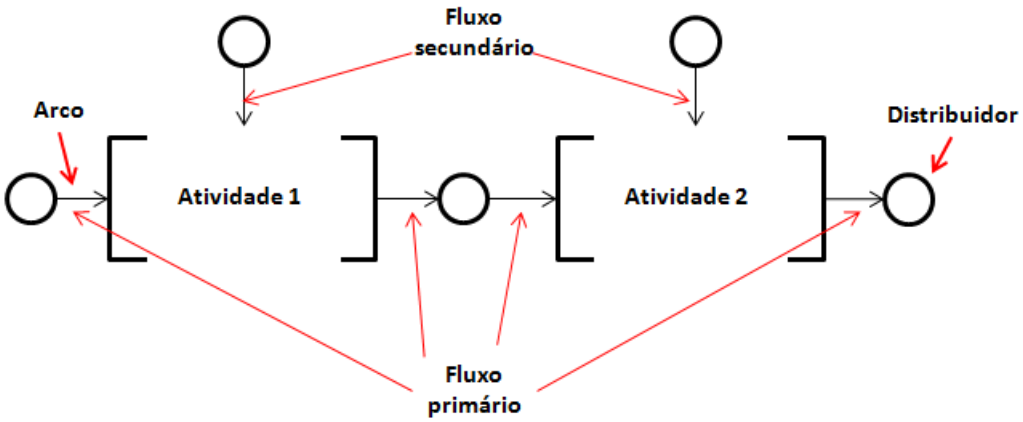
Constitui uma técnica para desenvolver uma descrição estrutural e comportamental de um sistema, a partir de uma visão conceitual em um nível alto de abstração. O PFS baseia-se no uso da técnica de refinamentos sucessivos, através de uma abordagem *top-down*, de maneira que seja possível inserir progressivamente no modelo o detalhamento dos processos do sistema. O objetivo é representar o fluxo de atividades pertinente à evolução de um determinado processo. A partir do PFS, outro modelo pode ser gerado em RdP para descrever o comportamento dinâmico detalhado do sistema de forma sistemática(JUNQUEIRA e MIYAGI, 2006). Os elementos do PFS, ilustrados na Figura 23, são os seguintes:

(i) Elementos ativos chamados `atividades`: representam um subprocesso ou um componente ativo do sistema capaz de realizar transformações. As `atividades` podem agregar uma ou mais operações e pode ser refinada em `subatividades`. Correspondem a um macro elemento delimitado por "[" e "]" que representam o início e o final de uma atividade, respectivamente.

(ii) Elementos passivos chamados `distribuidores`: representam componentes passivos, capazes de armazenar itens (materiais ou informações), e indicar determinados estados ou tornar os itens visíveis. É indicado graficamente por uma circunferência. Entre duas atividades sempre existe um elemento `distribuidor`.

(iii) `Arcos` que conectam `atividades` e `distribuidores` representando o fluxo de itens (materiais e/ou informações), explicitam uma relação lógica entre estes elementos. No PFS têm-se os fluxos primários, que estão conectados diretamente aos símbolos "[" e "]", e os fluxos secundários, que estão conectados à parte interna da `atividade` (a representação deste fluxo é opcional).

Figura 23 – Elementos do PFS



Fonte: próprio autor

Portanto, o PFS é uma técnica de modelagem para especificação de sistemas em nível conceitual e é efetiva como base para a derivação de modelos em RdP. Uma vez obtidos estes modelos, pode-se analisar a dinâmica do sistema modelado com base em propriedades do modelo como: limitabilidade, reiniciabilidade e vivacidade(CARDOSO e VALETTE, 1997).

2.9 SÍNTESE DO CAPÍTULO

Neste trabalho é proposta uma reclassificação de barreiras de segurança apresentada por Sklet (2006), endereçando a questão da prevenção e mitigação de eventos críticos e/ou indesejados, e que considera o uso da tecnologia de sistemas instrumentados de segurança (SIS) em substituição da operação humana. A reclassificação faz uso do conceito de sistemas reativos, do princípio de defesa em profundidade e da propriedade de diagnosticabilidade segura.

No que diz respeito à execução da função de cada barreira de segurança, este trabalho considera a hipótese de que só há duas possíveis respostas para uma barreira de segurança: sucesso ou falha.

Este trabalho foca também em modelos de acidentes para especificar requisitos de projetos de sistemas de controle relacionados à segurança. Dentre as técnicas de modelagem de acidentes pesquisadas, a técnica de *bowtie* mostra-se adequada aos objetivos pretendidos, pois permite a modelagem do cenário completo de um acidente, dado um risco, assim como, a descrição da sequência de eventos

envolvida no cenário, e a identificação de barreiras de segurança para prevenção e mitigação de acidentes. Dentre as abordagens propostas para a construção das estruturas de *bowtie*, a abordagem proposta por Badreddine e Ben Amor (2013), considera dados estatísticos para a tomada de decisão por especialistas e aspectos dinâmicos do SCr baseados em bancos de dados. Por outro lado, esta abordagem não considera que na prática, a maioria dos bancos de dados são incompletos, ou seja, possuem dados faltantes(LAKSHMINARAYAN, HARP e SAMAD, 1999).

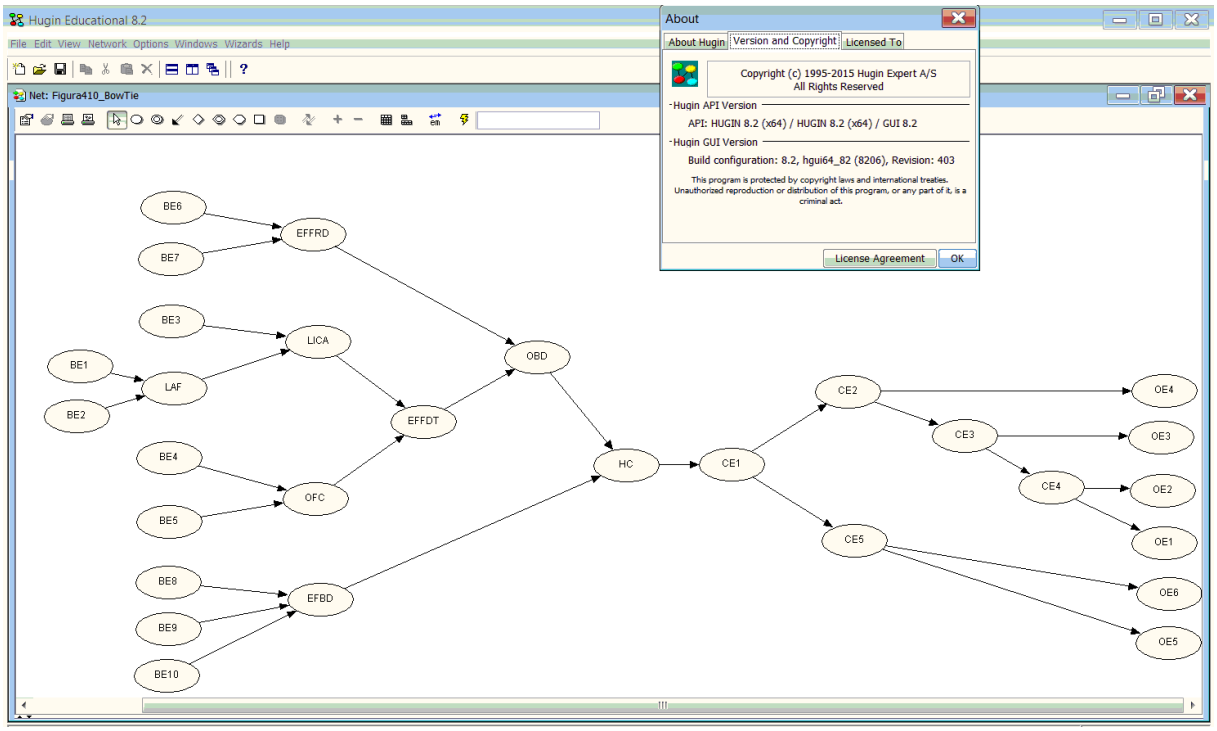
Com o propósito de se "preencher" os dados faltantes/ausentes de bancos de dados incompletos, o processo de imputação múltipla de dados via MICE[11] foi utilizado neste trabalho, por ser de domínio público e operado dentro do ambiente computacional estatístico R[12], fato esse que facilitou sua utilização.

Como o foco da aprendizagem de RdB é orientado à estrutura **S**, dado um banco de dados incompletos ou com dados faltantes, uma vez que, pretende-se obter a relação causal entre as possíveis causas e efeitos, dado um ET; as abordagens que lidam com a aprendizagem da estrutura **S** e parâmetros **Θ** da RdB, não se mostram soluções adequadas para tratar tal questão. Neste contexto, este trabalho lida primeiro com bancos de dados incompletos ou com dados faltantes, aplicando técnicas estatísticas de imputação de dados para completar os dados faltantes, e posteriormente, com a aprendizagem da estrutura **S** de uma RdB a partir de dados completos, cujas abordagens são bem conhecidas e algoritmos desenvolvidos para implementação destas abordagens com resultados eficientes.

A ferramenta computacional *Hugin® Educational* - v.8.2 foi utilizada neste trabalho, pois a versão *Lite* possui algumas limitações, como por exemplo, os bancos de dados de treinamento devem possuir até 500 linhas ou instâncias. A versão *Educational* possui uma licença temporária que foi gentilmente cedida pela empresa *Hugin Expert A/S*, uma vez que o propósito foi para pesquisa (Figura 24). Finalmente, o algoritmo para aprendizagem de estrutura **S** utilizado, foi o de Chow e Liu *Tree* (CHOW e LIU, 1968).

[11] Software livre para R, comercial com S-Plus.http://www.multiple-imputation.com
[12] Uma linguagem e ambiente para computação estatística (TEAM, 2016).

Figura 24 – Hugin Educational – v.8.2



Fonte: próprio autor

A técnica PFS permite a modelagem de estratégias de controle de segurança, de forma metódica, segundo uma abordagem *top-down* e refinamentos sucessivos para a especificação funcional e detalhamento até o nível de sensores e atuadores. Neste trabalho, a modelagem do comportamento dinâmico do sistema de controle relacionado à segurança, ou seja, a modelagem dos algoritmos de defesa de prevenção e mitigação de falhas críticas, foi desenvolvida por meio de rede de Petri devidamente interpretada para a aplicação considerada(CARDOSO e VALETTE, 1997). Uma possibilidade foi a utilização de uma derivação de RdP como o *Mark Flow Graph* (MFG)(MIYAGI, 2007), de modo que a metodologia PFS/MFG(MIYAGI, 2007) pudesse ser aplicada diretamente, para que os modelos em MFG representem os algoritmos de defesa de prevenção e mitigação de falhas.

3 METODOLOGIA PROPOSTA

Inicialmente, as hipóteses que são consideradas, no contexto de descrição dos processos de evolução de eventos críticos num cenário de acidente nas indústrias de processos, assim como, na abordagem de prevenção e mitigação desta classe de eventos são:

- Do ponto de vista de segurança funcional de um processo industrial, as falhas críticas e eventos críticos são assumidas como binárias, isto é, apresentam somente dois estados (ex: 0 e 1; Off, On; Desligado, Ligado) (BASILIO, CARVALHO e MOREIRA, 2010) (SQUILLANTE JR, 2011);
- Os sistemas de segurança são assumidos como sistemas a eventos discretos (SEDs) em especial para a modelagem e análise de questões relacionadas ao controle desses sistemas (BAKOLAS e SALEH, 2011);
- A dinâmica do comportamento de ocorrência de falhas críticas em indústrias de processos é orientada pela ocorrência de eventos críticos que podem ser tratados como instantâneos o que é coerente com a abordagem de SEDs (MIYAGI, 2007); e
- Estas hipóteses são fundamentais para a análise da observabilidade e rastreabilidade da sequência de eventos críticos durante o processo de evolução dos mesmos e está aderente com a consideração do conceito de modelagem de acidentes aliado ao princípio de defesa em profundidade e propriedade de diagnosticabilidade segura.

Adicionalmente, assume-se também que os eventos críticos podem ser “observados” ou “parcialmente observados”. Esta hipótese visa explorar informações de bancos de dados de acidentes, mesmo que incompletos e melhorar a eficácia do estudo de HAZOP, integrando a este, os eventos críticos e/ou indesejados obtidos por meio de modelos de acidentes. Estes modelos descrevem a sequência de eventos críticos e/ou indesejados, observados durante a evolução de um acidente, o que permite à equipe de especialistas inferir novas relações entre os eventos críticos e auxiliar na tomada de decisão.

Neste contexto, a metodologia proposta para o desenvolvimento de sistema de controle relacionado à segurança do processo (SCSP) envolve:

- Uma nova arquitetura orientada a projetos de sistemas de controle relacionados à segurança funcional nas indústrias de processos.
- Uma extensão da classificação de barreiras de segurança, para garantir níveis de segurança funcionais aceitáveis, considerando os recursos de automação e o conceito de SIS.
- Um *framework* para a síntese de soluções de controle, considerando a modelagem de cenários de acidentes a partir de abordagens probabilísticas, a integração destes cenários com a técnica de identificação de riscos operacionais (HAZOP), e uma sistemática para a geração de algoritmos de defesa para a prevenção e mitigação de falhas críticas.

3.1 ARQUITETURA DO SISTEMA DE CONTROLE RELACIONADO À SEGURANÇA

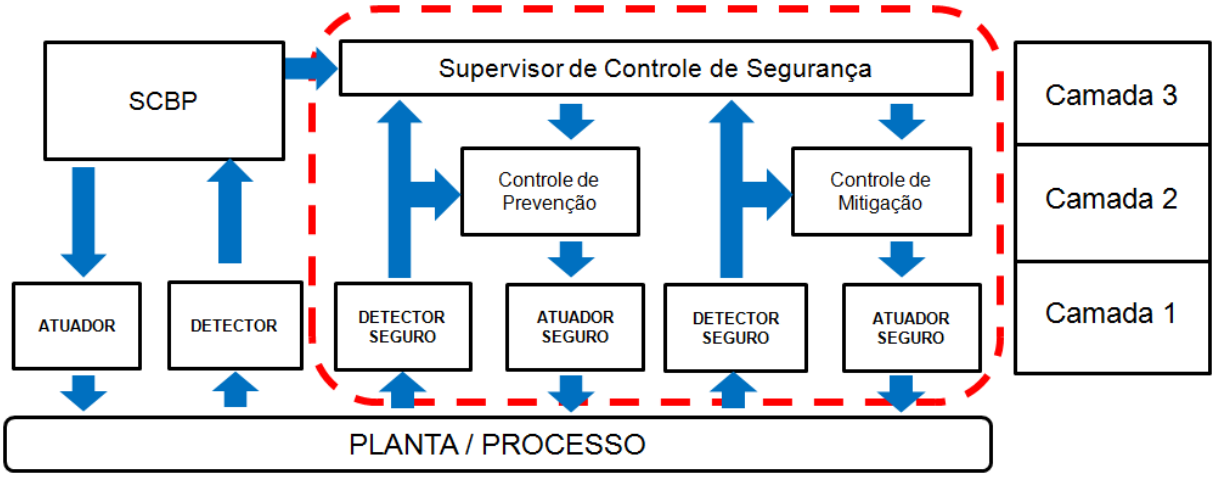
A arquitetura de sistema de controle relacionado à segurança nas indústrias de processos (SCSP), que integra o princípio de defesa em profundidade e a propriedade de diagnosticabilidade segura, considera os seguintes requisitos:

- Deve ter aderência ao conceito de sistema seguro proposto por Hollnagel (HOLLNAGEL, 2007);
- Deve ter um módulo para prevenção de eventos iniciadores e críticos, que incorpora barreiras de segurança reativas, que respondam de forma controlada e progressiva à degeneração do SCr;
- Deve ter um módulo para mitigação de eventos indesejados, que incorpora barreiras de segurança reativas, que respondam à mitigação antecipada destes eventos impedindo à propagação dos mesmos;
- Deve integrar esses módulos com o sistema de controle básico do processo (SCBP);
- Deve atender a norma IEC 61511 (IEC 61511, 2003).

Com base nestes requisitos, uma nova arquitetura de SCSP, é apresentada neste trabalho. A arquitetura é hierárquica, modular e distribuída e contempla as funções de segurança para prevenção e mitigação de eventos críticos e/ou indesejados.

Os eventos críticos e/ou indesejados são identificados por meio de uma abordagem que integra modelos de acidentes com a metodologia de HAZOP, recomendada pelas normas IEC 61882(IEC 61882, 2003) IEC 61508 (IEC 61508, 2010) e IEC 61511(IEC 61511, 2003). A arquitetura considera a aplicação do princípio de defesa em profundidade e a propriedade de diagnosticabilidade segura, assegurando que todos os eventos críticos e/ou indesejados observados e parcialmente observados, sejam adequadamente detectados, diagnosticados e tratados pelo sistema de controle. Na Figura 25 é mostrado o modelo estrutural desta arquitetura denominada Arquitetura do SCSP salientando que um modelo conceitual inicial da mesma foi apresentado inicialmente em (SQUILLANTE JR, SANTOS FO, *et al.*, 2015).

Figura 25 – Arquitetura do Sistema de Controle relacionado à Segurança para Indústrias de Processos (SCSP).



Fonte: adaptado de (SQUILLANTE JR, SANTOS FO, *et al.*, 2015)

A arquitetura do SCSP ilustrada na área pontilhada da Figura 25, é dividida em três camadas:

(i) Camada 1 - consiste de dispositivos seguros[13] de detecção e atuação, responsáveis pela interface entre o SCSP e os elementos da planta/processo;

(ii) Camada 2 - consiste dos módulos de controle de prevenção e mitigação de falhas críticas; e

[13] O termo "dispositivos seguros" segundo a norma (IEC 61508, 2010), são aqueles que desempenham suas funções quando demandados. Estes dispositivos possuem uma métrica relacionada à probabilidade de falha sob demanda (PFD) e que permite quantificar a confiabilidade destes dispositivos.

(iii) Camada 3 - consiste do módulo supervisor de controle de segurança.

Cada módulo de controle, contido nas camadas dois e três da arquitetura do SCSP, possui sua própria função de segurança.

A. Módulo de controle de prevenção

Este módulo tem como função de segurança, a redução da probabilidade de riscos por meio da prevenção de eventos críticos que antecedem a ocorrência do evento topo[14] (ET).

Este módulo de controle deve impor um comportamento seguro na planta/processo, por meio da degeneração dos elementos da mesma, quando o seu estado passar de um estado normal para um estado crítico controlado.

A implementação dos algoritmos de defesa deste módulo é baseada em modelos derivados da aplicação da metodologia PFS/MFG. Para maiores detalhes da metodologia PFS/MFG, consultar o Anexo A.

Este módulo de controle está conectado com seus próprios elementos detectores e atuadores, localizados na Camada 1 da arquitetura do SCSP ilustrada na Figura 25.

B. Módulo de controle de mitigação

Este módulo de controle de mitigação tem como função de segurança, mitigar ou reduzir as consequências indesejadas provocadas pela ocorrência do evento topo (ET), de maneira a proteger as pessoas, meio ambiente e instalações.

Este módulo de controle deve minimizar ou reduzir os efeitos provocados pelos eventos indesejados.

A implementação dos algoritmos de defesa deste módulo é baseada em modelos derivados da aplicação da metodologia PFS/MFG. Para maiores detalhes da metodologia PFS/MFG, consultar o Anexo A.

[14] A terminologia evento topo está sendo utilizada neste trabalho, com base na definição do diagrama de *bowtie*. Esta terminologia algumas vezes é mencionada neste trabalho como falhas críticas.

Este módulo de controle está conectado com seus próprios elementos detectores e atuadores, localizados na Camada 1 da arquitetura SCSP ilustrada na Figura 25.

C. Módulo supervisor de controle de segurança

Este módulo de controle tem como função de segurança, a detecção e filtragem de eventos espúrios que possam estar associados a cada evento crítico e/ou indesejado que surgir durante a operação da planta/processo. Esta consideração endereça a propriedade de diagnosticabilidade segura(PAOLI e LAFORTUNE, 2005), que exige a existência de um diagnosticador local para cada evento crítico do sistema em operação. A detecção dos eventos pode ser na forma direta ou indireta e, com base em regras (ex: lógica de votação 2oo3), fazer o diagnóstico destes eventos.

Este módulo também é responsável pela supervisão de quais barreiras de segurança são pertinentes para tratamento destes eventos, via módulos de controle de prevenção e mitigação, localizados na Camada 2 da arquitetura SCSP, assegurando um estado seguro da planta/processo.

A implementação dos algoritmos de defesa deste módulo é baseada em modelos derivados da metodologia PFS/MFG. Inicialmente, para cada cenário crítico, são desenhados os modelos em PFS para detecção e filtragem de eventos espúrios dos sensores relacionados a cada evento crítico e/ou indesejado deste cenário. Posteriormente, os modelos PFS são refinados em MFG representando os algoritmos de detecção e diagnóstico destes eventos.

Neste módulo, os algoritmos de detecção e diagnósticos são integrados com os algoritmos de defesa de prevenção e mitigação correspondentes, com o objetivo de diagnosticar de forma segura os eventos críticos e/ou indesejados que acionam as barreiras de prevenção e mitigação para tratamento destes eventos.

Este módulo supervisor de controle de segurança, utiliza os elementos detectores do módulo de controle de prevenção e do módulo de controle de mitigação, localizados na Camada 1 da arquitetura SCSP (Figura 25).

D. Comunicação entre SCSP e SCBP

O sistema de controle básico da planta/processo (SCBP), assim como, seus dispositivos de detecção e atuação, também são ilustrados na Figura 25.

De acordo com as normas IEC 61508(IEC 61508, 2010) e IEC 61511(IEC 61511, 2003), o SCBP não realiza quaisquer funções de segurança. Entretanto, ele é considerado nesta arquitetura, uma vez que uma falha neste dispositivo de controle pode conduzir a planta/processo a um estado crítico controlável ou incontrolável[15]. (SQUILLANTE JR, SANTOS FO, *et al.*, 2015).

3.2 RECLASSIFICAÇÃO DE BARREIRAS DE SEGURANÇA

Com base nas hipóteses e requisitos do SCSP, o sistema de barreiras de segurança:

- Deve atuar sob o módulo de controle de prevenção de eventos críticos da arquitetura do SCSP;
- Deve atuar também sob o módulo de controle de mitigação de eventos indesejados da arquitetura do SCSP;
- Deve considerar a possível substituição do elemento humano de tal forma que determinadas atividades de observação, diagnóstico e ação sejam realizadas pelo SCSP.

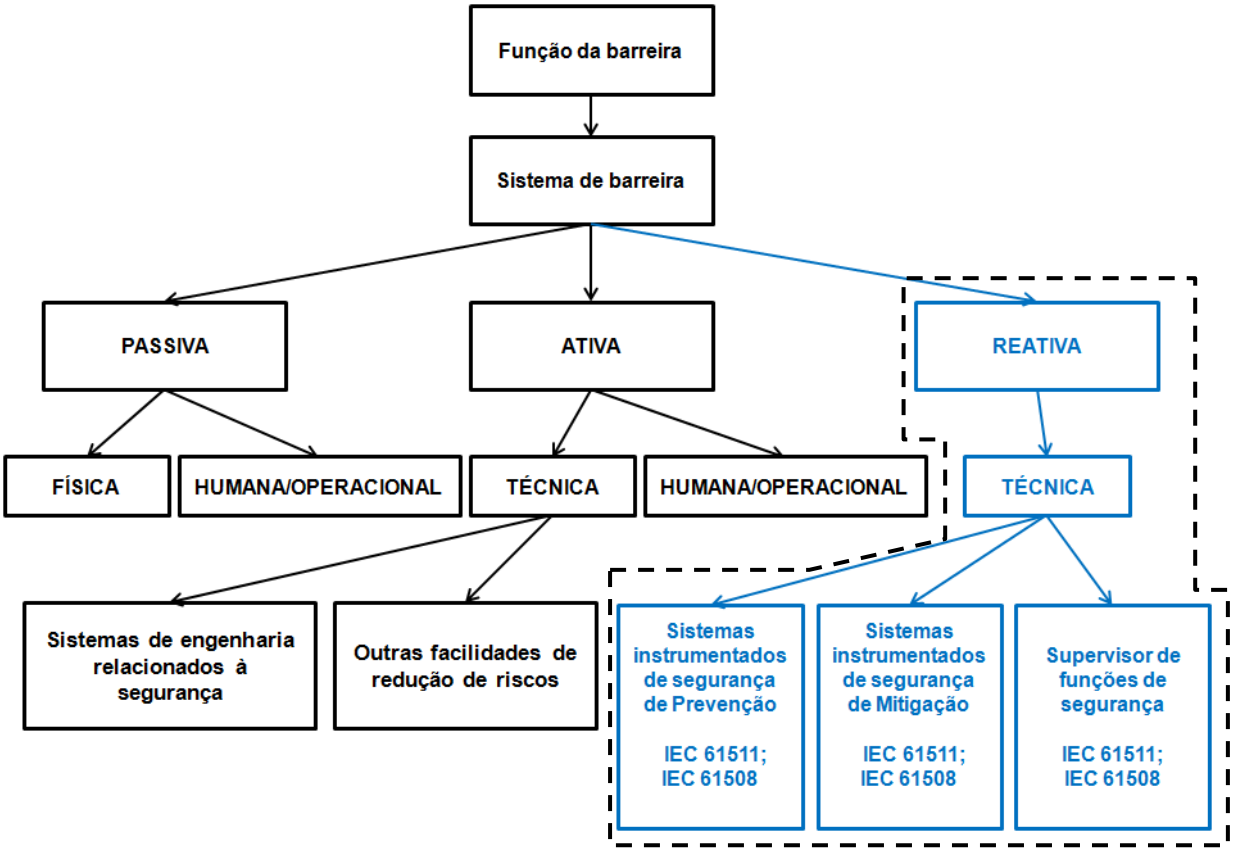
Assim, apresenta-se aqui uma reclassificação de sistemas de barreiras de segurança que é uma extensão da classificação proposta por Sklet (2006). A reclassificação considera um sistema de barreiras de prevenção e mitigação reativas, que inclui o conceito de SIS, de modo que cada barreira tem autonomia para realizar a observação, o diagnóstico e a atuação contra eventos críticos e/ou indesejados.

A Figura 26 mostra uma reclassificação de barreiras de segurança. A parte destacada por uma moldura tracejada corresponde à extensão considerada.

[15] O termo "estado crítico controlado" refere-se a estados críticos que podem ser previnidos via módulo de controle de prevenção, antes de se alcançar a falha crítica. Por outro lado, o termo "estado crítico incontrolado" refere-se a estados provocados pela ocorrência da falha crítica - devido à falha na prevenção, e que devem ser minimizados via módulo de controle de mitigação.

Esta classificação mantém as mesmas definições de sistemas de barreiras passivas e físicas descritas por Sklet (2006), e acrescenta um novo sistema de barreira denominado de reativa que tem como fundamento o conceito de sistemas reativos. Estas barreiras devem reagir de forma dinâmica com o ambiente externo no qual estão inseridas, ou seja, são baseadas em eventos que reagem a estímulos internos e/ou externos do ambiente, de forma a produzir resultados corretos, dentro de intervalos de tempo determinado pelo próprio ambiente. Considera-se que este tipo de barreira só tem uma forma de implementação que é chamada de “técnica”, pois, aplica-se ao uso de tecnologias de sistemas instrumentados de segurança (SIS) e das normas (IEC 61508, 2010) e (IEC 61511, 2003).

Figura 26 – Reclassificação de sistemas de barreiras de segurança



Fonte: próprio autor

As barreiras reativas técnicas são divididas em três tipos:

(i) **Supervisor de funções de segurança**: barreiras relacionadas ao módulo supervisor de controle de segurança do SCSP, que realizam a observação e diagnóstico dos eventos críticos/indesejados do sistema. Caso este tipo de barreira perceba a presença de algum evento crítico/indesejado, pela propriedade de diagnosticabilidade segura, o mesmo deve reagir

acionando as barreiras reativas de prevenção e/ou mitigação de falhas críticas.

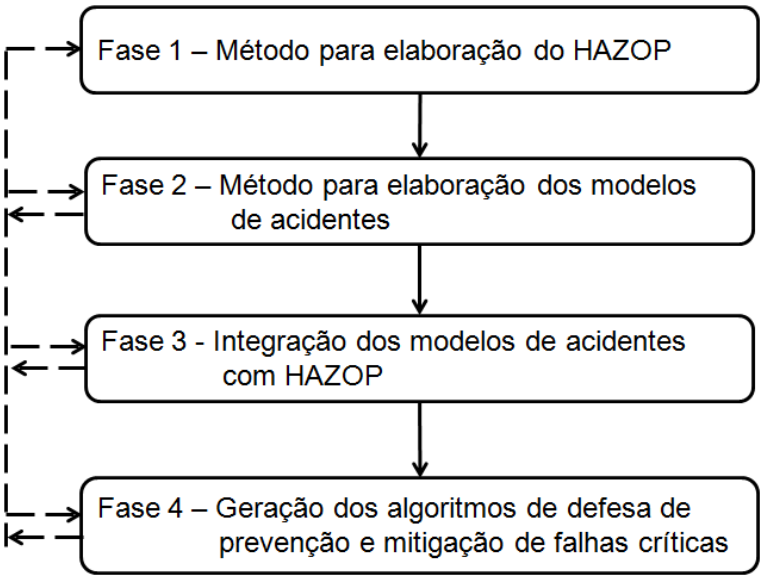
(ii) **Sistema instrumentado de segurança de prevenção**: barreiras relacionadas ao módulo de controle de prevenção do SCSP, que realizam o tratamento de eventos críticos, por meio de algoritmos de defesa de prevenção de falhas críticas.

(iii) **Sistema instrumentado de segurança de mitigação**: barreiras relacionadas ao módulo de controle de mitigação do SCSP, que realizam o tratamento de eventos indesejados, por meio de algoritmos de defesa de mitigação de falhas críticas que não puderam ser prevenidas pelo SIS de prevenção.

3.3 *FRAMEWORK* PARA A SÍNTESE DO SISTEMA DE CONTROLE RELACIONADO À SEGURANÇA

Esta seção apresenta um *framework* para a síntese do sistema de controle relacionado à segurança para indústrias de processos (SCSP). O *framework* ilustrado na Figura 27, combina diferentes métodos baseados em técnicas, ferramentas e conceitos como, por exemplo, estudo de HAZOP, imputação de dados, aprendizagem de redes bayesianas, diagrama de *bowtie* e metodologia PFS/MFG.

Figura 27 – *Framework* para a síntese do SCSP



Fonte: próprio autor

O *framework* mostrado na Figura 27 é composto por quatro fases:

- Fase 1 – Método para elaboração do HAZOP
- Fase 2 – Método para elaboração dos modelos de acidentes
- Fase 3 – Integração dos modelos de acidentes com HAZOP
- Fase 4 – Geração dos algoritmos de defesa de prevenção e mitigação de falhas críticas

A seguir, cada fase do *framework* será descrita detalhadamente.

3.3.1 Fase 1 – Método para elaboração do HAZOP

O HAZOP, do termo inglês *Hazard and Operability study,* é um método clássico que é empregado para a identificação e análise de riscos e perigos operacionais de um sistema, assim como, falhas de elementos deste sistema. Este método envolve uma revisão detalhada do projeto e da operação da planta/processo, focando em desvios nos parâmetros envolvidos, tais como, pressão, fluxo, temperatura, vibração, dentre outros parâmetros ou elementos que estão associados à ocorrência de eventos críticos e/ou indesejados. Este método é amplamente utilizado nas indústrias de processos e suportado pelas normas IEC 61511(IEC 61511, 2003) e IEC 61882 (IEC 61882, 2003).

A Fase 1 compreende as atividades fundamentais do processo de elaboração do HAZOP, para identificação e análise de riscos do objeto de controle. O processo envolvido é descrito em PFS conforme ilustra a Figura 28, e a seguir são descritas cada uma das atividades identificadas.

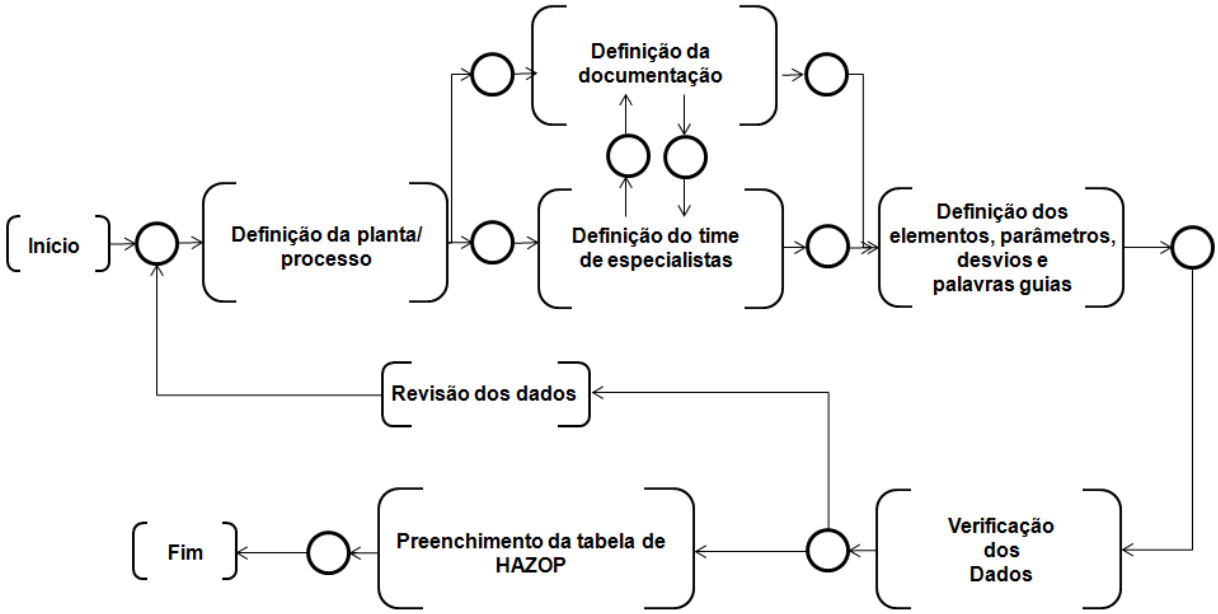
3.3.1.1 Definição da planta/processo

Nesta atividade é definida a planta/processo que faz parte do objeto de controle.

3.3.1.2 Definição do time de especialistas

Nesta atividade, são definidos os membros da equipe multidisciplinar que conhecem o comportamento dinâmico do objeto de controle, assim como, os riscos inerentes deste objeto de controle.

Figura 28 – Processo de elaboração do HAZOP



Fonte: adaptado de (CAVALHEIRO, 2013).

De uma forma geral, os membros são coordenadores e/ou responsáveis por áreas de conhecimento (ex: engenharia de processos; engenharia de automação; instrumentação; elétrica; mecânica; operação e engenharia de segurança de processos), necessários para o desenvolvimento do projeto. Ainda segundo a norma IEC 61882 (IEC 61882, 2003), devem ser definidas funções como: líder, redator, projetista, usuário, especialista, mantenedor, etc., onde cada membro com sua respectiva função tem sua própria responsabilidade sobre o HAZOP. Independentemente do pessoal e das funções atribuídas, todos os membros da equipe devem ter conhecimento suficiente da dinâmica de operação do objeto de controle, sendo atribuído à equipe, sob a supervisão do engenheiro de segurança de processos, o conhecimento pleno das técnicas de identificação e análise de riscos; para que participem de forma colaborativa e efetiva no estudo.

3.3.1.3 Definição da documentação

Esta atividade tem como objetivo, definir e obter a documentação fundamental do objeto de controle, para a identificação e análise de riscos do mesmo. A definição da documentação a ser utilizada no estudo de HAZOP, é executada com base nas decisões da equipe multidisciplinar anteriormente definida. A documentação fornece informações fundamentais para a tomada de decisão da equipe com relação às

estratégias e ações de controle para prevenção e mitigação de falhas críticas. Basicamente, os documentos relevantes a serem obtidos são:

a) Diagramas do processo e da instrumentação do processo, também chamado de P&ID do termo inglês, *Process and Instrumentation Diagram*; preconizado pela norma ISA S-5.1(ISA-S5.1-1984, 2009),
b) Descritivo de funcionamento dos elementos que fazem parte do objeto de controle (ex: planta/processo, SCBP e seus dispositivos associados),
c) Lista dos instrumentos contendo: (i) a identificação do mesmo no objeto de controle, (ii) faixa de operação normal do instrumento, (iii) faixa de calibração do instrumento, e (iv) lista com os valores máximos e mínimos de referência permitidos para desvios de parâmetros.
d) Lista de sensores e atuadores que fazem a interface entre o SCBP e a planta/projeto. É importante ressaltar que o projeto do SCSP é orientado à mesma planta que é controlada pelo SCBP (Figura 25).

3.3.1.4 Definição dos elementos, parâmetros, desvios e palavras guias

De acordo com a norma IEC 61882(IEC 61882, 2003), cada elemento é usado para identificar características pertinentes do sistema ou parte do sistema, que neste trabalho é o objeto de controle. As características de um elemento são as propriedades qualitativas ou quantitativas que podem ser mensuradas de forma direta por meio de sensores, ou de forma indireta por meio do conhecimento sintetizado na forma de modelos matemáticos (CAVALHEIRO, 2013).

A escolha dos elementos depende diretamente de cada objeto de controle em particular, de modo que, possam estar relacionados com: (i) material envolvido, (ii) atividade realizada, (iii) equipamento ou elemento utilizado, (iv) material transportado ou transformado, etc.

Os parâmetros estão associados às características quantitativas de um elemento, como por exemplo, temperatura, pressão, nível, fluxo, etc. A determinação destes parâmetros é feita por meio de medições diretas e indiretas, como já descrito. Neste contexto, para cada elemento do objeto de controle e/ou sistema de controle relacionado à segurança, deve-se definir os parâmetros pertinentes ao estudo de HAZOP.

Os desvios correspondem à diferença obtida com relação ao valor medido do parâmetro e seus limites máximos e mínimos permitidos. Os desvios sinalizam eventos críticos (EC) e/ou eventos indesejados (UE) do objeto de controle.

Finalmente, a palavra guia, segundo a norma IEC 61882(IEC 61882, 2003), pode ser definida como uma palavra ou frase que expressa e define um tipo específico de desvio de uma característica de um elemento do objeto de controle. As palavras guias mais comuns segundo a norma são: ALTO, MUITO ALTO, BAIXO, MUITO BAIXO, IGUAL, AUMENTANDO, DIMINUINDO, etc. Porém, a norma permite a criação ou adaptação de palavras guias para o contexto de cada projeto. Desta forma, dependendo do caso, podem ser criadas palavras guias específicas. O importante é que estas palavras guias definam claramente os desvios de cada característica para cada elemento do objeto de controle.

3.3.1.5 Verificação e revisão dos dados

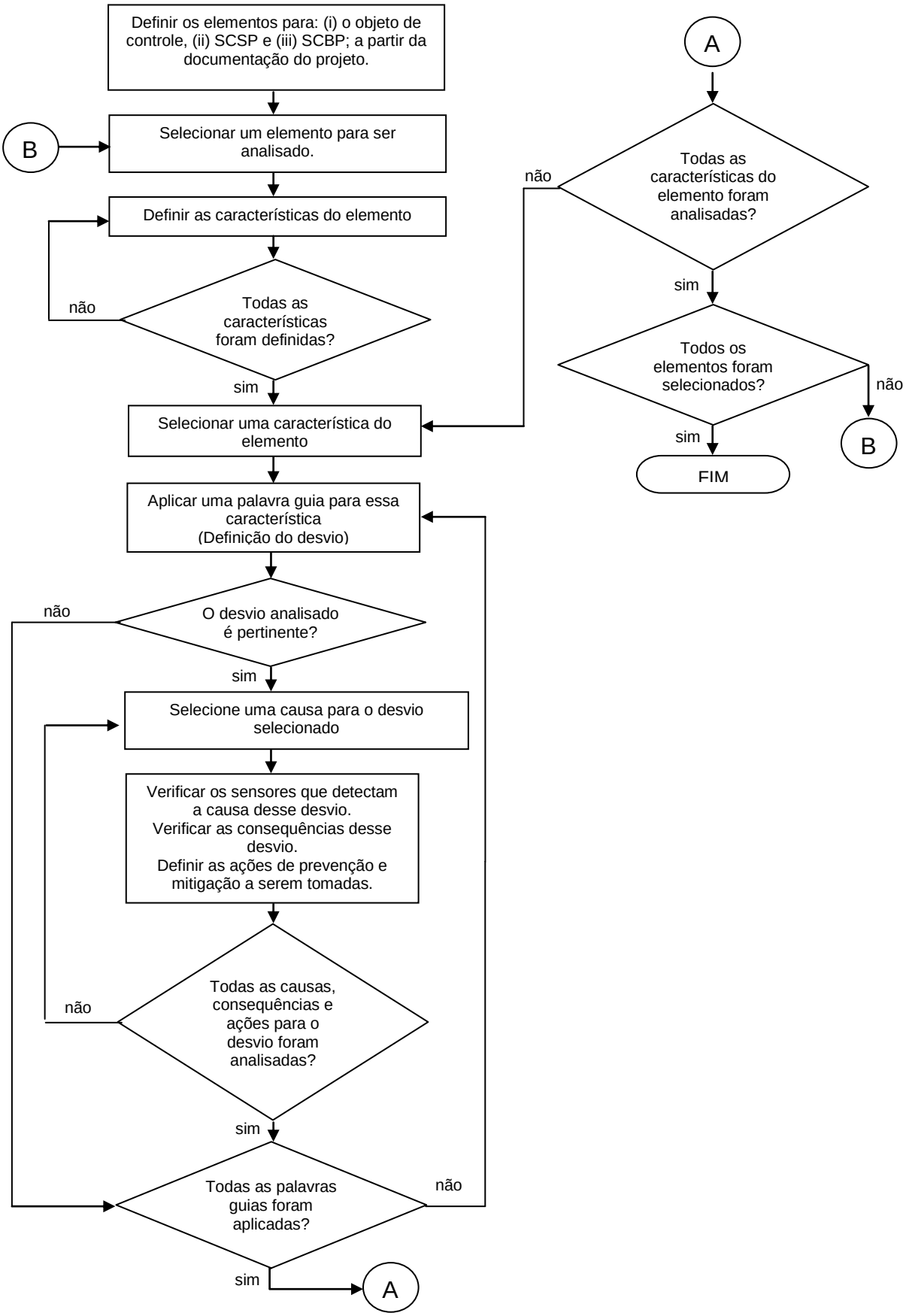
Nesta atividade devem ser verificados os elementos do objeto de controle, seus parâmetros, palavras guias e desvios pertinentes. Caso seja necessário, devem ser criados novos elementos ou eliminados aqueles elementos ou parâmetros ou palavras guias que não definem claramente um determinado desvio, tendo como referência as características da planta/processo (objeto de controle).

Caso seja necessário deve-se rever os resultados obtidos, desde o início desta fase.

3.3.1.6 Preenchimento da tabela de HAZOP

Para o preenchimento da tabela de HAZOP, utiliza-se o algoritmo descrito na Figura 29.

Figura 29 – Algoritmo para preenchimento da tabela de HAZOP



Fonte: adaptado de (CAVALHEIRO, 2013).

A Tabela 1 mostra um possível esquema para uma tabela do estudo de HAZOP a ser considerado neste trabalho.

O esquema proposto na Tabela 1 possui a seguinte interpretação:

- "Sistema" ou "parte do sistema" identificam o conjunto de equipamentos, máquinas, aparatos ou objeto de controle;
- A **coluna 1** indica o tipo da barreira de segurança e outros dados pertinentes, para o elemento do objeto de controle considerado. O formato geral de identificação da barreira de segurança é:

BWx.y.z

Onde:

B: barreira de segurança

W: tipo da barreira: P – prevenção ou M – mitigação

x: número do evento topo (ET) ou falha crítica

y: número do cenário crítico[16]

z: número da barreira

- A **coluna 2** indica o nome do elemento do objeto de controle;
- A **coluna 3** indica o nome do evento crítico/indesejado;
- A **coluna 4** indica as possíveis causas do evento crítico/indesejado;
- A **coluna 5** indica as possíveis consequências após a ocorrência do evento crítico/indesejado;
- A **coluna 6** indica o conjunto de medidas de segurança a serem tomadas para reduzir, eliminar ou mitigar as causas identificadas. Também indica como diagnosticar e tratar o evento crítico/indesejado;

[16] No caso da AF, o cenário crítico representa uma concatenação de eventos críticos até se atingir o evento topo (ET) ou falha crítca. Por outro lado, no caso da AE, o cenário crítico representa uma possível concatenação de eventos indesejados até se alcançar resultado indesejado da planta/processo.

Tabela 1 – Esquema proposto para preenchimento da tabela de HAZOP

Título: ESTUDO DE HAZOP								
Número do documento			**Número da Revisão**				**Número da Folha:**	
Responsáveis pelo estudo:							**Data da reunião:**	
Sistema / parte do sistema: Refinaria BP Texas / Unidade de Isomerização								
Barreira	Elemento	Evento Crítico/Desvio	Possíveis Causas	Consequências	Ação	Equipamento (1)	Sensores	Atuadores
BP1.1.1	Torre de isomerização	Alarme de nível alto 1	a) Inexistência de regras de segurança	nível de refinado acima do nível crítico 1	a) Elaboração ou modificação de regras de segurança durante start-up			
BP1.2.1		LAH-1	b) Violação das regras de segurança		b) Treinamento dos operadores			
BP1.3.1	Torre de isomerização	Nível de combustível acima do 1º nível crítico	a) Violação ou inexistência de regras de segurança	a) nível de refinado acima 1º nível crítico	a) instalação de sensores redundantes	a)SIS	nível (LT1.1 e LT1.2)	a) sinalização de
				b) transbordamento de refinado	b) Indicação de alarme (LAH-1)	b)Sistema supervisório		Alarme LAH-1
BP1.3.2			b) Falta de tratamento de segurança	c) elevação da pressão interna	c) Intertravamento de segurança realizado			b) fechamento automático
				d) elevação da temperatura interna	por EEP			válvula de entrada

1 2 3 4 5 6 7 8 9

Fonte: próprio autor

- A **coluna 7** indica os equipamentos relacionados à segurança a serem utilizados para implementar a barreira de segurança, como por exemplo, equipamentos eletrônicos programáveis (EEP) e sistemas de monitoração de dados e informações do processo/planta;
- A **coluna 8** indica os sensores utilizados para detectar os desvios de parâmetros e/ou falhas de elementos; e
- A **coluna 9** indica os atuadores a serem utilizados pelas barreiras de segurança.

3.3.2 Fase 2 – Método para elaboração dos modelos de acidentes

A Fase 2 do *framework* ilustrado na Figura 27, compreende as atividades do processo de modelagem de acidentes, a partir de:

(a) banco de dados incompletos da planta/processo que faz parte do objeto de controle, endereçando além dos eventos críticos e/ou indesejados observados, os eventos críticos e/ou indesejados parcialmente observados, e/ou

(b) relatórios de acidentes da planta/processo.

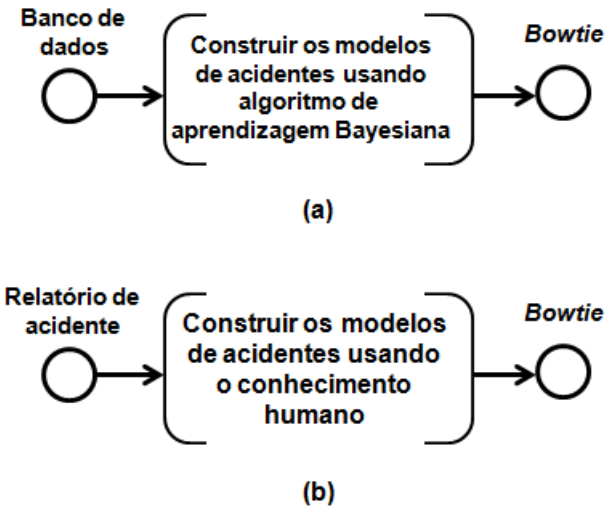
Os processos de modelagem são apresentados em PFS, conforme ilustra a Figura 30. O método ilustrado na Figura 30 permite a construção dos modelos de acidentes nas seguintes situações:

(a) a partir o banco de dados de acidentes da planta/processo com dados faltantes ou incompletos, ou

(b) a partir do(s) relatório(s) de acidente(s).

A Figura 30a ilustra o processo de modelagem de acidentes a partir do banco de dados com dados faltantes ou incompletos. Utiliza-se técnicas de imputação de dados e de aprendizagem bayesiana para se trabalhar com uma base de dados completa. A Figura 30b ilustra o processo de modelagem de acidentes a partir de relatórios de acidentes. Utiliza-se como base o conhecimento humano. O resultado obtido a partir da execução destes dois processos é o diagrama de *bowtie*.

Figura 30 – Método para elaboração de modelos de acidentes



Fonte: próprio autor

3.3.2.1 Construção dos modelos de acidentes usando algoritmo de aprendizagem bayesiana

Apresenta-se aqui o processo de modelagem de cenários de acidentes, considerando banco de dados incompletos ou com dados faltantes em algumas instâncias; considera-se que os eventos críticos e/ou indesejados foram observados ou parcialmente observados. O método em questão (Figura 31) considera duas abordagens probabilísticas: (i) uma para estimativa dos dados faltantes por valores “plausíveis” pelo método de imputação múltipla de dados, e (ii) uma para aprendizagem das estruturas pertinentes à AF e AE, pelo método de aprendizagem bayesiana *Chow e Liu tree*.

O método ilustrado na Figura 31 é composto por seis etapas principais:

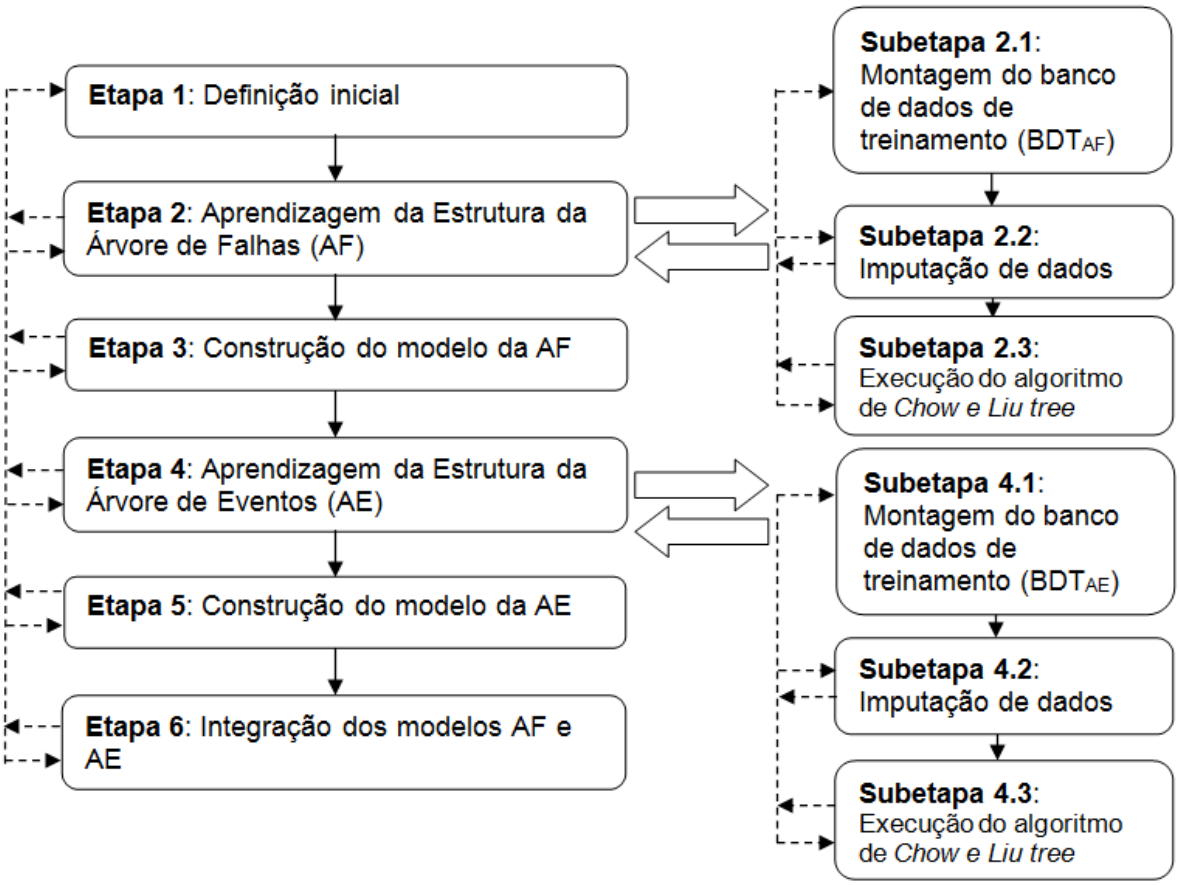
- Etapa 1 – Definição inicial
- Etapa 2 – Aprendizagem da estrutura da árvore de falhas (AF)
- Etapa 3 – Construção do modelo da AF
- Etapa 4 – Aprendizagem da estrutura da árvore de eventos (AE)
- Etapa 5 – Construção do modelo da AE

- Etapa 6 – Integração dos modelos AF e AE

As etapas 2 e 4 são compostas por três subetapas cada:

- Subetapas 2.1 e 4.1 – Montagem dos bancos de dados de treinamento de árvore de falhas (BDT_{AF}) e árvore de eventos (BDT_{AE}), respectivamente,
- Subetapas 2.2 e 4.2 – Imputação de dados, e
- Subetapas 2.3 e 4.3 – Execução do algoritmo de aprendizagem bayesiana de *Chow e Liu tree*, a partir dos bancos de dados BDT_{AF} e BDT_{AE} respectivamente.

Figura 31 – Método para modelagem de acidentes considerando banco de dados incompletos ou com dados faltantes



Fonte: próprio autor

A seguir, cada etapa e subetapa deste método são descritas.

- **Etapa 1 - Definição inicial**

Nesta etapa são coletadas informações fundamentais a respeito da planta/processo cujos eventos críticos e/ou indesejados devem ser prevenidos e/ou mitigados de forma controlada. As informações fundamentais são: (i) registros

históricos de falhas; (ii) documentação do projeto (ex: diagrama do processo e da instrumentação do processo (P&ID[17])(ISA-S5.1-1984, 2009)). Nesta etapa também é realizada a seleção do time de especialistas com conhecimento multidisciplinar sobre a planta/processo do objeto de controle (ex: engenheiros de processos; engenheiros elétricos, engenheiros mecânicos, operadores de processos; engenheiros de segurança de processos).

- **Etapa 2 - Aprendizagem da estrutura da árvore de falhas (AF)**

Nesta etapa são identificadas as relações de dependência entre os eventos críticos observados e parcialmente observados antes da ocorrência do evento topo (ET). Ela é subdividida em três subetapas: subetapa 2.1 que trata da montagem de um banco de dados de treinamento (BDT_{AF}), subetapa 2.2 que trata da imputação de dados por valores plausíveis onde existirem dados faltantes, e da subetapa 2.3 que trata da execução do algoritmo de aprendizagem pelo método de *Chow e Liu tree*, a partir do BDT_{AF}.

- **Subetapa 2.1 – Montagem do banco de dados de treinamento (BDTAF)**

Nesta subetapa tem-se a montagem do banco de dados de treinamento (BDT_{AF}) que tem como objetivo, a obtenção do grafo acíclico orientado (GAO) ou estrutura da Árvore de Falha (AF). O BDT_{AF} é construído como uma matriz de dados compatível com o formato exigido pelo algoritmo de aprendizagem a ser utilizado, contendo: (i) a falha crítica ou evento topo (ET) e (ii) todos os eventos críticos, isto é, possíveis causas que foram observadas ou parcialmente observadas antes da ocorrência do ET.

O BDT_{AF} é montado a partir de registros históricos de falhas. A abordagem considera bancos de dados de históricos de falhas com dados incompletos ou com dados faltantes, ou seja, alguns eventos críticos podem apresentar dados faltantes em algumas instâncias da matriz de dados.

Assim, a técnica de IM é usada para estimar dados ausentes no banco de dados, considera-se que: (i) o padrão de dados ausentes no BDT_{AF} possui uma

[17] Esta norma foi concebida para ser uma padronização de simbologia e identificação de instrumentos e equipamentos de processo; sua abrangência é nível mundial. Esta norma é utilizada na elaboração dos seguintes documentos: (i) Diagramas de Processo e da Instrumentação do processo, (ii) Especificações e Listas de instrumentos e (iv) Identificação de instrumentos e funções de controle.

estrutura arbitrária, e portanto, constitui um padrão não monotônico, e (ii) o mecanismo de dados ausentes no BDT_{AF} é do tipo MCAR.

O BDT_{AF} é então montado como uma matriz de dados onde: (i) a primeira coluna representa o ET e (ii) as demais colunas da matriz representam os eventos críticos (EC_i) (ex: causas) em qualquer ordem. Cada linha ou instância da matriz contém um valor binário para o ET e também um valor binário para cada EC_i. O ET e os EC_i são tratados neste trabalho, como variáveis aleatórias com valores binários (ex: 0 ou 1 / falso ou verdadeiro) que representam desvios de parâmetros e/ou falhas de elementos. Para os EC_i que foram observados, os valores contidos no BDT_{AF} podem ser valores binários, enquanto que, para EC_i não observados (ex: dados faltantes), os valores contidos no BDT_{AF} devem ser nulos (ex. NA), ou seja, não contém valores binários associados. Um exemplo do BDT_{AF} é ilustrado na Figura 32.

Figura 32 – Exemplo de BDT_{AF}

	ET	EC_1	EC_2	EC_3	EC_4	EC_5	EC_6	. . .	EC_n
Linha 1	**0**	**0**	**NA**	**1**	**NA**	**0**	**NA**	. . .	**0**
Linha 2	**1**	**1**	**1**	**0**	**NA**	**0**	**1**	. . .	**NA**
. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .
Linha M	**1**	**1**	**NA**	**0**	**1**	**NA**	**1**	. . .	**1**

Fonte: próprio autor

- **Subetapa 2.2 – Imputação de dados**

Nesta subetapa tem-se a imputação dos dados faltantes do BDT_{AF} por valores plausíveis. O algoritmo MICE é aqui considerado. Como resultado desta subetapa, ter-se-á uma ou várias possibilidades de BDT_{AF} com dados completos.

- **Subetapa 2.3 – Execução do algoritmo de aprendizagem**

Nesta subetapa tem-se a execução do algoritmo de aprendizagem bayesiana para a construção do GAO da AF. O banco de dados completo de treinamento BDT_{AF}, é utilizado como entrada de dados para a execução do algoritmo de aprendizagem. O algoritmo de aprendizagem de estrutura bayesiana considerado neste trabalho é o de *Chow e Liu tree* (CHOW e LIU, 1968), onde o evento topo do

BDT_{AF} como nó raiz. Ferramentas computacionais como o *Hugin Educational*® podem ser utilizadas para executar esta subetapa.

- **Etapa 3 – Construção do modelo da árvore de falhas (AF)**

A partir da estrutura obtida após a execução do algoritmo de aprendizagem na subetapa 2.3, realiza-se nesta etapa a inferência do conhecimento por parte do time de especialistas envolvidos no processo; verificando e aprimorando as relações causais de dependência entre o evento topo (ET) e as possíveis causas (eventos críticos - EC_i).

O time de especialistas pode modificar manualmente as relações de dependência e de independência entre os EC_i e o ET, adicionando e/ou removendo arcos e/ou eventos críticos até convergir para um modelo adequado de AF.

Esta ação dos especialistas é relevante pois embora os algoritmos de aprendizagem sejam eficazes, as relações de dependência entre as variáveis são inferidas a partir do BDT_{AF} sob condições de incerteza, e, portanto, é fundamental considerar o conhecimento humano. Este procedimento procura identificar novas relações de dependência e/ou independência entre EC_i não observados com os EC_i observados.

- **Etapa 4 - Aprendizagem da estrutura da árvore de eventos (AE)**

Nesta etapa obtem-se as relações de dependência entre os eventos indesejados e o ET que foram observados ou parcialmente observados após a ocorrência do evento topo (ET). Ela é subdividida em três subetapas: subetapa 4.1 que trata da montagem do banco de dados de treinamento (BDT_{AE}), subetapa 4.2 que trata da imputação de dados faltantes por valores plausíveis, e da subetapa 4.3 que trata da execução do algoritmo de aprendizagem pelo método de *Chow e Liu tree*, a partir do BDT_{AE}.

- **Subetapa 4.1 – Montagem do banco de dados de treinamento (BDTAE)**

Nesta subetapa tem-se a montagem do banco de dados de treinamento (BDT_{AE}) que tem como objetivo, a obtenção da estrutura ou GAO da Árvore de Eventos (AE). O BDT_{AE} é construído como uma matriz de dados compatível com o formato exigido pelo algoritmo de aprendizagem a ser utilizado. Ele contém: (i) a falha crítica ou

evento topo (ET) e (ii) todos os eventos indesejados ou consequências indesejadas que foram observadas ou parcialmente observadas após a ocorrência do ET.

O BDT_{AE} é semelhante ao BDT_{AF}, ou seja, é montado a partir de registros históricos de falhas com dados incompletos ou dados faltantes em algumas instâncias da matriz. Aqui também a técnica de IM é usada para estimar dados ausentes no banco de dados. Considera-se que: (i) o padrão de dados ausentes no BDT_{AE} possui uma estrutura arbitrária, e portanto, constitui um padrão não monotônico, e (ii) o mecanismo de dados ausentes no BDT_{AE} é do tipo MCAR.

O BDT_{AE} é então montado como uma matriz de dados onde: (i) a primeira coluna representa o ET e (ii) as demais colunas da matriz representam os eventos indesejados (UE_i) em qualquer ordem. Cada linha ou instância da matriz contém um valor binário para o ET e também um valor binário para cada UE_i. O ET e os UE_i são tratados neste trabalho, como variáveis aleatórias com valores binários (ex: 0 ou 1 / falso ou verdadeiro). Para os UE_i que foram observados, os valores contidos no BDT_{AE} podem ser binários, enquanto que, para os UE_i que não foram observados (ex: dados faltantes), os valores contidos no BDT_{AE} devem ser nulos (ex. NA), ou seja, não contém valores binários associados. Um exemplo do BDT_{AE} é mostrado na Figura 33.

- **Subetapa 4.2 – Imputação de dados**

Nesta subetapa tem-se a imputação dos dados faltantes do BDT_{AE} por valores “plausíveis”. O algoritmo MICE executado é aqui considerado. Como resultado desta subetapa, ter-se-á o BDT_{AE} com dados completos.

Figura 33 – Exemplo de BDT_{AE}

	ET	EI_1	EI_2	EI_3	EI_4	EI_5	EI_6	. . .	EI_n
Linha 1	**1**	**1**	**NA**	**1**	**0**	**1**	**0**	. . .	**NA**
Linha 2	**0**	**0**	**0**	**NA**	**1**	**NA**	**NA**	. . .	**0**
. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .
Linha M	**1**	**1**	**NA**	**0**	**NA**	**0**	**1**	. . .	**NA**

Fonte: próprio autor

- **Subetapa 4.3 – Execução do algoritmo de aprendizagem**

Nesta subetapa tem-se a execução do algoritmo de aprendizagem bayesiana para a construção do GAO da AE. O banco de dados completo de treinamento BDT_{AE} é utilizado como entrada de dados para a execução do algoritmo de aprendizagem. O algoritmo de aprendizagem de estrutura bayesiana considerado neste trabalho é o de Chow e Liu tree (CHOW e LIU, 1968), onde o evento topo do BDT_{AE} é o nó raiz. Aqui também ferramentas computacionais como o *Hugin Educational*® podem ser utilizadas para executar esta subetapa.

- **Etapa 5 – Construção do modelo da árvore de eventos (AE)**

A partir da estrutura obtida após a execução do algoritmo de aprendizagem na subetapa 4.3, realiza-se agora a inferência do conhecimento por parte do time de especialistas envolvidos no processo; verificando e aprimorando as relações causais de dependência entre o evento topo (ET) e os eventos indesejados (UE_i).

O time de especialistas pode modificar manualmente as relações de dependência e independência entre os UE_i e o ET, adicionando e/ou removendo arcos e/ou UE_i até convergir para um modelo adequado de AE.

Esta ação dos especialistas é relevante pois, embora os algoritmos de aprendizagem sejam eficazes, as relações de dependência entre as variáveis são inferidas a partir do BDT_{AE} sob condições de incerteza, e, portanto, é fundamental considerar o conhecimento humano. Este procedimento procura identificar novas relações de dependência e/ou independência entre UE_i parcialmente observados com os UE_i observados.

- **Etapa 6 – Integração dos modelos AF e AE**

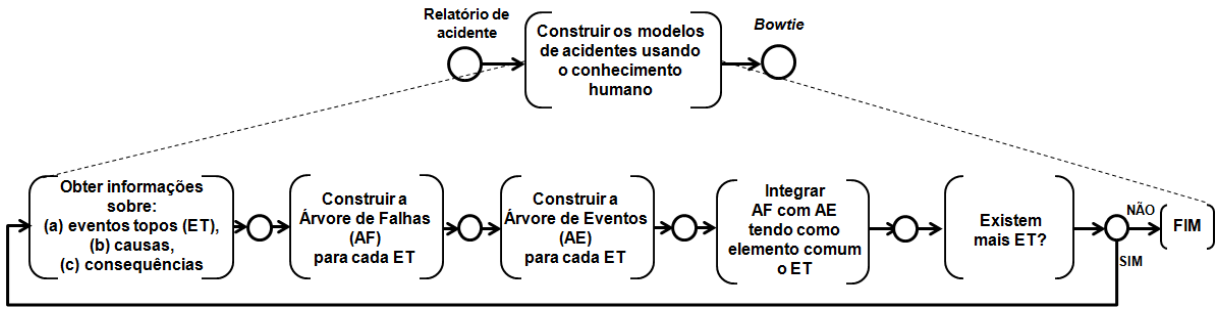
Nesta etapa tem-se a integração dos modelos resultantes para AF e AE, obtidos a partir das etapas 3 e 5 respectivamente. A integração entre os dois modelos AF e AE é executada, considerando como elemento comum entre os dois modelos, o evento topo (ET).

3.3.2.2 Construção dos modelos de acidentes usando o conhecimento humano

Com base em relatório(s) de acidente(s) em plantas/processos semelhantes, a Figura 34 ilustra as atividades que devem ser executadas para a obtenção dos

modelos de acidentes a partir da identificação das causas precedentes (eventos críticos) à ocorrência do mesmo

Figura 34 – Processo para construção de modelos de acidentes a partir de relatório(s) de acidente(s)



Fonte: próprio autor

A seguir são descritas cada atividade deste método.

- **Obter informações sobre: (a) eventos topos (ET), (b) causas, (c) consequências.**

Esta atividade compreende a obtenção das seguintes informações de cada relatório:

(a) Definição dos eventos topos (ET) para cenários críticos ocorridos;

(b) Identificação das causas ou eventos críticos (EC_i) precursores à ocorrência do ET;

(c) Identificação das consequências indesejadas ou eventos indesejados (UE_i) observados após a ocorrência do ET.

- **Construção da árvore de Falhas (AF) para cada ET**

Esta atividade compreende as etapas para construção da AF, para cada ET. As informações fundamentais para a construção da AF são:

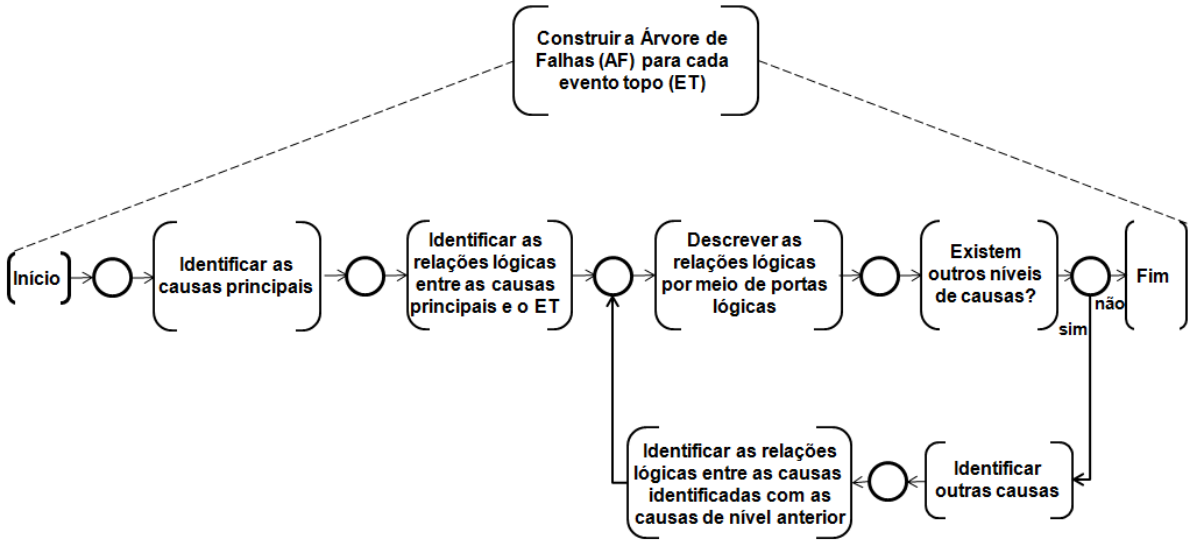
(a) Evento topo (ET); e

(b) Eventos críticos (EC) que foram identificados como causas do ET.

O método de construção da AF é hierárquico e baseia-se em uma abordagem *top-down*, partindo-se do ET para as causas ou EC. No caso onde não se tem um banco de dados que represente o conjunto de eventos ET e ECi envolvidos, esta atividade deve ser executada baseada no conhecimento humano para se estabelecer as relações de dependência causal.

Um processo em PFS, mostrado na Figura 35, é proposto para a construção da árvore de Falhas (AF) para cada ET.

Figura 35 – Processo para construção da AF para cada ET



Fonte: próprio autor

- **Construção da árvore de Eventos (AE) para cada ET**

Esta atividade compreende as etapas para construção da AE, para cada ET. As informações fundamentais para a construção da AE são:

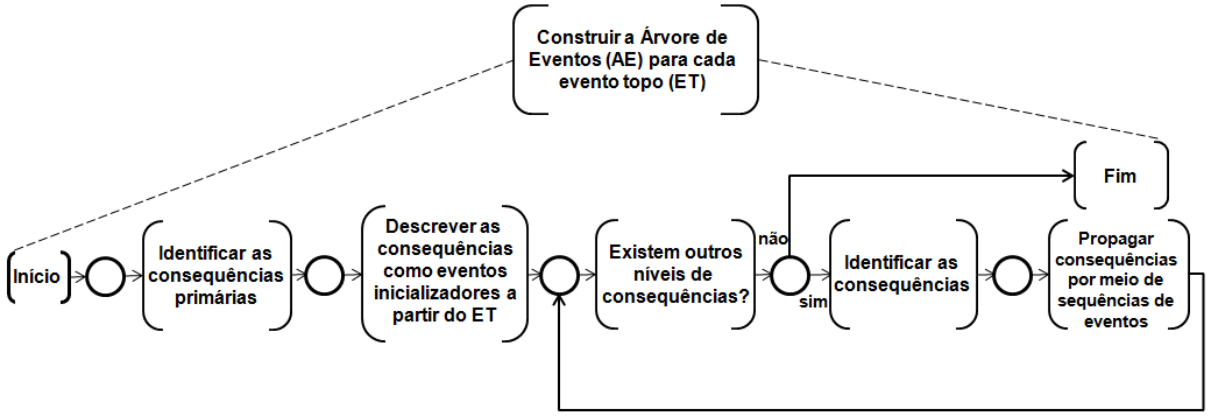
(c) Evento topo (ET); e

(d) Eventos indesejados (UE) que foram identificados como consequências indesejadas do ET.

O método de construção da AE é semelhante ao método de construção da AF, ou seja, é hierárquico e baseia-se em abordagem *top-down*, partindo do ET para as consequências ou UE. No caso onde não se tem um banco de dados que represente o conjunto de estados dos ET e UE envolvidos, esta atividade deve ser executada baseada no conhecimento humano para se estabelecer as relações de dependência causa x efeito.

Um processo em PFS, mostrado na Figura 36, é proposto para a construção da árvore de eventos (AE) para cada evento topo (ET).

Figura 36 – Processo para construção da AE para cada ET



Fonte: próprio autor

- **Integrar AF com AE**

Esta atividade compreende a integração dos modelos AF e AE tendo como elemento comum em ambos os modelos, o evento topo (ET). Esta atividade deve ser realizada para cada ET.

O resultado esperado com a integração destes modelos é a obtenção do diagrama de *bowtie* que representa um cenário de acidente.

A construção dos diagramas de *bowtie* é baseada assim no conhecimento de especialistas. Um método baseado nesta abordagem pode ser encontrado em (HENLEY e KUMAMOTO, 1981).

- **Existência ou não de mais eventos topos (ET)**

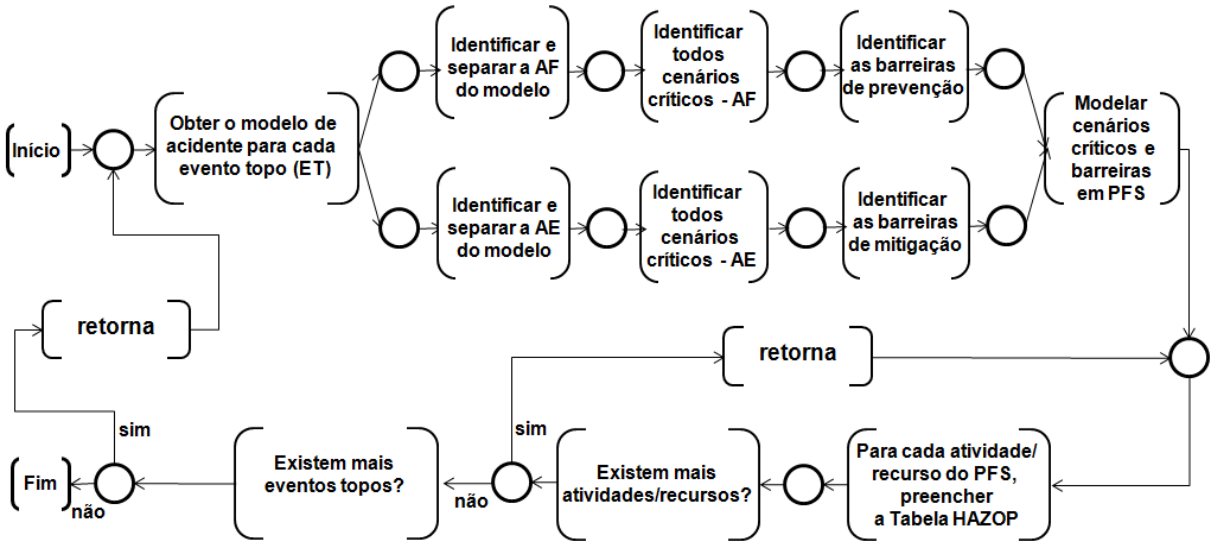
As atividades relacionadas com a construção da AF, construção da AE e integração da AF com AE, devem ser repetidas para cada ET identificado a partir do(s) relatório(s) de acidente(s) obtidos.

3.3.3 Fase 3 – Integração dos modelos de acidentes com HAZOP

A Fase 3 compreende as atividades do processo de integração dos modelos de acidentes com o HAZOP.

As atividades do processo de integração são apresentadas em PFS, conforme mostra a Figura 37.

Figura 37 – Processo para integração dos modelos de acidentes com HAZOP



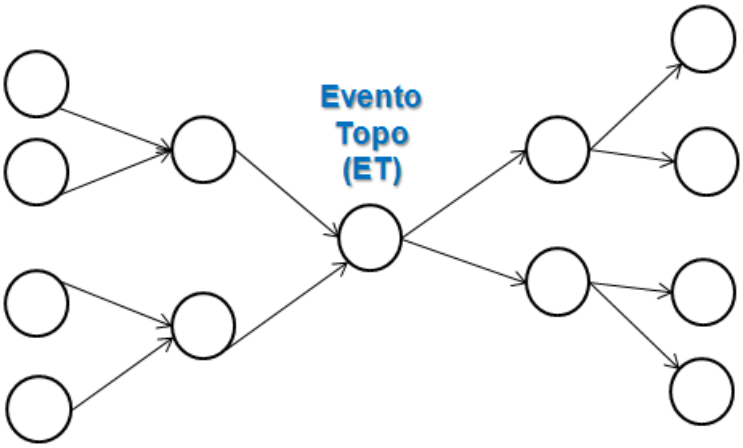
Fonte: próprio autor

A seguir serão descritas cada uma das atividades da Figura 37.

3.3.3.1 Obter o modelo de acidente para cada evento topo (ET)

Esta atividade procura obter o modelo de acidente, ou seja, o diagrama de *bowtie* para cada evento topo identificado. A Figura 38 mostra um exemplo de modelo de acidente para um evento topo (ET).

Figura 38 - Exemplo de um modelo de acidente para um evento topo (ET)

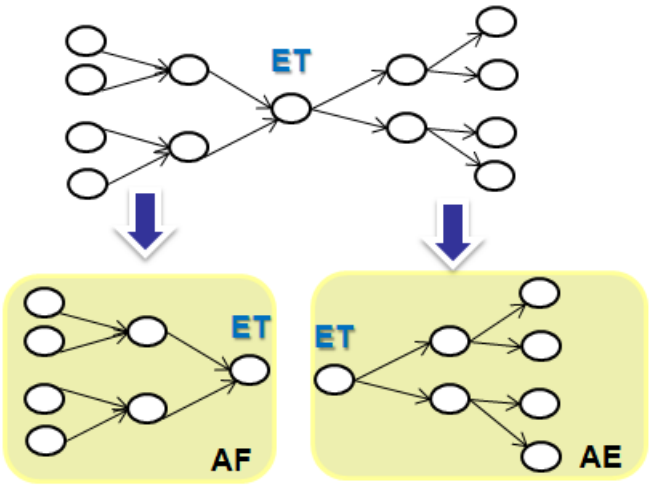


Fonte: próprio autor

3.3.3.2 Identificar e separar a AF e AE de cada modelo

As atividades de identificação e separação das árvores de falhas (AF) e das árvores de eventos (AE) devem ser executadas para cada modelo de acidente. Elas podem ser realizadas paralelamente, conforme método mostrado na Figura 37. Um exemplo destas atividades é mostrado na Figura 39.

Figura 39 – Separação da AF e AE para cada modelo de acidente obtido

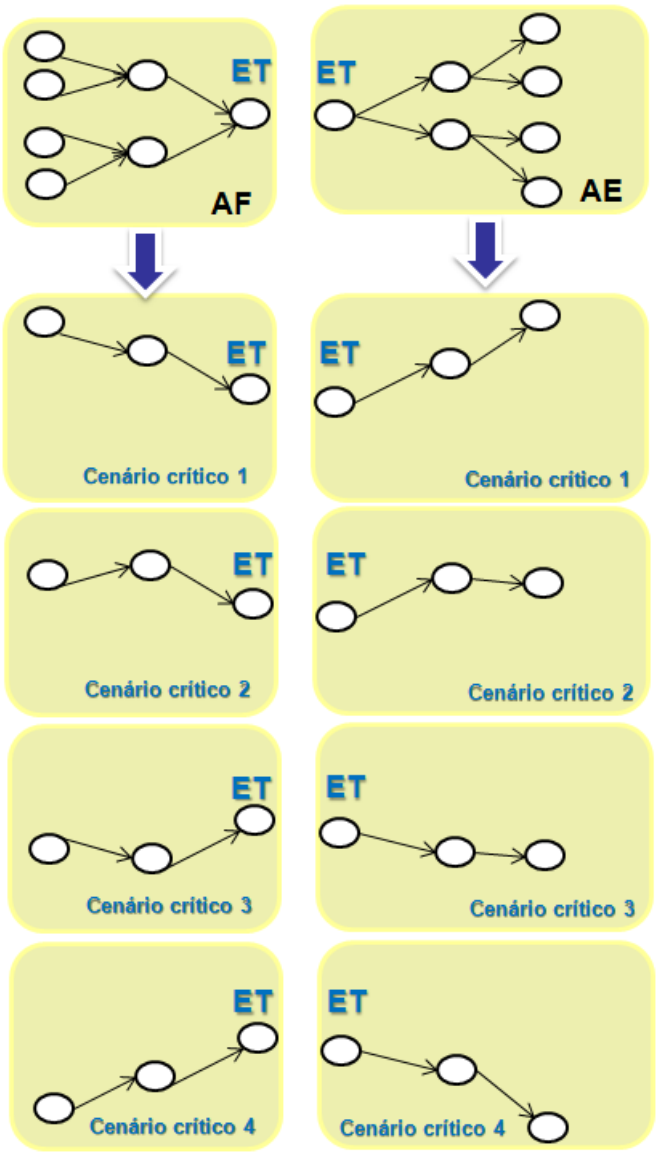


Fonte: próprio autor

3.3.3.3 Identificar todos os cenários críticos pertinentes à AF e AE

Estas atividades procuram identificar todos os cenários críticos a partir das AF e AE; dado um modelo de acidente. Um cenário crítico é um caminho crítico que representa uma possível concatenação de eventos críticos ou eventos indesejados. No caso da AF, o cenário crítico representa uma concatenação de eventos críticos até se obter o evento topo (ET). Por outro lado, no caso da AE, o cenário crítico representa uma concatenação de eventos indesejados, a partir do ET até se obter um resultado indesejado da planta/processo. Um exemplo destas atividades é mostrado na Figura 40.

Figura 40 – Identificação dos cenários críticos a partir da AF e AE



Fonte: próprio autor

3.3.3.4 Identificar as barreiras de prevenção e mitigação

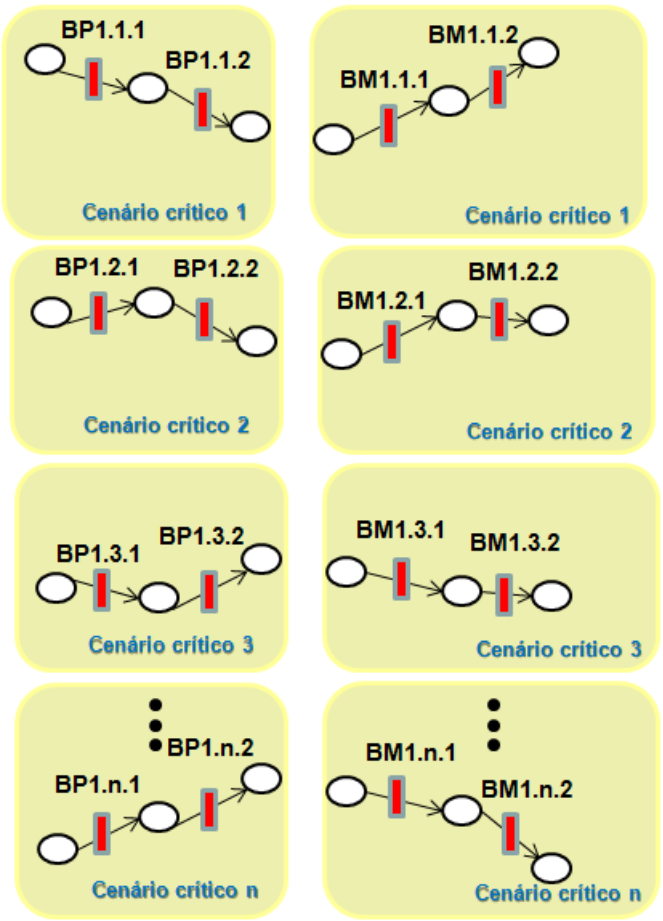
Estas atividades procuram identificar as barreiras de prevenção e mitigação de eventos críticos e/ou indesejados a partir de cada cenário crítico identificado para cada AF e AE, respectivamente.

De acordo com a propriedade de diagnosticabilidade segura e dado um cenário de acidente, todos os eventos críticos e eventos indesejados identificados durante a rastreabilidade dos mesmos, devem ser observados e diagnosticados de forma não ambígua a fim de se obter um diagnóstico seguro para posterior tratamento adequado destes eventos, impossibilitando a ocorrência de eventos que possam

violar os requisitos de segurança da planta/processo (BAKOLAS e SALEH, 2011) (PAOLI e LAFORTUNE, 2005). Com base nesta propriedade, cada barreira identificada nesta atividade, deve ser a implementação da estratégia de controle para prevenção e mitigação dos eventos críticos e/ou indesejados. Cada estratégia de controle compreende a forma de como diagnosticar de forma não ambígua o evento crítico/indesejado e as ações a serem tomadas para evitar a ocorrência do evento crítico/indesejado posterior à barreira.

Ainda de acordo com as normas IEC 61508(IEC 61508, 2010) e IEC 61511(IEC 61511, 2003), as barreiras de prevenção e mitigação no contexto deste trabalho, estão relacionadas às funções de segurança a serem realizadas por EEP e/ou outros equipamentos relacionados à segurança funcional. Em outras palavras, cada função de segurança corresponde a uma estratégia de controle que é definida pelo time de especialistas durante a fase de identificação e análise de riscos do projeto de SCSP. Um exemplo destas atividades é mostrado na Figura 41.

Figura 41 – Identificação das barreiras de prevenção e mitigação a partir dos cenários críticos



Fonte: próprio autor

As barreiras de prevenção e mitigação na Figura 41 são indicadas pelas barras vermelhas. O endereçamento das mesmas segue a formatação descrita na subseção 3.4.1.6. Cada cenário crítico com a identificação das barreiras corresponde a um diagrama de barreiras(DUIJM, 2009).

3.3.3.5 Modelagem dos cenários críticos e barreiras em PFS

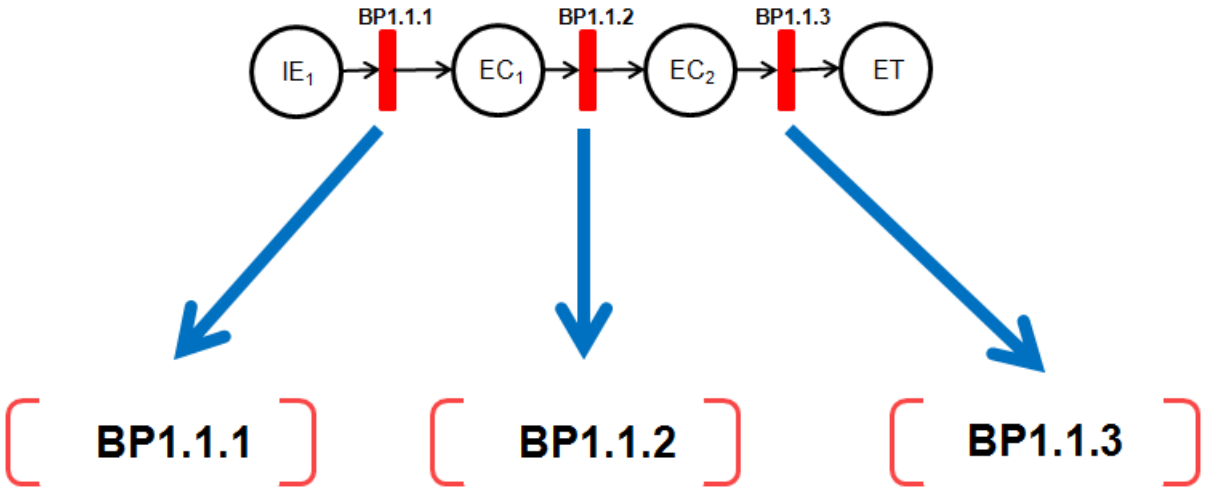
Nesta atividade se realiza a modelagem em PFS de cada cenário crítico considerando as barreiras identificadas para cada cenário crítico. Aqui o foco está:

- Na identificação da nova classe de barreiras reativas para integração com a Tabela de HAZOP, e
- Na descrição do comportamento do conjunto de barreiras reativas propostas, e dos algoritmos que desempenham a função de cada uma destas barreiras.

A. Identificação das Barreiras Reativas

Um exemplo de diagrama de barreiras para cada cenário crítico, assim como, suas respectivas barreiras de segurança são ilustradas na Figura 42.

Figura 42 – Exemplo de um diagrama de barreiras para um cenário crítico e barreiras de segurança em PFS



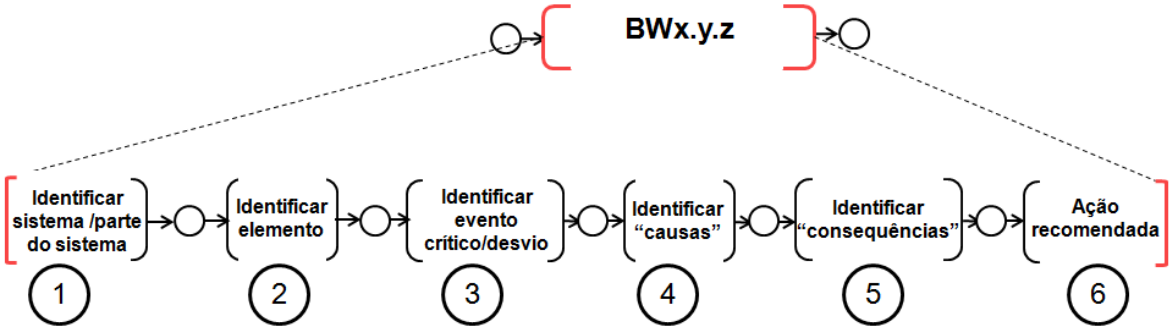
Fonte: próprio autor

Inicialmente, cada barreira de segurança identificada para cada cenário crítico, é modelada como uma atividade em PFS.

Cada `atividade` BPx.y.z é então refinada em uma sequência de `atividades` a serem executadas para a implementação de cada barreira de segurança em questão, conforme ilustrado na Figura 43. A descrição dessas `atividades` é apresentada a seguir:

- A `atividade` 1 corresponde à identificação do sistema ou parte do sistema da planta/processo (objeto de controle).
- A `atividade` 2 corresponde à identificação do elemento que é usado para identificar características essenciais do objeto de controle. A definição de elemento segundo a norma (IEC 61882, 2003) foi descrita na seção 3.3.1.4.
- A `atividade` 3 corresponde à identificação do evento crítico ou evento indesejado, que pode ser um desvio de parâmetro ou falha do elemento analisado.
- A `atividade` 4 corresponde à identificação das possíveis causas do evento crítico/indesejado, assim como, a definição de recursos para detecção e diagnóstico destas causas de forma não ambígua; segundo a propriedade de diagnosticabilidade segura.

Figura 43 – Refinamento da `atividade` BWx.y.z



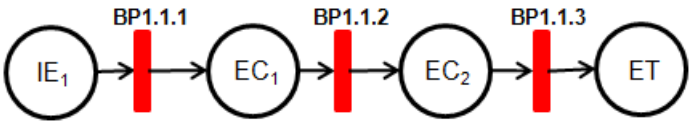
Fonte: próprio autor

- A `atividade` 5 corresponde à identificação das possíveis consequências ocorridas após a ocorrência do evento crítico/indesejado, assim como, a definição de recursos para detecção e diagnóstico destas consequências de forma não ambígua.
- Por fim, a `atividade` 6 orienta a definição da estratégia de controle de segurança, ou seja, um conjunto de medidas de segurança a serem tomadas para reduzir ou eliminar a probabilidade de ocorrência das causas identificadas (abordagem baseada em prevenção) e/ou mitigar ou reduzir as consequências identificadas (abordagem baseada em mitigação).

B. Descrição conceitual do comportamento das Barreiras Reativas

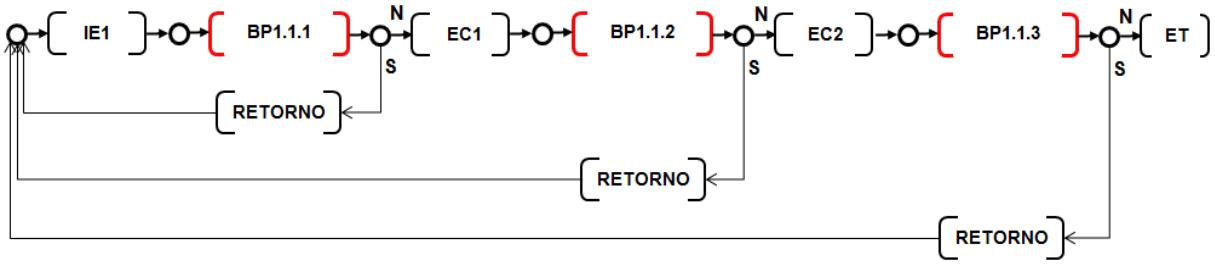
Com base no diagrama de barreiras de um cenário crítico que representa o sequenciamento de ocorrência de eventos críticos/indesejados, dado o evento inicial (IE) até culminar no evento topo (ET); pode-se derivar um modelo PFS que representa a relação de `atividades` associadas aos eventos críticos/indesejados e as barreiras de segurança envolvidas com estes eventos. A execução de cada `atividade` associada à cada barreira de segurança pode ser assim devidamente verificada. Se a barreira de segurança atua de forma satisfatória, o modelo em PFS descreve o retorno do cenário a um estado inicial, aguardando a ocorrência de novos eventos e garantindo a segurança desejada, caso contrário, ou seja, se a barreira de segurança não atua de forma satisfatória, o modelo em PFS descreve a evolução para o próximo evento e o acionamento da próxima barreira de segurança, sucessivamente, até culminar no ET, se todas as barreiras de segurança falharem em suas funções. A Figura 44 ilustra o cenário crítico 1 representado como um diagrama de barreiras, e a Figura 45 o modelo PFS correspondente.

Figura 44 – Diagrama de barreiras para o cenário crítico 1



Fonte: próprio autor

Figura 45 – Modelo do cenário crítico 1 em PFS



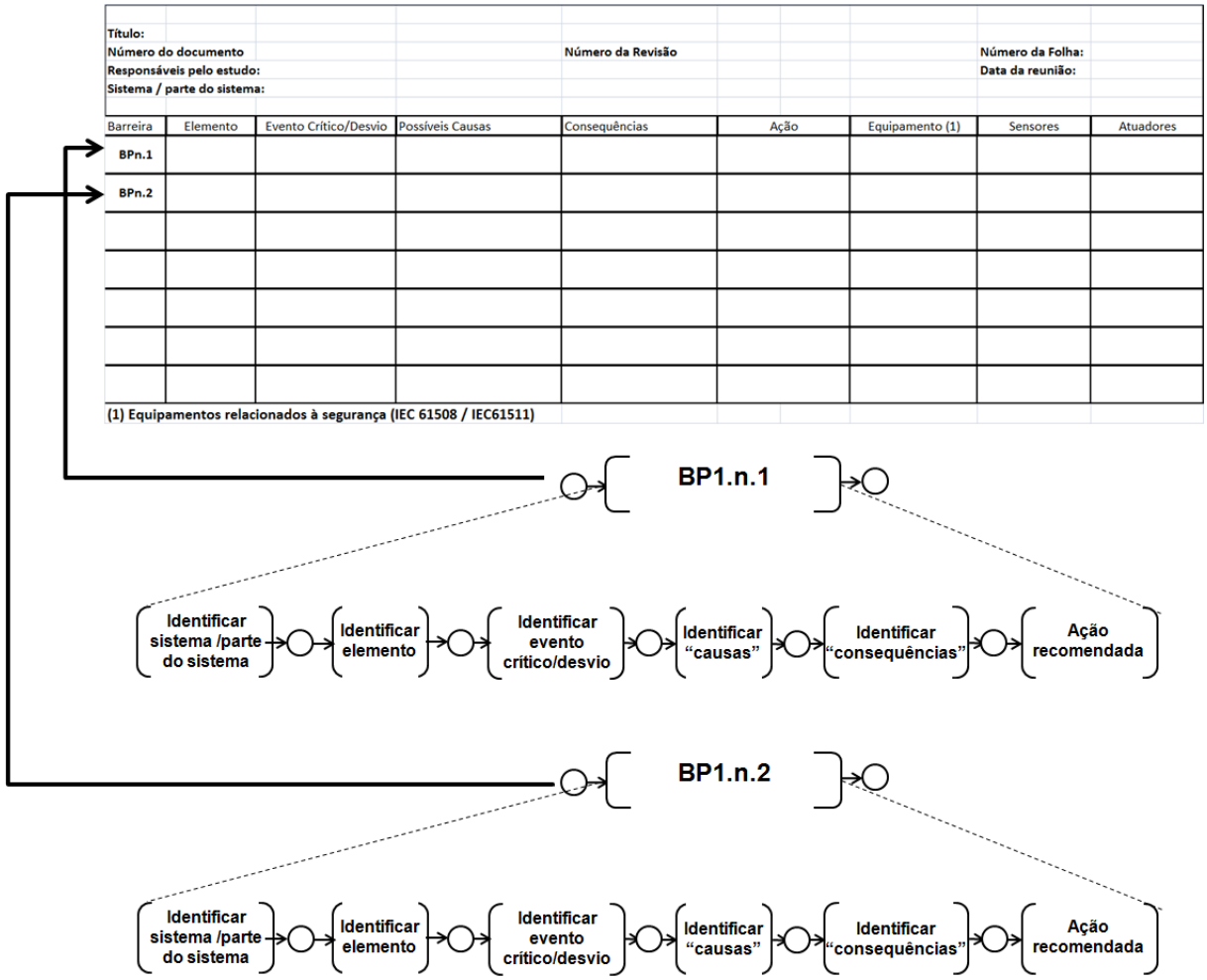
Fonte: próprio autor

3.3.3.6 Para cada atividade/recurso do PFS, preencher a tabela de HAZOP

Com base nos modelos em PFS de cada cenário crítico obtido anteriormente, associa-se agora cada `atividade` e respectivos recursos com uma linha da tabela de HAZOP. A Figura 46 mostra um exemplo de como se preenche a tabela de HAZOP para duas barreiras de prevenção BP1.n.1 e BP1.n.2.

As atividades 1, 2, 3, 4, 5 e 6 indicadas na Figura 43 correspondem às informações relativas às colunas 1, 2, 3, 4, 5 e 6 da tabela de HAZOP (Tabela 1).

Figura 46 – Preenchimento da Tabela de HAZOP



Fonte: próprio autor

3.3.3.7 Existência ou não de mais atividades/recursos

A atividade descrita em 3.3.3.6 deve ser repetida para cada `atividade`/recursos existente em cada cenário de acidente, até que não exista mais `atividade`/recursos.

3.3.3.8 Existência ou não de mais ET

As atividades descritas em 3.3.3.1 até 3.3.3.7 deverão ser repetidas para cada evento topo, até que não existam mais eventos topos (ETs).

3.3.4 Fase 4 – Geração dos algoritmos de defesa de prevenção e mitigação de falhas críticas

A partir da identificação das barreiras reativas, adota-se aqui um procedimento para o desenvolvimento dos algoritmos de defesa de prevenção e mitigação de falhas críticas (ET).

O procedimento é constituído pelos passos descritos abaixo:

Passo 1 – Coleta/listagem de todos os modelos de cenários críticos em PFS derivados da AF e com as barreiras de prevenção (exemplo Figura 45).

Passo 2 - Para cada cenário crítico de prevenção em PFS, detalhar as `atividades` correspondentes às barreiras de prevenção em modelos MFG que representam os algoritmos de defesa para tratamento dos eventos iniciadores (IE) e críticos (EC) com base nas ações identificadas no HAZOP. Os atuadores a serem considerados, são obtidos também a partir do estudo de HAZOP realizado na Fase 3.

Passo 3 - Para cada cenário crítico (de prevenção), detalhar o processo de diagnóstico de cada evento iniciador/crítico em um modelo em PFS, com base no HAZOP.

Passo 4 – Para cada modelo em PFS que representa o processo de diagnóstico obtido no passo 3, refinar a `atividade` de detecção e filtragem de sinais espúrios de cada evento iniciador/crítico, em um modelo MFG correspondente. Os sensores a serem considerados, são obtidos a partir do HAZOP realizado na Fase 3.

Passo 5 - Integrar os modelos MFG de detecção e filtragem de eventos iniciadores/críticos, gerados no passo 4, com os modelos MFG correspondentes ao tratamento destes eventos gerados no passo 2.

Passo 6 - Verificar as propriedades de segurança e vivacidade de cada modelo resultante da integração obtida pelo Passo 5.

Passo 7 - Integrar os modelos de diagnóstico e defesa para prevenção de cada evento iniciador/crítico. Como resultado obtêm-se o modelo funcional do algoritmo de defesa de prevenção da falha crítica (ET) referente a cada cenário crítico.

Passo 8 - Verificar as propriedades de segurança, vivacidade e reiniciabilidade do modelo resultante da integração obtida pelo Passo 7.

Passo 9 – Coleta/listagem de todos os modelos de cenários críticos em PFS derivados da AE e com as barreiras de mitigação.

Passo 10 - Para cada cenário crítico de mitigação em PFS, detalhar as `atividades` correspondentes às barreiras de mitigação em modelos MFG que representam os algoritmos de defesa para tratamento dos eventos indesejados (UE) com base nas ações identificadas no HAZOP. Os atuadores a serem considerados, são obtidos também a partir do estudo de HAZOP realizado na Fase 3.

Passo 11 - Para cada cenário crítico (de mitigação), detalhar o processo de diagnóstico de cada evento indesejado em um modelo em PFS, com base no HAZOP.

Passo 12 – Para cada modelo em PFS que representa o processo de diagnóstico obtido no passo 11, refinar a `atividade` de detecção e filtragem de sinais espúrios de cada evento indesejado, em um modelo MFG correspondente. Os sensores a serem considerados, são obtidos a partir do HAZOP realizado na Fase 3.

Passo 13 - Integrar os modelos MFG de detecção e filtragem de eventos indesejados, gerados no passo 12, com os modelos MFG correspondentes ao tratamento destes eventos gerados no passo 10.

Passo 14 - Verificar as propriedades de segurança e vivacidade de cada modelo resultante da integração obtida pelo Passo 13.

Passo 15 - Integrar os modelos de diagnóstico e defesa para mitigação de cada evento indesejado. Como resultado, obtêm-se o modelo funcional do algoritmo de defesa de mitigação da falha crítica (ET) referente a cada cenário crítico.

Passo 16 - Verificar as propriedades de segurança, vivacidade e reiniciabilidade do modelo resultante da integração obtida pelo Passo 15.

3.4 SÍNTESE DO CAPÍTULO

A metodologia proposta para o desenvolvimento do SCSP tem como ponto de partida, a definição de uma arquitetura que considera explicitamente a segurança nas indústrias de processos.

Na sequência, foi introduzida uma extensão da classificação de sistemas de barreiras de segurança para incluir as barreiras de prevenção e mitigação que atuam de modo reativo.

Foi proposto também um *framework* para a síntese de SCSP que considera a elaboração do estudo de HAZOP de forma sistemática, a modelagem de acidentes a partir de dois cenários: (a) quando se possui banco de dados, e (b) quando se possui relatório(s) de acidente(s). O método de modelagem de acidentes a partir de banco de dados é uma extensão do trabalho de (BADREDDINE e BEN AMOR, 2013) que utilizam uma abordagem probabilística a partir de aprendizagem de redes Bayesianas usando o algoritmo de *Chow* e *Liu Tree*. Este trabalho entretanto, extende a proposta de Badreddine e Bem Amor (2013) para incluir a técnica de imputação de dados, de modo a considerar e tratar bancos de dados incompletos ou com dados faltantes que são muito comuns nas indústrias de processos(LAKSHMINARAYAN, HARP e SAMAD, 1999).

O *framework* inclui também uma sistemática para a geração de algoritmos de defesa de prevenção e mitigação de falhas críticas, com base em cenários críticos em modelos baseados na técnica de rede de Petri. Estes modelos são validados com relação às propriedades de segurança, vivacidade e reiniciabilidade, e podem ser convertidos para programas em linguagens de programação para SIS e prescritas pela norma (IEC 61508, 2010).

4 EXEMPLOS DE APLICAÇÃO

O *framework* (Figura 27) proposto na seção 3.3, é aplicado em dois exemplos obtidos da literatura.

O primeiro exemplo é baseado num acidente ocorrido na unidade de isomerização da refinaria da *British Petroleum* (BP). Os dados deste acidente foram encontrados em (BAKOLAS e SALEH, 2011) e em (FERDOUS, KHAN, *et al.*, 2013).

O segundo exemplo é baseado num acidente que ocorreu em um sistema de carregamento de hidrocarbonetos na forma líquida em um caminhão tanque. Este acidente envolveu três diferentes cenários:

- Cenário (A) - Incêndio e explosão do caminhão tanque transportando hidrocarbonetos;
- Cenário (B) - Dispersão de produtos seguido de colisão entre dois veículos; e
- Cenário (C) - Transbordamento do tanque durante o carregamento do mesmo.

Aqui se considera apenas o cenário (A) com base nos dados disponíveis no trabalho de (BADREDDINE e BEN AMOR, 2013).

Neste capítulo, o *framework* será aplicado no primeiro exemplo de aplicação. A aplicação do mesmo *framework* para o segundo exemplo de aplicação é mostrada no Apêndice D.

4.1 EXEMPLO DE APLICAÇÃO 1

Na Figura 47 são ilustradas algumas imagens do acidente ocorrido na unidade de isomerização da refinaria da *British Petroleum* (BP) na cidade do Texas nos Estados Unidos, em 23 de março de 2005. Segundo dados obtidos de relatórios de investigação, este acidente provocou a morte de aproximadamente 15 pessoas e o ferimento de mais de 180 pessoas (FERDOUS, KHAN, *et al.*, 2013).

Figura 47 – Acidente ocorrido na unidade de isomerização da refinaria BP

(a) Explosão na planta de isomerização da refinaria BP – cidade do Texas nos Estados Unidos.

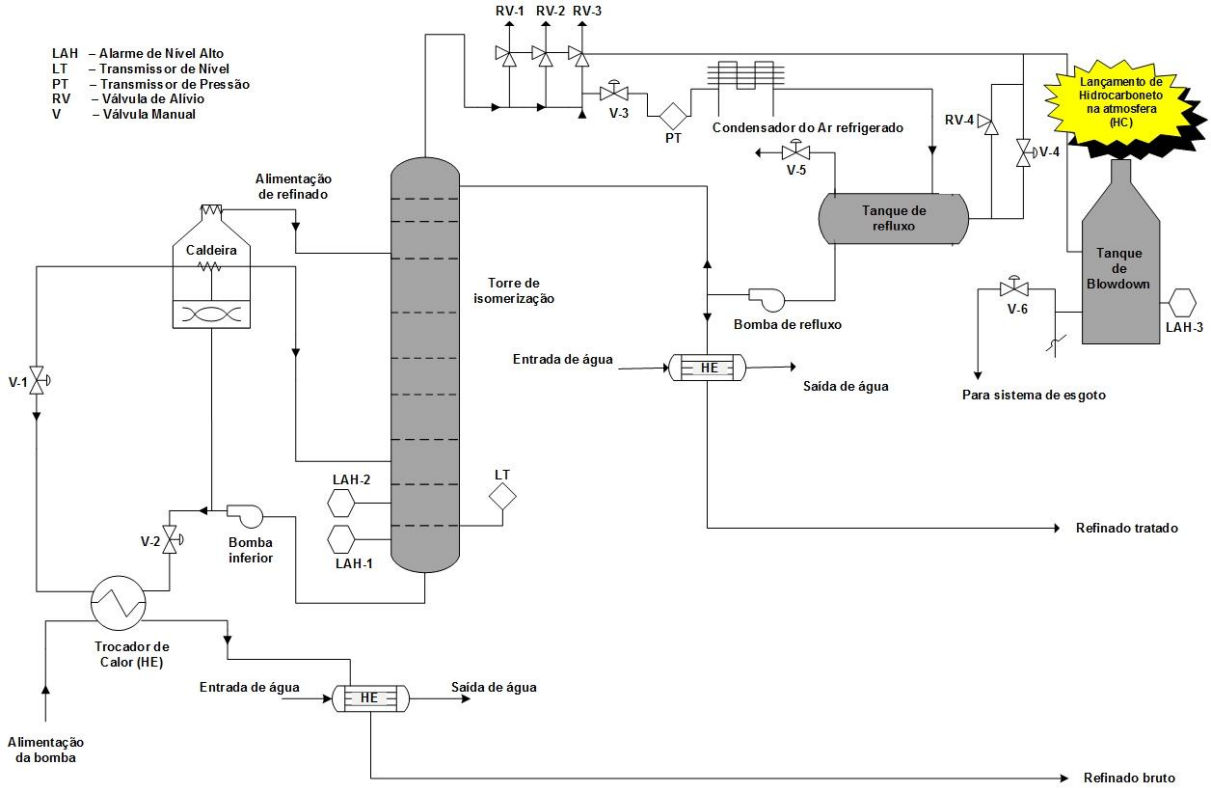
(b) Local onde estavam localizados os trailers que funcionavam como escritórios das empresas contratadas.

Fonte: (http://inspecaoequipto.blogspot.com.br/2013/05/caso-010-explosao-em-unidade-de.html. Acesso em 10/04/15)

Em (BAKOLAS e SALEH, 2011), estão disponíveis os dados dos relatórios de investigação do acidente. Em (FERDOUS, KHAN, *et al.*, 2013), estão disponibilizados dados como o diagrama de processos e de instrumentação (P&ID) da unidade de isomerização e a descrição do processo, assim como, um diagrama de *bowtie*. Não foram encontrados dados sobre os registros históricos de falhas relacionados com este acidente.

O incêndio seguido de explosão ocorreu na unidade de isomerização (ISOM) da refinaria. O acidente envolveu o derramamento de combustível refinado do tanque de *blowdown,* durante o processo de repartida da unidade (FERDOUS, KHAN, *et al.*, 2013). A explosão ocorreu devido a liberação de grande quantidade de hidrocarboneto (HC) altamente inflamável na atmosfera a partir do tanque de *blowdown*. O lançamento de HC na atmosfera formou uma nuvem de vapor dos gases, que explodiu na presença de uma fonte de ignição, proveniente de um caminhão diesel estacionado próximo à unidade com os motores ligados(FERDOUS, KHAN, *et al.*, 2013). A Figura 48 mostra o diagrama de processos e de instrumentação (P&ID) desta unidade.

Figura 48 – Lançamento de HC da Unidade de ISOM que resultou no acidente



Fonte: adaptado de (FERDOUS, KHAN, *et al.*, 2013)

Descreve-se a seguir a aplicação do framework para a síntese do sistema de controle relacionado à segurança (SCSP).

4.1.1 *Framework* para a síntese do SCSP

4.1.1.1 Fase 1 – Método para elaboração do HAZOP

Para este exemplo de aplicação, o HAZOP da unidade de ISOM já existe, assim a `atividade` aqui se resume em organizar a tabela de HAZOP de acordo com a estrutura indicada na Tabela 1.

4.1.1.2 Fase 2 – Método para elaboração dos modelos de acidentes

Considerando a disponibilidade de um registro de histórico de falhas, e apesar deste possuir dados ausentes/faltantes devido à observabilidade parcial de alguns eventos críticos e/ou indesejados, a construção do modelo pode ser realizada usando abordagem probabilística via algoritmo de aprendizagem bayesiana.

Etapa 1 – Definição inicial

- **Definição da planta/processo**

A planta/processo a ser considerado é a unidade de ISOM, assim como seus dispositivos de realização de controle básico (SCBP). Este conjunto é o objeto de controle para o SCSP.

- **Definição do time de especialistas:**

O time selecionado é constituído por engenheiros de processos, operadores de processos e engenheiros de segurança de processos. Este time possui conhecimento multidisciplinar sobre a planta/processo e sobre as normas de segurança de processos em indústrias de processos, como as normas (IEC 61511, 2003) e (IEC 61508, 2010).

- **Definição da documentação do projeto:**

A documentação básica foi coletada de (FERDOUS, KHAN, *et al.*, 2013), como por exemplo, o P&ID da unidade de ISOM da refinaria BP (Figura 48).

- **Registros históricos de falhas:**

(BAKOLAS e SALEH, 2011) e (FERDOUS, KHAN, *et al.*, 2013), não apresentam explicitamente os registros históricos de falhas. Por outro lado, como a abordagem deste trabalho endereça a modelagem de acidentes considerando bancos de dados incompletos ou com dados faltantes, correspondentes aos eventos críticos e/ou indesejados observados e parcialmente observados, os bancos de dados de treinamentos BDT_{AF} e BDT_{AE}, que consideram dados faltantes ou incompletos, foram obtidos de forma sistemática via procedimentos descritos nos Apêndice A e Apêndice B deste trabalho.

- **Etapa 2 - Aprendizagem da estrutura da árvore de falhas (AF)**

Subetapa 2.1 – Montagem do banco de dados de treinamento (BDT_{AF})

As amostras aleatórias de dados completos obtidas via Simulação Monte Carlo, foram obtidas de acordo com o procedimento descrito no Apêndice A. Adicionalmente, foram gerados artificialmente bancos de dados incompletos com 5%, 10%, 15%, 20%, 25% e 30% de dados faltantes, via algoritmo para remoção completamente aleatória de dados (MCAR) descrito no Apêndice B.

Ainda com base no resultado do estudo de fiabilidade de modelos de acidentes aprendidos via imputação de dados e abordagem bayesiana, considerando bancos

de dados faltantes, e que é apresentado no Apêndice C deste trabalho, considera-se neste exemplo de aplicação, que o BDT_{AF} possui 20% (vinte por cento) de dados faltantes.

O BDT_{AF} resultante possui 1024 linhas por 18 colunas. A Tabela 2 mostra parte do BDT_{AF} (com dados incompletos ou faltantes), usado para aprendizagem da AF. Nesta tabela, o evento topo (ET) é denominado de HC, e as colunas restantes correspondem aos eventos iniciadores (IE_i) e críticos (EC_i) como "causas" observadas ou parcialmente observadas antes da ocorrência do ET, em qualquer combinação, como por exemplo: IE2, IE1, IE3, IE5, IE4, IE6, IE7, IE9, IE10, IE8, EC1 = LAF, EC2 = OFC, EC3 = LICA, EC4 = EFFDT, EC5 = EFFRD, EC6 = OBD e EC7 = EFBD. A descrição dos IE_i e EC_i é mostrada na Figura 49.

Figura 49 – Descrição das "causas" do HC.

Acrônimo	Descrição das "causas"
IE1	Falha de alarme 1 de nível alto de refinado na torre de ISOM (LAH-1)
IE2	Falha de alarme 2 de nível alto do refinado na torre de ISOM (LAH-2)
IE3	Falha na leitura do transmissor de nível LT
IE4	Alarme de nível alto 1 ignorado pelo operador
IE5	Alarmes de temperatura ignorados pelo operador
IE6	Falha no fechamento da válvula RV-4
IE7	Falha da bomba de refluxo
IE8	Falha no fechamento das válvulas RV-1,2,3
IE9	Falha na abertura da válvula V-6
IE10	Falha de alarme de nível alto no tanque de blowdown (LAH-3)
EC1 = LAF	Falhas de alarme de nível (N-1)
EC2 = OFC	Falhas na operação (N-2)
EC3 = LICA	Falhas LICA (N-3)
EC4 = EFFDT	Excesso de alimentação da torre ISOM (N—4)
EC5 = EFFRD	Excesso de alimentação do tanque de refluxo (N-5)
EC6 = OBD	Nível de refinado acima do nível máximo permitido dentro do tanque de *blowdown* (N-7)
EC7 = EFBD	Excesso de alimentação do tanque de *blowdown* (N-6)

Fonte: adaptada de (FERDOUS, KHAN, *et al.*, 2013)

Cada linha ou instância da matriz mostrada na Tabela 2, contém um valor binário (ex: 0 / Falso ou 1 / Verdadeiro) para o HC e para cada IE / EC que foi observado. Entretanto, para os IE_S / EC_s ou "causas" que não foram observados em algumas instâncias, os valores contidos no BDT_{AF} para estes eventos, não contém valores binários e são representados como "NA" (do termo em inglês "*Not Available*").

Tabela 2 – Parte do banco de dados de treinamento com vinte por cento (20%) de dados faltantes para aprendizagem da árvore de falhas (AF)

HC	IE2	IE1	IE3	IE5	IE4	IE6	IE7	IE9	IE10	IE8	LAF	OFC	LICA	EFFDT	EFFRD	OBD	EFBD
1	0	1	0	0	0	0	0	1	0	NA	NA	0	0	0	0	0	1
1	NA	1	0	0	1	0	NA	1	0	0	1	0	NA	NA	0	0	1
NA	1	NA	1	0	1	1	1	0	0	1	0	NA	0	0	NA	1	1
NA	NA	0	1	NA	0	1	0	1	NA	0	0	0	0	0	1	1	1
1	0	0	1	0	1	0	NA	0	0	0	0	NA	0	0	1	1	0
1	1	1	0	1	0	0	1	NA	0	1	1	NA	0	0	1	NA	1
1	1	0	0	0	1	0	1	NA	0	NA	NA	0	0	0	1	NA	1
1	1	0	0	1	0	NA	0	1	0	0	0	0	NA	NA	1	1	NA
1	0	NA	0	0	NA	1	0	NA	1	0	NA	0	0	0	1	NA	1
NA	0	0	0	0	0	0	0	0	0	1	NA	0	0	0	0	0	1
1	1	1	0	0	NA	NA	NA	NA	1	0	1	NA	0	0	1	1	1
1	0	1	0	0	0	1	1	0	0	0	0	NA	0	0	1	1	0
1	NA	1	1	0	0	1	0	1	NA	0	1	0	1	0	NA	1	1
1	1	0	1	0	1	0	1	NA	NA	0	0	NA	0	0	1	1	1
1	1	0	NA	1	0	1	NA	0	0	1	0	NA	0	0	NA	1	NA
1	1	1	NA	0	0	1	0	0	0	1	1	NA	NA	0	1	NA	1
1	1	0	1	1	0	NA	1	1	1	NA	0	0	0	NA	1	1	1
1	0	1	0	1	1	0	1	1	1	0	0	1	0	0	1	1	1
1	1	0	1	0	NA	0	1	NA	1	1	0	0	0	0	1	1	1
1	0	NA	0	0	1	1	0	0	NA	0	0	0	NA	0	1	NA	0
1	NA	0	1	0	0	NA	0	1	0	1	0	0	0	0	NA	NA	1
1	1	0	NA	0	0	1	0	NA	1	1	NA	0	0	0	1	1	1
1	1	1	0	1	1	1	0	1	1	0	1	1	0	NA	1	NA	1
1	NA	0	NA	1	0	1	NA	0	NA	0	0	NA	0	0	1	1	NA
NA	1	0	NA	1	0	1	1	0	0	1	0	NA	0	0	NA	1	NA
1	1	1	1	NA	0	0	1	0	0	0	1	0	NA	0	1	1	0
1	1	NA	1	0	NA	0	0	1	0	1	1	0	NA	0	0	NA	1
1	NA	NA	1	0	0	1	0	1	0	0	0	0	0	0	1	1	1
NA	NA	0	0	1	0	0	NA	NA	1	0	0	NA	0	0	1	NA	1
1	1	NA	1	1	1	0	0	1	NA	0	0	NA	0	0	0	NA	NA
1	0	NA	0	NA	0	0	1	0	NA	1	0	0	0	0	1	1	1
NA	1	1	1	1	1	NA	1	NA	NA	1	NA	1	1	1	1	NA	1
1	1	1	0	0	NA	1	NA	0	0	1	1	NA	0	NA	1	1	1
NA	0	0	0	1	0	0	1	1	0	1	NA	0	0	0	NA	1	1
0	1	0	NA	NA	0	0	0	0	0	0	NA	0	0	0	0	0	0
1	NA	1	1	1	NA	0	NA	0	1	1	0	0	0	0	0	0	NA
1	NA	1	0	0	0	1	0	1	NA	0	1	NA	0	0	1	NA	1
1	1	1	1	NA	1	0	1	1	0	0	1	1	1	1	NA	NA	1
1	1	1	0	0	1	0	NA	0	1	1	1	0	0	0	0	0	1
NA	0	NA	0	0	1	0	1	NA	0	0	0	0	0	0	1	1	0
1	0	NA	1	1	0	0	0	0	1	0	0	0	0	0	0	0	1
1	0	1	0	1	NA	1	NA	0	1	NA	0	0	0	0	1	1	1
1	0	1	0	0	1	0	NA	0	1	0	0	NA	0	0	1	1	1
1	1	0	1	0	1	0	0	1	1	0	0	0	0	0	0	0	1
1	1	1	0	0	0	1	1	0	0	1	1	0	0	0	1	1	1
1	NA	1	0	0	NA	1	0	NA	1	0	1	NA	0	0	1	1	1
1	1	NA	1	1	0	NA	1	1	0	1	NA	0	1	0	1	1	1
1	0	0	0	1	1	0	0	1	0	1	0	1	0	0	NA	NA	1
1	0	1	0	1	1	1	1	1	NA	1	0	1	0	0	1	1	1
1	1	1	0	NA	1	1	0	0	0	1	1	1	0	NA	1	1	1

Fonte: próprio autor

Subetapa 2.2 – Imputação de Dados

A imputação dos dados faltantes do BDT_{AF} por valores “plausíveis” é realizada via algoritmo MICE que pode ser acionado via um software computacional estatístico R. A versão do software computacional estatístico R utilizada neste trabalho foi a 3.2.4 e a versão do MICE para R foi a 3.25. O BDT_{AF} (com dados incompletos/faltantes) obtido na subetapa 2.1, é convertido para um arquivo com formato texto (*.txt*), para ser importado para o software computacional estatístico R. O comando para a execução da imputação de dados tem o seguinte formato:

$$imp1 \leftarrow mice(BDT_{AF}, defaultMethod=c(\text{“pmm”}))$$

Um resumo das informações pertinentes à parametrização do processo de imputação, é mostrado na Figura 50.

Figura 50 – Resumo de informações do processo de imputação via MICE

```
> print(imp1)
Multiply imputed data set
Call:
mice(data = BDTAF, Defaultmethod = c("pmm"))
Number of multiple imputations:  5
Missing cells per column:
   TE   IE2   IE1   IE3   IE5   IE4   IE6   IE7   IE9  IE10   IE8   LAF   OFC  LICA EFFDT EFFRD   OBD
  206   213   205   192   201   202   211   188   204   219   194   206   240   197   190   197   216
 EFBD
  205
Imputation methods:
   TE   IE2   IE1   IE3   IE5   IE4   IE6   IE7   IE9  IE10   IE8   LAF   OFC  LICA EFFDT EFFRD   OBD
"pmm" "pmm" "pmm" "pmm" "pmm" "pmm" "pmm" "pmm" "pmm" "pmm" "pmm" "pmm" "pmm" "pmm" "pmm" "pmm" "pmm"
 EFBD
"pmm"
VisitSequence:
   TE   IE2   IE1   IE3   IE5   IE4   IE6   IE7   IE9  IE10   IE8   LAF   OFC  LICA EFFDT EFFRD   OBD
    1     2     3     4     5     6     7     8     9    10    11    12    13    14    15    16    17
 EFBD
   18
PredictorMatrix:
      TE IE2 IE1 IE3 IE5 IE4 IE6 IE7 IE9 IE10 IE8 LAF OFC LICA EFFDT EFFRD OBD EFBD
TE     0   1   1   1   1   1   1   1   1    1   1   1   1    1     1     1   1    1
IE2    1   0   1   1   1   1   1   1   1    1   1   1   1    1     1     1   1    1
IE1    1   1   0   1   1   1   1   1   1    1   1   1   1    1     1     1   1    1
IE3    1   1   1   0   1   1   1   1   1    1   1   1   1    1     1     1   1    1
IE5    1   1   1   1   0   1   1   1   1    1   1   1   1    1     1     1   1    1
IE4    1   1   1   1   1   0   1   1   1    1   1   1   1    1     1     1   1    1
IE6    1   1   1   1   1   1   0   1   1    1   1   1   1    1     1     1   1    1
IE7    1   1   1   1   1   1   1   0   1    1   1   1   1    1     1     1   1    1
IE9    1   1   1   1   1   1   1   1   0    1   1   1   1    1     1     1   1    1
IE10   1   1   1   1   1   1   1   1   1    0   1   1   1    1     1     1   1    1
IE8    1   1   1   1   1   1   1   1   1    1   0   1   1    1     1     1   1    1
LAF    1   1   1   1   1   1   1   1   1    1   1   0   1    1     1     1   1    1
OFC    1   1   1   1   1   1   1   1   1    1   1   1   0    1     1     1   1    1
LICA   1   1   1   1   1   1   1   1   1    1   1   1   1    0     1     1   1    1
EFFDT  1   1   1   1   1   1   1   1   1    1   1   1   1    1     0     1   1    1
EFFRD  1   1   1   1   1   1   1   1   1    1   1   1   1    1     1     0   1    1
OBD    1   1   1   1   1   1   1   1   1    1   1   1   1    1     1     1   0    1
EFBD   1   1   1   1   1   1   1   1   1    1   1   1   1    1     1     1   1    0
```

Fonte: próprio autor

No processo de imputação, são geradas 5 amostras de dados contendo valores estimados para cada dado faltante. Logo, faz-se necessário considerar as 5 amostras de dados para análise das mesmas. A fim de se obter os 5 bancos de dados completos a partir das 5 amostras geradas, digita-se os comandos abaixo:

BADTAF1 ← complete(imp1,1)

BADTAF2 ← complete(imp1,2)

BADTAF3 ← complete(imp1,3)

BADTAF4 ← complete(imp1,4)

BADTAF5 ← complete(imp1,5)

A Tabela 3 mostra como exemplo o BDT_{AF3} com os dados imputados.

Tabela 3 – Parte do banco de dados de treinamento (BDT_{AF3}) com dados imputados via MICE

HC	IE2	IE1	IE3	IE5	IE4	IE6	IE7	IE9	IE10	IE8	LAF	OFC	LICA	EFFDT	EFFRD	OBD	EFBD
1	0	1	0	0	0	0	0	1	0	0	0	0	0	0	0	0	1
1	1	1	0	0	1	0	0	1	0	0	1	0	0	0	0	0	1
1	1	0	1	0	1	1	1	0	1	1	0	0	0	0	1	1	1
1	0	0	1	1	0	1	0	1	1	1	0	0	0	0	1	1	1
1	0	1	1	0	1	0	1	0	0	0	0	0	0	0	1	1	0
1	1	1	0	1	0	0	1	0	1	1	1	0	0	0	1	1	1
1	1	0	0	0	1	0	1	1	0	0	0	0	0	0	1	1	1
1	1	0	0	1	0	1	0	1	0	0	0	0	0	0	1	1	1
1	0	1	1	0	1	1	0	1	1	0	0	0	0	0	1	1	1
1	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	1
1	1	1	0	0	0	1	1	1	1	0	1	0	0	0	1	1	1
1	0	1	0	0	0	1	1	0	0	0	0	0	0	0	1	1	0
1	1	1	1	0	0	1	0	1	0	0	1	0	1	0	1	1	1
1	0	0	1	0	1	0	1	1	0	0	0	0	0	0	1	1	1
1	1	0	0	1	0	1	0	1	0	1	0	0	0	0	1	1	1
1	1	1	0	0	0	1	0	0	0	1	1	0	0	0	1	1	1
1	1	0	1	1	0	0	1	1	1	1	0	0	0	0	1	1	1
1	0	1	0	1	1	0	1	1	1	0	0	1	0	0	1	1	1
1	1	0	1	1	0	0	1	1	1	1	0	0	0	0	1	1	1
1	1	1	0	0	1	1	0	0	0	0	1	0	0	0	1	1	1
1	1	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	1
1	1	0	0	0	0	1	0	0	1	1	0	0	0	0	1	1	1
1	1	1	0	1	1	1	0	1	1	0	1	1	0	0	1	1	1
1	0	0	0	1	0	1	0	0	1	0	0	0	0	0	1	1	1
1	1	0	1	1	1	1	1	0	1	1	0	1	0	0	1	1	1
1	1	1	1	0	0	0	1	0	0	1	0	0	1	0	1	1	0
1	1	1	1	0	1	0	0	1	0	1	1	0	1	0	0	0	1
1	0	1	1	0	0	1	0	1	0	0	0	0	0	0	1	1	1
1	1	0	0	1	0	0	1	1	1	0	0	0	0	0	1	1	1
1	1	0	1	1	1	0	0	1	1	0	0	1	0	0	0	0	1
1	1	1	0	1	0	0	1	0	0	1	1	0	0	0	1	1	1
1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1	1
1	1	1	0	0	1	1	0	0	0	1	1	0	0	0	1	1	1
1	0	1	1	0	1	0	1	1	0	1	0	0	0	0	1	1	1
0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	1	1	0	0	0	0	1	0	0	0	0	0	0	0	1
1	1	1	0	0	0	1	0	1	0	0	1	0	0	0	1	1	1
1	1	1	0	1	1	0	1	1	0	1	1	1	1	1	1	1	1
1	1	1	0	0	1	0	0	1	1	1	1	0	0	0	0	0	1
1	1	0	0	0	1	0	1	0	0	0	0	0	0	0	1	1	0
1	0	1	1	0	0	0	0	0	1	0	0	0	0	0	0	0	1
1	0	1	0	1	0	1	1	0	1	1	0	0	0	0	1	1	1
1	0	1	1	0	1	1	1	1	1	0	0	0	0	0	1	1	1
1	1	0	1	0	1	0	0	1	1	0	0	0	0	0	0	0	1
1	1	1	0	0	0	1	1	0	1	1	1	0	0	0	1	1	1
1	1	1	0	0	0	1	0	1	1	0	1	0	0	0	1	1	1
1	1	1	0	1	0	1	1	0	0	1	1	0	0	0	1	1	1
1	0	1	0	1	1	0	0	1	0	1	0	1	0	0	0	0	1
1	0	0	0	1	1	1	1	1	0	1	0	1	0	0	1	1	1
1	1	1	0	1	1	1	0	0	1	1	1	1	0	0	1	1	1

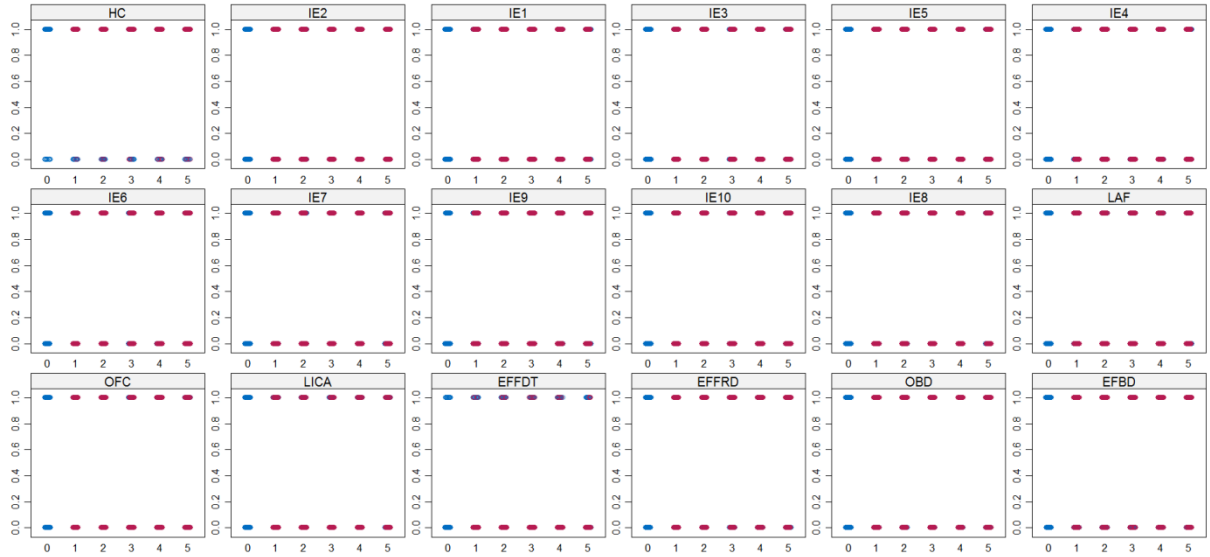
Fonte: próprio autor

De acordo com Buueren e Oudshoom (2011), deve-se inspecionar se não existem discrepâncias entre as distribuições dos dados originais (dados que foram observados) com os dados imputados via MICE no BDT_{AF}. O formato do comando para esta atividade tem o seguinte formato:

stripplot(imp1)

Gera-se assim gráficos com a distribuição de cada variável do banco de dados BDT_{AF} imputado, conforme mostra a Figura 51. Nestes gráficos, os pontos azuis representam os dados observados e os vermelhos representam os dados que foram imputados.

Figura 51 – Distribuições entre dados observados e imputados via MICE



Fonte: próprio autor

Como se pode observar na Figura 51, as distribuições entre os dados originais (pontos azuis) e os dados imputados (pontos vermelhos) são semelhantes, não existindo discrepância entre elas. Este fato está diretamente relacionado com o método de imputação selecionado. Neste sentido, o método “PMM” empregado para imputação é pertinente à aplicação envolvida.

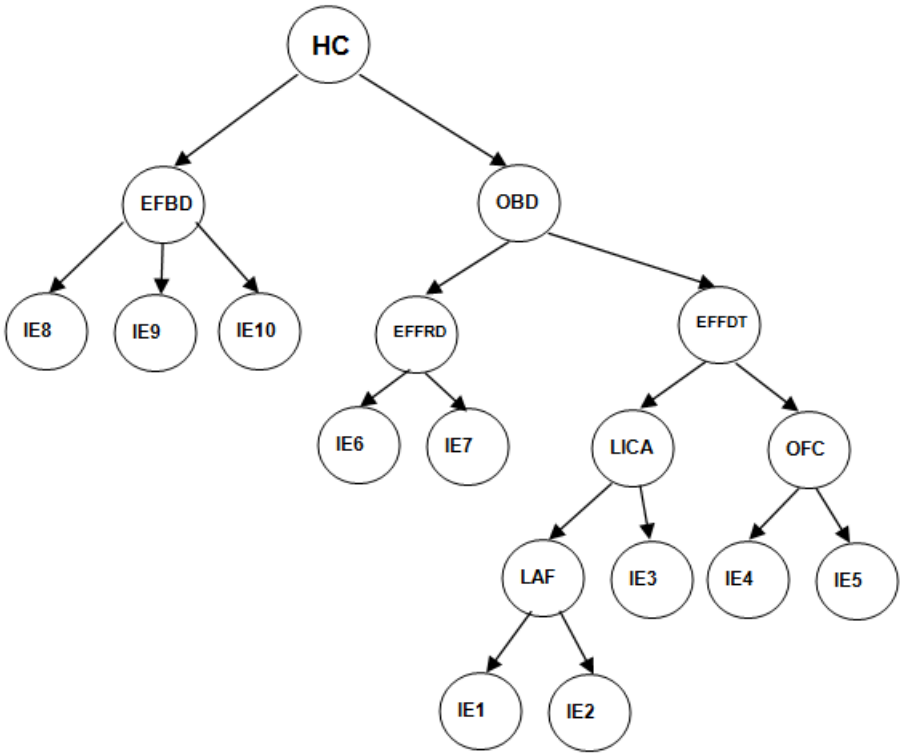
Subetapa 2.3 – Execução do algoritmo de aprendizagem Chow e Liu tree

Os 5 bancos de dados de treinamento: BDTAF1, BDTAF2, BDTAF3, BDTAF4 e BDTAF5, são utilizados como entradas de dados para a execução do algoritmo de aprendizagem.

O algoritmo de aprendizagem utilizado que é o algoritmo proposto por Chow e Liu (CHOW e LIU, 1968), basicamente aproxima a distribuição de probabilidade de um conjunto de dados discretos para uma distribuição na forma de árvore, onde todos os `arcos` partem (saem) do `nó` raiz da mesma que é o evento topo. A estrutura ou GAO obtida nesta subetapa é derivada a partir de cada banco de treinamento, sendo obtidos 5 GAOs. Os 5 GAOs são comparados um a um e os que se mostram semelhantes são considerados como sendo a árvore de falha (AF) resultante. O(s) que se mostra(am) discrepante(s) é(são) desconsiderado(s).

A estrutura ou GAO da AF obtida nesta subetapa é mostrada na Figura 52.

Figura 52 – GAO da árvore de falhas (AF)



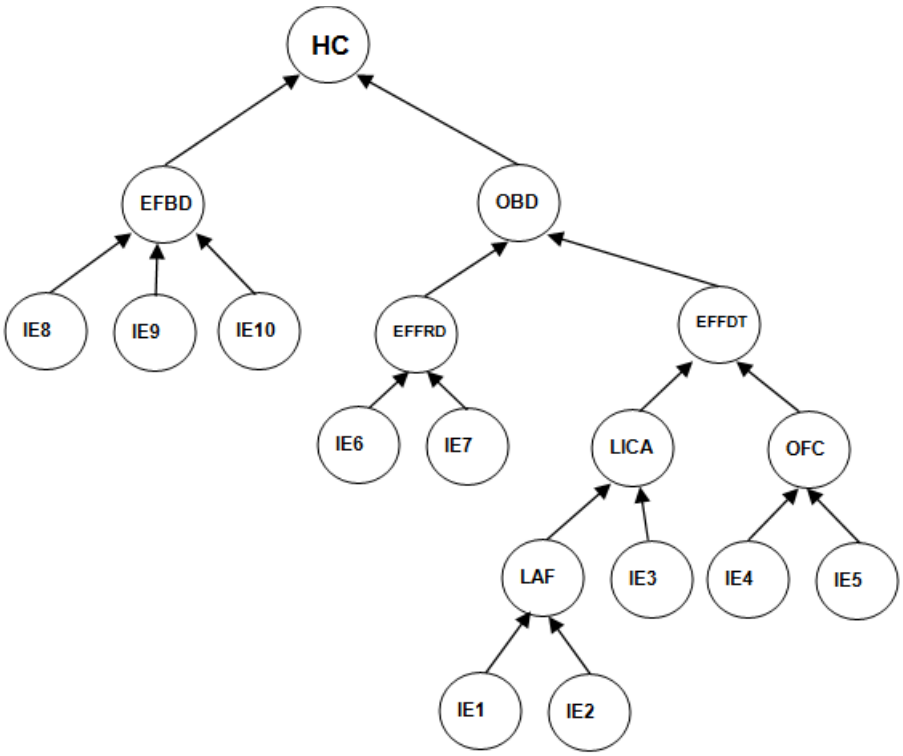
Fonte: próprio autor

- **Etapa 3 – Construção do modelo da árvore de falhas (AF)**

A estrutura da AF mostrada na Figura 52, é submetida à equipe de especialistas, que verificam se as relações de dependência são pertinentes ou não e modificam a estrutura adicionando e/ou removendo `arcos` e/ou IE_i/EC_i até convergir a um modelo da AF que seja pertinente com a realidade do processo/planta.

Observa-se que a estrutura da rede bayesiana mostrada na Figura 52, representa uma distribuição de probabilidade conjunta na forma de árvore com os `arcos` que partem (saem) do HC, que no caso é o `nó` raiz, para as “causas”. Esta estrutura é então revista como um diagrama da árvore de falhas (AF), de modo que os `arcos` têm sua orientação invertida, ou seja, os mesmos devem ser dirigidos das “causas” para o HC. A Figura 53 mostra a AF resultante.

Figura 53 – Árvore de falhas (AF) com os `arcos` invertidos das causas para o evento topo (HC)



Fonte: próprio autor

- **Etapa 4 – Aprendizagem da estrutura da árvore de eventos (AE)**

Subetapa 4.1 – Montagem do banco de dados de treinamento (BDT_{AE})

Da mesma forma que o $BDT_{AF,}$ considera-se que o banco de dados (BDT_{AE}) possui dados faltantes ou incompletos. Este banco de dados foi obtido a partir dos procedimentos mostrados nos Apêndice A e Apêndice B, uma vez que não foram encontrados registros históricos de falhas para este exemplo de aplicação.

Ainda com base no resultado do estudo de fiabilidade de modelos de acidentes derivados via imputação de dados e abordagem bayesiana, considerando bancos de dados faltantes (Apêndice C), assume-se neste exemplo de aplicação, que o BDT_{AE} possui 20% (vinte por cento) de dados faltantes.

O BDT_{AE} resultante possui 1024 linhas por 12 colunas. A Tabela 4 mostra parte do BDT_{AE} com dados incompletos ou faltantes para aprendizagem da AE. Nesta tabela o evento topo é o (HC) e as demais colunas correspondem aos eventos indesejados (UE_i) e consequências indesejadas (OE_i) observadas ou parcialmente observadas, após a ocorrência do HC, em qualquer combinação, como por exemplo:

OE6, OE5, OE4, OE3, OE2, OE1, UE5, UE4, UE3, UE2 e UE1 que são descritos na Figura 54.

Figura 54 – Descrição das consequências do HC.

Acrônimo	Descrição das “consequências”
OE1	Nuvem de vapor e explosão
OE2	Incêndio
OE3	Nuvem de vapor de HC
OE4	Nuvem de vapor de HC sobre unidade ISOM
OE5	Piscina de fogo
OE6	Piscina de HC
UE1	Aparecimento de nuvem de vapor
UE2	Movimentação da nuvem de vapor
UE3	Ignição
UE4	Nuvem de vapor e explosão (VCE)
UE5	Após incêndio e explosão

Fonte: adaptado de (FERDOUS, KHAN, *et al.*, 2013)

Cada linha ou instância da matriz mostrada na Tabela 4, contém um valor binário (ex: 0 / Falso ou 1 / Verdadeiro) para o HC e para cada UE/OE que foi observado. Para os UE_s e OE_s que não foram observados em algumas instâncias, os valores contidos no BDT_{AE} para estes eventos, não contém valores binários disponíveis e são representados na Tabela 4 como “NA” (do termo em inglês “*Not Available*”).

Subetapa 4.2 – Imputação de Dados

A imputação dos dados faltantes do BDT_{AE} por valores plausíveis é feita via algoritmo de imputação multivariada baseada em equações encadeadas (MICE). O BDT_{AE} com dados incompletos/faltantes é convertido para um arquivo com formato texto (*.txt*) para ser importado para o software de computação estatística R. O comando para a execução da imputação de dados tem o seguinte formato:

imp2 ← mice(BDTAE, defaultMethod=c(“pmm”))

O resumo das informações pertinentes à parametrização do processo de imputação é mostrado na Figura 55.

Tabela 4 – Parte do banco de dados de treinamento com vinte por cento (20%) de dados faltantes para aprendizagem da árvore de eventos (AE)

HC	OE6	OE5	OE4	OE3	OE2	OE1	UE5	UE4	UE3	UE2	UE1
0	1	1	1	NA	0	NA	1	0	0	0	0
0	1	1	1	0	0	1	1	0	0	0	0
0	0	1	0	1	NA	0	0	0	0	NA	0
NA	1	0	1	0	0	NA	NA	0	0	0	0
0	1	0	0	NA	1	0	NA	0	NA	0	0
0	0	1	0	0	1	1	NA	NA	NA	0	0
0	NA	0	NA	1	0	1	0	0	0	NA	0
0	0	0	0	0	0	NA	NA	0	NA	0	0
0	0	NA	0	NA	NA	NA	0	0	0	0	0
0	0	NA	NA	1	0	NA	0	0	0	0	0
0	0	NA	1	0	1	0	0	0	0	0	NA
0	NA	0	1	1	1	1	NA	1	1	1	0
0	1	NA	1	1	0	1	1	NA	NA	0	0
0	1	1	1	0	0	1	1	0	0	NA	0
0	1	NA	0	0	1	1	0	1	0	0	NA
0	NA	NA	1	NA	1	0	0	0	NA	0	0
0	NA	0	1	0	NA	0	0	NA	0	0	NA
0	0	0	NA	1	1	1	0	1	1	1	0
0	0	0	1	0	1	NA	0	0	NA	0	0
0	1	NA	0	1	NA	0	0	0	0	0	0
0	1	1	1	0	1	1	1	NA	0	0	NA
0	0	1	0	NA	NA	1	0	1	1	NA	0
0	0	1	0	1	NA	0	NA	0	NA	0	0
0	1	0	NA	NA	0	1	0	NA	0	0	0
0	0	0	1	1	NA	0	NA	0	0	0	0
0	0	1	0	1	NA	0	0	NA	NA	0	0
0	0	1	0	0	1	1	NA	1	NA	NA	0
0	1	NA	0	0	NA	0	0	0	0	0	0
0	0	0	1	0	0	0	0	NA	0	0	0
0	1	1	0	0	NA	1	1	0	0	0	NA
NA	0	1	1	1	NA	0	0	0	0	NA	0
1	1	1	NA	1	1	1	1	1	NA	1	1
0	1	0	0	NA	1	0	0	NA	0	0	0
0	1	NA	1	1	0	1	0	0	0	0	0
NA	NA	0	NA	0	NA	NA	0	NA	0	0	0
NA	0	NA	0	0	NA	1	NA	1	NA	0	NA
NA	1	0	1	0	1	NA	NA	1	0	0	0
0	1	1	0	0	1	0	NA	NA	0	0	NA
NA	0	NA	1	1	1	1	NA	1	1	1	0
0	0	1	NA	1	NA	0	0	NA	0	0	0
0	1	NA	NA	1	0	1	0	0	0	0	0
0	0	1	1	1	1	NA	0	1	1	NA	0
0	0	0	1	NA	0	0	NA	0	0	0	0
NA	1	0	0	1	1	NA	0	0	0	0	0
0	0	1	NA	1	1	0	0	0	0	0	0
0	1	0	0	0	1	NA	NA	1	0	0	0
0	1	1	0	1	1	0	1	0	0	0	0
0	0	1	0	0	0	0	0	0	0	0	NA
0	0	1	0	1	1	0	NA	0	0	0	0
0	1	NA	1	0	NA	0	0	0	0	0	0

Fonte: próprio autor

Figura 55 – Resumo de informações do processo de imputação via MICE

```
> print(imp2)
Multiply imputed data set
Call:
mice(data = BDTAE, Defaultmethod = c("pmm"))
Number of multiple imputations:  5
Missing cells per column:
 HC OE6 OE5 OE4 OE3 OE2 OE1 UE5 UE4 UE3 UE2 UE1
204 191 211 214 192 225 215 206 183 197 213 207
Imputation methods:
   HC   OE6   OE5   OE4   OE3   OE2   OE1   UE5   UE4   UE3   UE2   UE1
"pmm" "pmm" "pmm" "pmm" "pmm" "pmm" "pmm" "pmm" "pmm" "pmm" "pmm" "pmm"
VisitSequence:
 HC OE6 OE5 OE4 OE3 OE2 OE1 UE5 UE4 UE3 UE2 UE1
  1   2   3   4   5   6   7   8   9  10  11  12
PredictorMatrix:
    HC OE6 OE5 OE4 OE3 OE2 OE1 UE5 UE4 UE3 UE2 UE1
HC   0   1   1   1   1   1   1   1   1   1   1   1
OE6  1   0   1   1   1   1   1   1   1   1   1   1
OE5  1   1   0   1   1   1   1   1   1   1   1   1
OE4  1   1   1   0   1   1   1   1   1   1   1   1
OE3  1   1   1   1   0   1   1   1   1   1   1   1
OE2  1   1   1   1   1   0   1   1   1   1   1   1
OE1  1   1   1   1   1   1   0   1   1   1   1   1
UE5  1   1   1   1   1   1   1   0   1   1   1   1
UE4  1   1   1   1   1   1   1   1   0   1   1   1
UE3  1   1   1   1   1   1   1   1   1   0   1   1
UE2  1   1   1   1   1   1   1   1   1   1   0   1
UE1  1   1   1   1   1   1   1   1   1   1   1   0
```

Fonte: próprio autor

Neste processo de imputação, têm-se bancos de dados completos a partir das 5 amostras geradas. Desta forma, deve-se digitar os comandos abaixo:

BDTAE1 ← complete(imp2,1)

BDTAE2 ← complete(imp2,2)

BDTAE3 ← complete(imp2,3)

BDTAE4 ← complete(imp2,4)

BDTAE5 ← complete(imp2,5)

A Tabela 5 mostra como exemplo, uma parte do BDTAE3 com os dados imputados.

Tabela 5 – Parte do banco de dados de treinamento (BDTAE3) com dados imputados via MICE

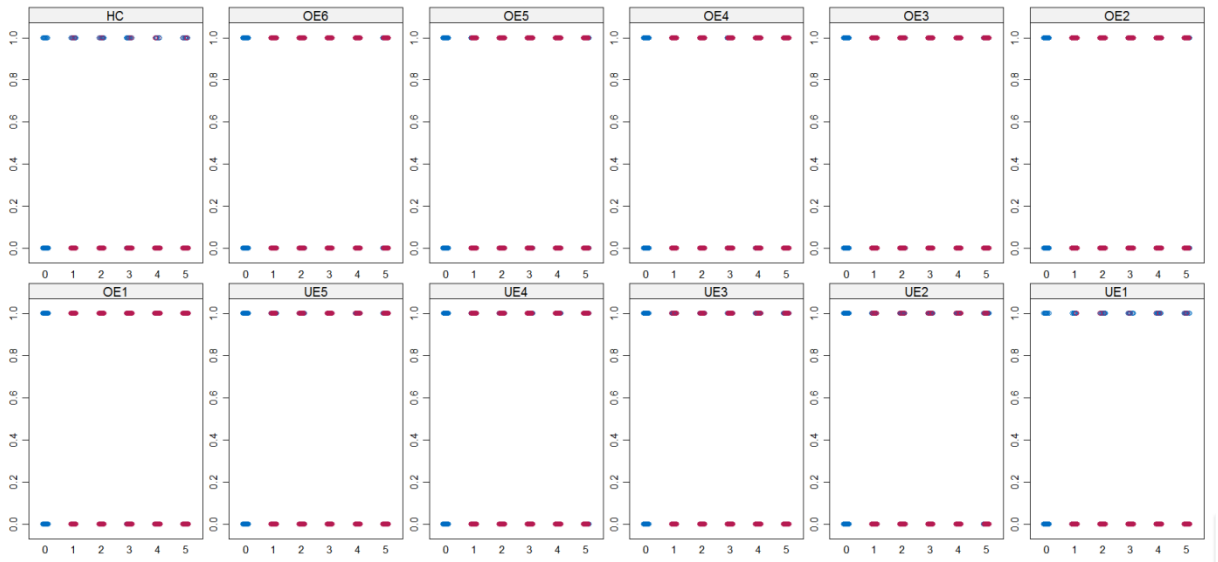
HC	OE6	OE5	OE4	OE3	OE2	OE1	UE5	UE4	UE3	UE2	UE1
0	1	1	1	0	0	1	1	0	0	0	0
0	1	1	1	0	0	1	1	0	0	0	0
0	0	1	0	1	1	0	0	0	0	0	0
0	1	0	1	0	0	0	0	0	0	0	0
0	1	0	0	0	1	0	0	0	0	0	0
0	0	1	0	0	1	1	0	1	0	0	0
0	0	0	1	1	0	1	0	0	0	0	0
0	0	0	0	0	0	1	0	0	0	0	0
0	0	1	0	0	0	0	0	0	0	0	0
0	0	1	1	1	0	0	0	0	0	0	0
0	0	1	1	0	1	0	0	0	0	0	0
0	1	0	1	1	1	1	0	1	1	1	0
0	1	1	1	1	0	1	1	0	0	0	0
0	1	1	1	0	0	1	1	0	0	0	0
0	1	0	0	0	1	1	0	1	0	0	0
0	0	0	1	0	1	0	0	0	0	0	0
0	1	0	1	0	1	0	0	0	0	0	0
0	0	0	1	1	1	1	0	1	1	1	0
0	0	0	1	0	1	0	0	0	0	0	0
0	1	0	0	1	0	0	0	0	0	0	0
0	1	1	1	0	1	1	1	1	0	0	0
0	0	1	0	1	1	1	0	1	1	0	0
0	0	1	0	1	0	0	0	0	0	0	0
0	1	0	1	0	0	1	0	0	0	0	0
0	0	0	1	1	0	0	0	0	0	0	0
0	0	1	0	1	1	0	0	0	0	0	0
0	0	1	0	0	1	1	0	1	0	0	0
0	1	0	0	0	1	0	0	0	0	0	0
0	0	0	1	0	0	0	0	0	0	0	0
0	1	1	0	0	0	1	1	0	0	0	0
0	0	1	1	1	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1	1	1	1	1
0	1	0	0	1	1	0	0	0	0	0	0
0	1	0	1	1	0	1	0	0	0	0	0
0	0	0	0	0	0	1	0	0	0	0	0
0	0	1	0	0	1	1	0	1	0	0	0
0	1	0	1	0	1	1	0	1	0	0	0
0	1	1	0	0	1	0	1	0	0	0	0
0	0	0	1	1	1	1	0	1	1	1	0
0	0	1	0	1	1	0	0	0	0	0	0
0	1	0	1	1	0	1	0	0	0	0	0
0	0	1	1	1	1	1	0	1	1	1	0
0	0	0	1	1	0	0	0	0	0	0	0
0	1	0	0	1	1	0	0	0	0	0	0
0	0	1	1	1	1	0	0	0	0	0	0
0	1	0	0	0	1	1	0	1	0	0	0
0	1	1	0	1	1	0	1	0	0	0	0
0	0	1	0	0	0	0	0	0	0	0	0
0	0	1	0	1	1	0	0	0	0	0	0
0	1	0	1	0	1	0	0	0	0	0	0

Fonte: próprio autor

Para inspecionar se existem discrepâncias entre as distribuições dos dados observados com os dados imputados, gera-se os gráficos com a distribuição de cada variável do banco de dados BDT_{AE} imputado, conforme mostra a Figura 56. Nestes

gráficos os pontos azuis representam os dados observados e os vermelhos representam os dados que foram imputados.

Figura 56 – Distribuições entre dados observados e imputados via MICE



Fonte: próprio autor

Como se pode observar na Figura 56, as distribuições entre os dados originais (pontos azuis) e os dados imputados (pontos vermelhos) são semelhantes, não existindo discrepância entre elas. Este fato está diretamente relacionado com o método de imputação selecionado. Neste sentido, o método “PMM” empregado para imputação é pertinente à aplicação envolvida.

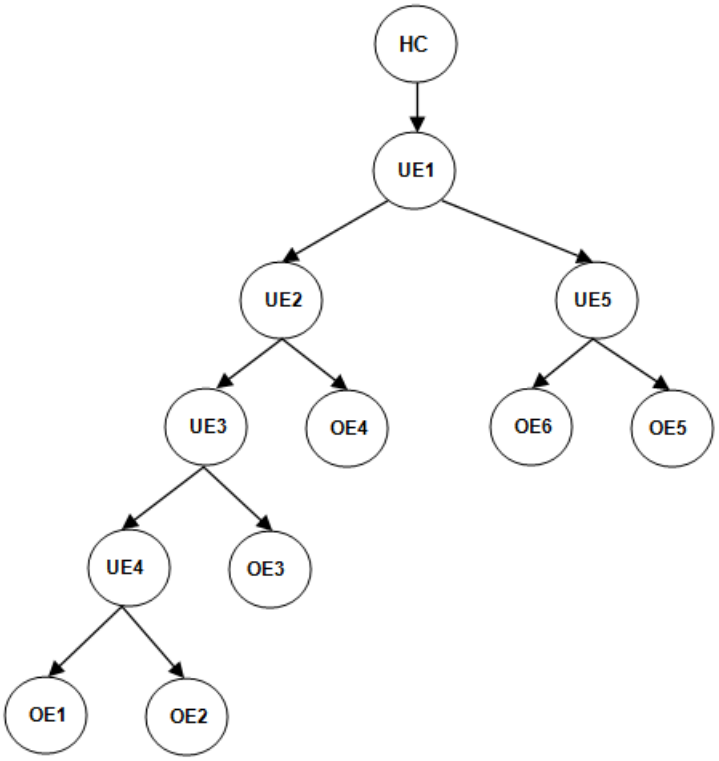
Subetapa 4.3 – Execução do algoritmo de aprendizagem Chow e Liu tree

Os 5 bancos de dados de treinamento: BDTAE1, BDTAE2, BDTAE3, BDTAE4 e BDTAE5, contendo os dados imputados, são utilizados como entradas de dados para a execução do algoritmo de aprendizagem nesta subetapa.

O algoritmo de aprendizagem utilizado neste trabalho é o proposto por Chow e Liu(CHOW e LIU, 1968). A estrutura ou GAO obtido é derivada a partir de cada banco de dado de treinamento, sendo obtidos 5 GAOs. Os 5 GAOs são comparados um a um e os que se mostram semelhantes são considerados como sendo a árvore de eventos (AE) resultante. O(s) que se mostra(am) discrepante(s) é(são) desconsiderado(s).

A estrutura ou GAO da AF obtida nesta subetapa é mostrada na Figura 57.

Figura 57 – GAO da árvore de eventos (AE)



Fonte: próprio autor

- **Etapa 5 – Construção do modelo da árvore de eventos (AE)**

A estrutura da AE mostrada na Figura 57 é submetida à equipe de especialistas que verificam se as relações de dependência são pertinentes ou não, e modificam a estrutura, adicionando e/ou removendo `arcos` e/ou UE_i e OE_i até convergir a um modelo da AE que seja pertinente com a realidade do processo/planta.

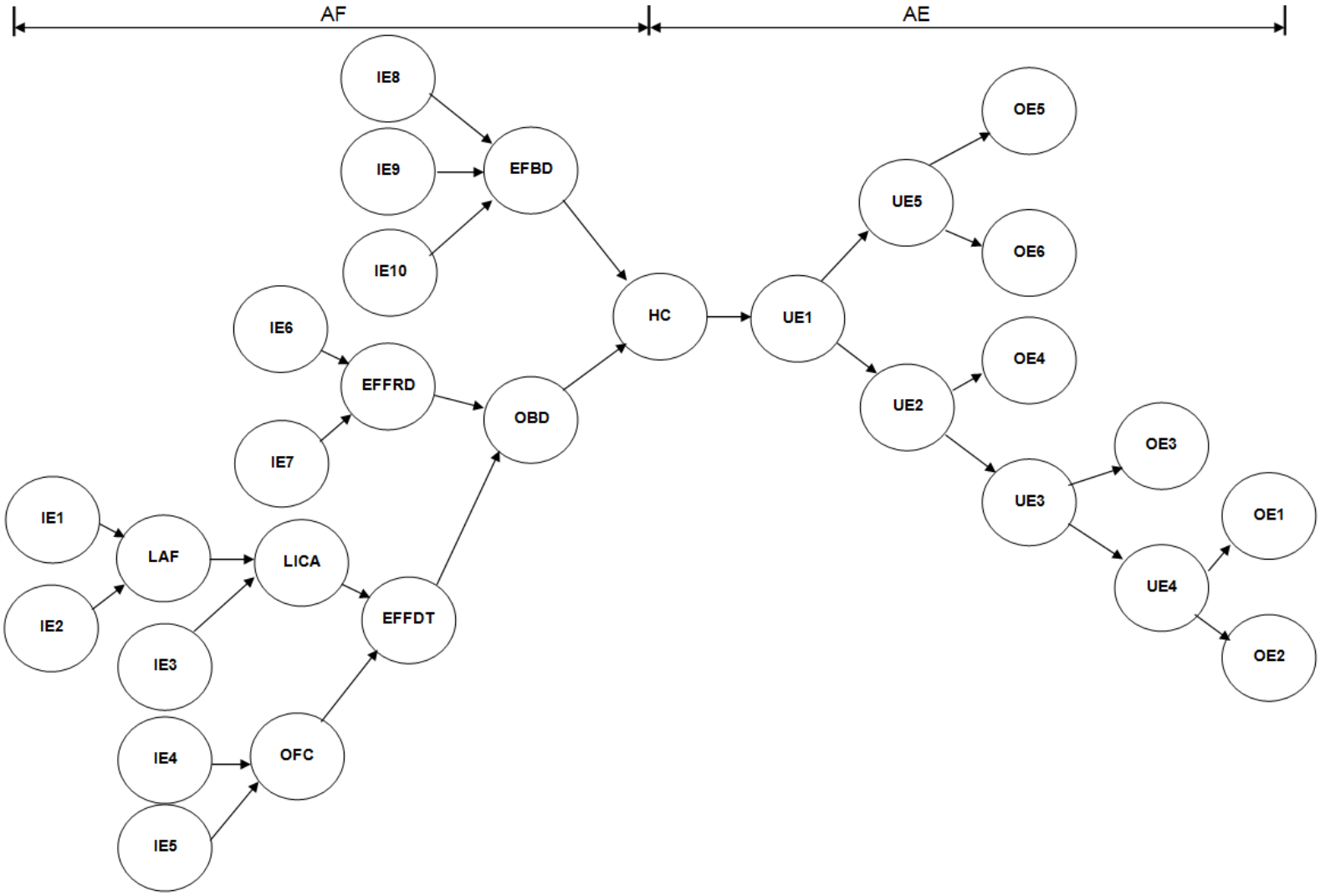
Observa-se também, que a estrutura da rede bayesiana mostrada na Figura 57, representa uma distribuição de probabilidade conjunta na forma de árvore com os `arcos` que partem (saem) do HC, que no caso é o `nó` raiz, para as consequências indesejadas. Esta estrutura é então interpretada, da forma como está, como o diagrama da árvore de eventos (AE). Neste exemplo o modelo na Figura 57 é a árvore de eventos resultante.

- **Etapa 6 – Integração dos modelos AF e AE**

Nesta etapa, procede a integração dos modelos de AF e AE. A integração destes modelos é obtida, tendo como elemento comum o evento topo (HC). A Figura 58 mostra o resultado da integração dos modelos de AF e AE e representa um cenário completo de acidente, dado o ET (HC), baseado no diagrama de *bowtie*. O

lado esquerdo do HC representa a árvore de falhas (AF) e o lado direito do HC representa a árvore de eventos (AE).

Figura 58 – Modelo de acidente resultante da integração dos modelos de AF e de AE.



4.1.1.3 Fase 3 – Integração dos modelos de acidentes com HAZOP

As atividades pertinentes a esta fase são descritas abaixo e baseadas no processo ilustrado na Figura 37.

- **Obtenção do modelo de acidente para cada evento topo (ET)**

Neste exemplo, considera-se apenas 1 evento topo, o HC e o modelo de acidente considerado é o apresentado na Figura 58 .

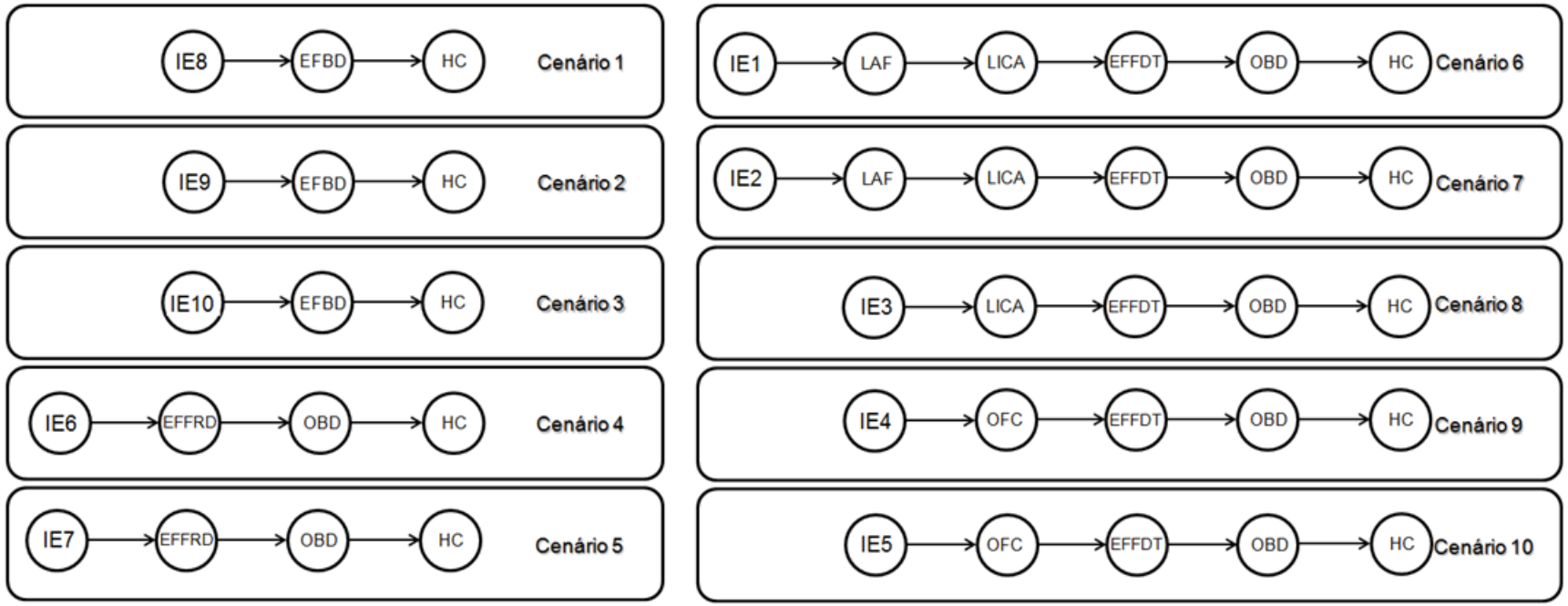
- **Identificação e separação da AF e AE de cada modelo**

A identificação da AF e da AE também é mostrada na Figura 58.

- **Identificação de todos os cenários críticos pertinentes à AF e AE**

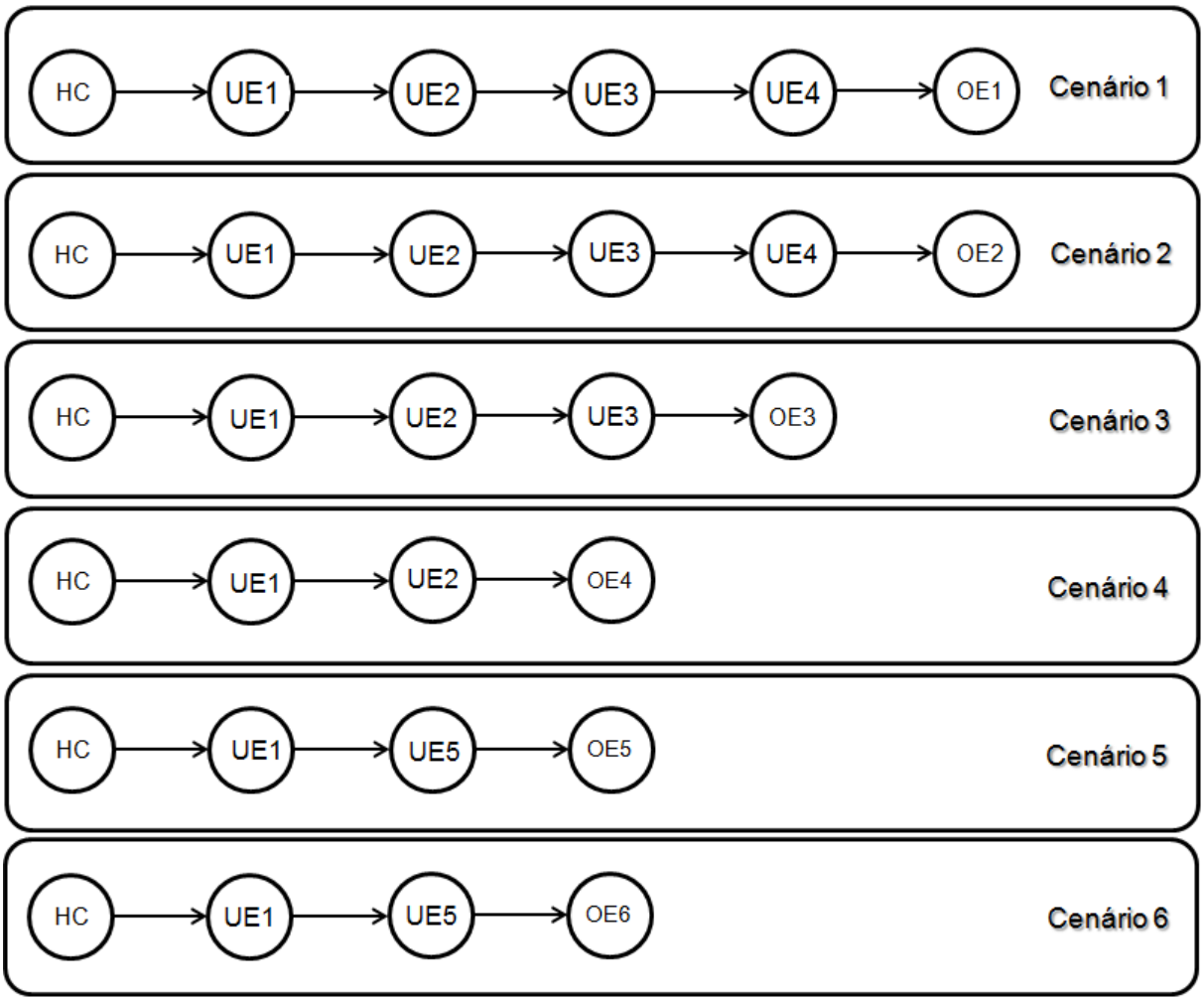
A Figura 59 mostra os cenários críticos pertinentes à árvore de falhas (AF). A Figura 60 mostra os cenários críticos pertinentes à árvore de eventos (AE).

Figura 59 – Cenários críticos pertinentes à AF



Fonte: próprio autor

Figura 60 – Cenários críticos pertinentes à AE



Fonte: próprio autor

- **Identificação das barreiras de prevenção e mitigação**

A Figura 61 mostra todas as barreiras de prevenção para cada cenário crítico da AF. Cada barreira é descrita por uma barra vermelha e representa uma função de segurança a ser executada pelo SCSP. O endereço associado a cada barreira aparece acima de cada barreira.

Nesta mesma figura, os conjuntos indicados por retângulos com bordas arredondadas e pontilhadas são formados pelas seguintes barreiras de prevenção:

(a) BP1.1.2, BP1.2.2 e BP1.3.2;

(b) BP1.4.2 e BP1.5.2;

(c) BP1.4.3, BP1.5.3, BP1.6.5, BP1.7.5, BP1.8.4, BP1.9.4 e BP1.10.4;

(d) BP1.6.4, BP1.7.4, BP1.8.3, BP1.9.3 e BP1.10.3;

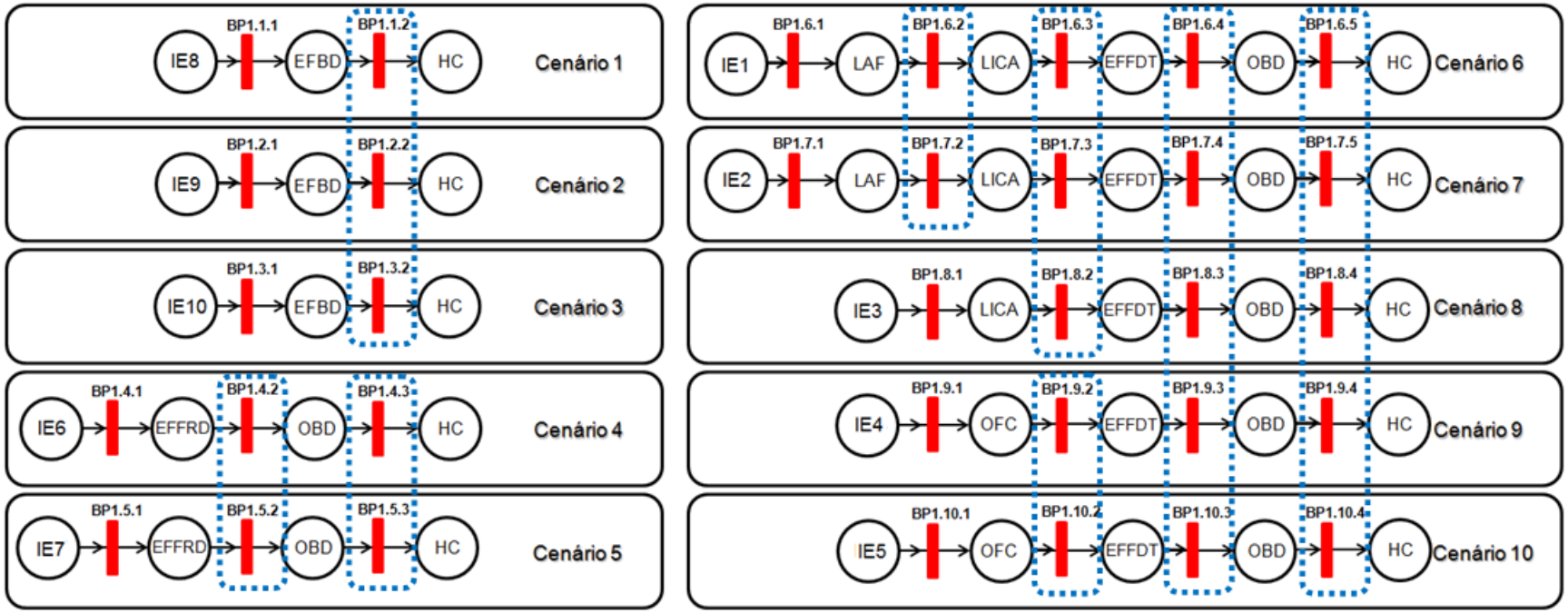
(e) BP1.6.3, BP1.7.3 e BP1.8.2;

(f) BP1.9.2 e BP1.10.2; e

(g) BP1.6.2 e BP1.7.2.

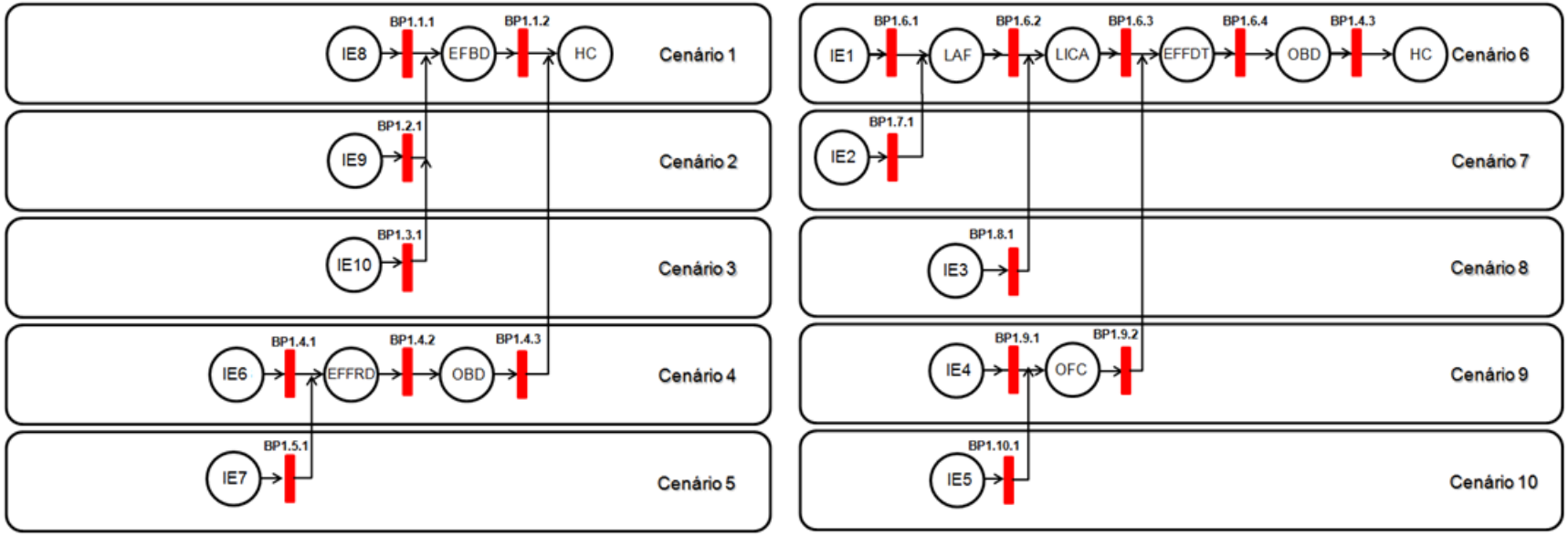
As barreiras pertencentes a um conjunto apresentam a mesma funcionalidade. Neste contexto, considera-se apenas uma barreira para cada conjunto. A Figura 62 mostra o diagrama resultante.

Figura 61 – Identificação das barreiras de prevenção



Fonte: próprio autor

Figura 62 – Identificação das barreiras de prevenção



Fonte: próprio autor

A Figura 63 mostra todas as barreiras de mitigação para cada cenário crítico da AE. Cada barreira é descrita por uma barra vermelha e representa uma função de segurança a ser executada pelo SCSP. O endereço associado a cada barreira aparece acima de cada barreira. Nesta mesma figura os conjuntos indicados por retângulos com bordas arredondadas e pontilhadas são formados pelas seguintes barreiras de mitigação:

(a) BM1.1.1, BM1.2.1, BM1.3.1, BM1.4.1, BM1.5.1 e BM1.6.1;

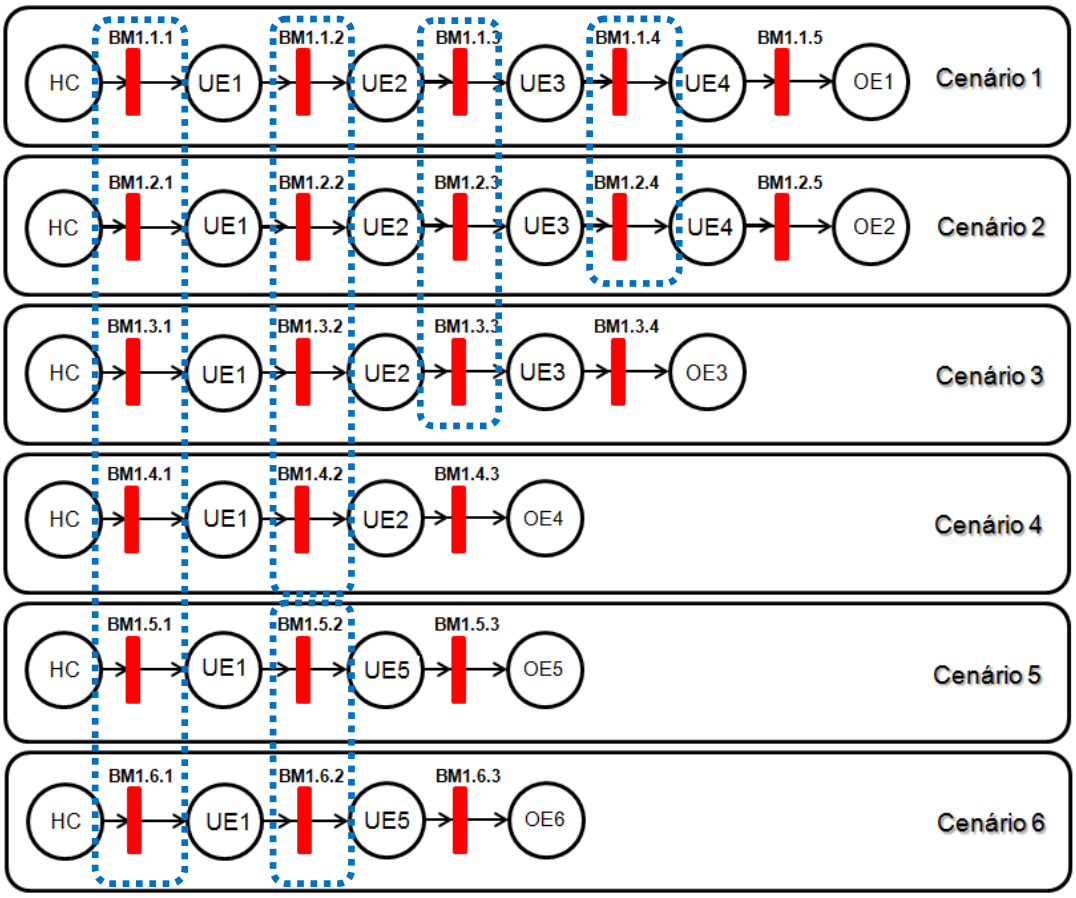
(b) BM1.1.2, BM1.2.2, BM1.3.2 e BM1.4.2;

(c) BM1.1.3, BM1.2.3 e BM1.3.3;

(d) BM1.1.4 e BM1.2.4; e

(e) BM1.5.2 e BM1.6.2,

Figura 63 – Identificação das barreiras de mitigação

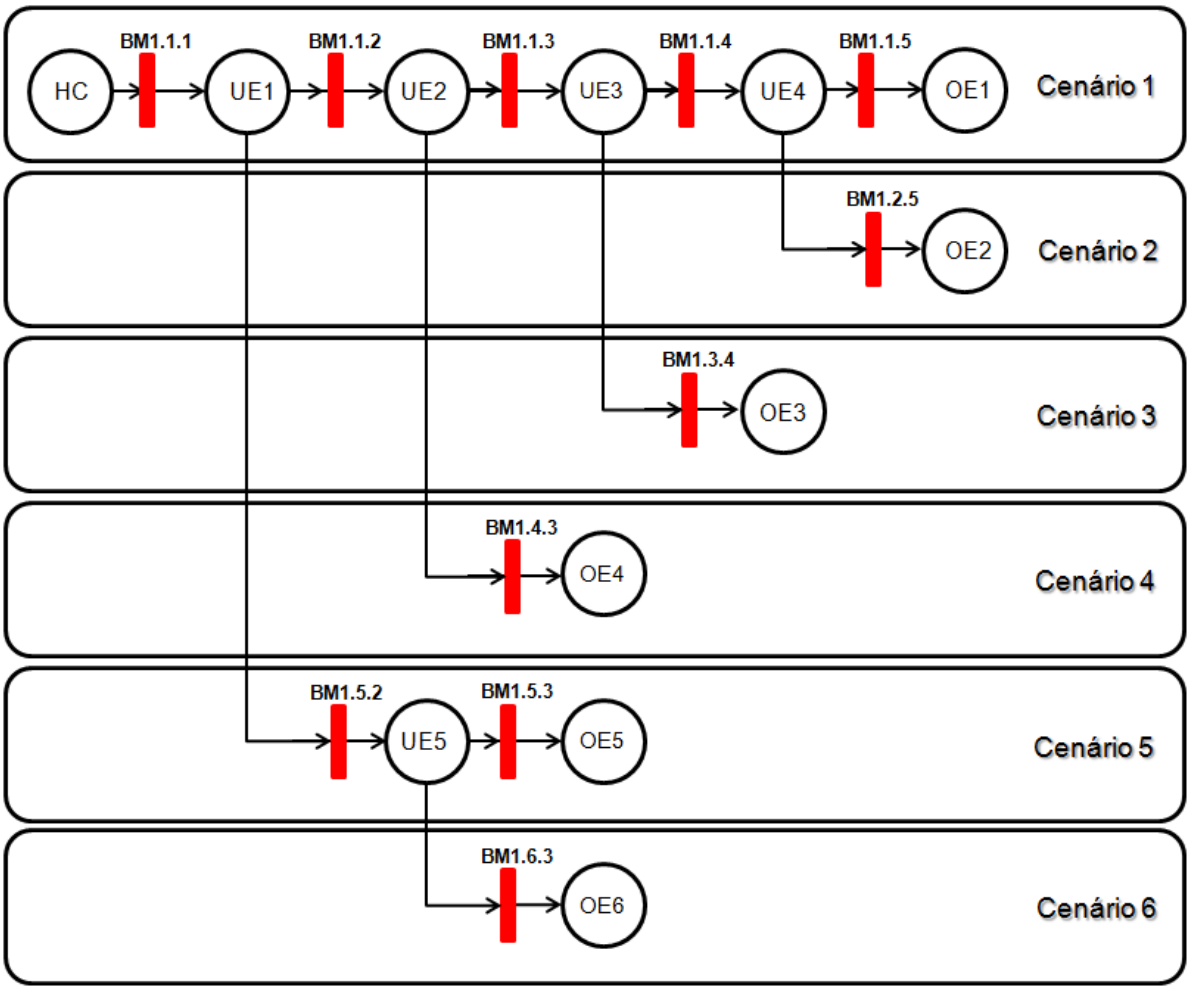


Fonte: próprio autor

As barreiras pertencentes a um conjunto apresentam a mesma funcionalidade, não sendo necessário repeti-las. Assim, considera-se apenas uma barreira para cada conjunto.

A Figura 64 mostra a identificação das barreiras de mitigação.

Figura 64 – Identificação das barreiras de mitigação

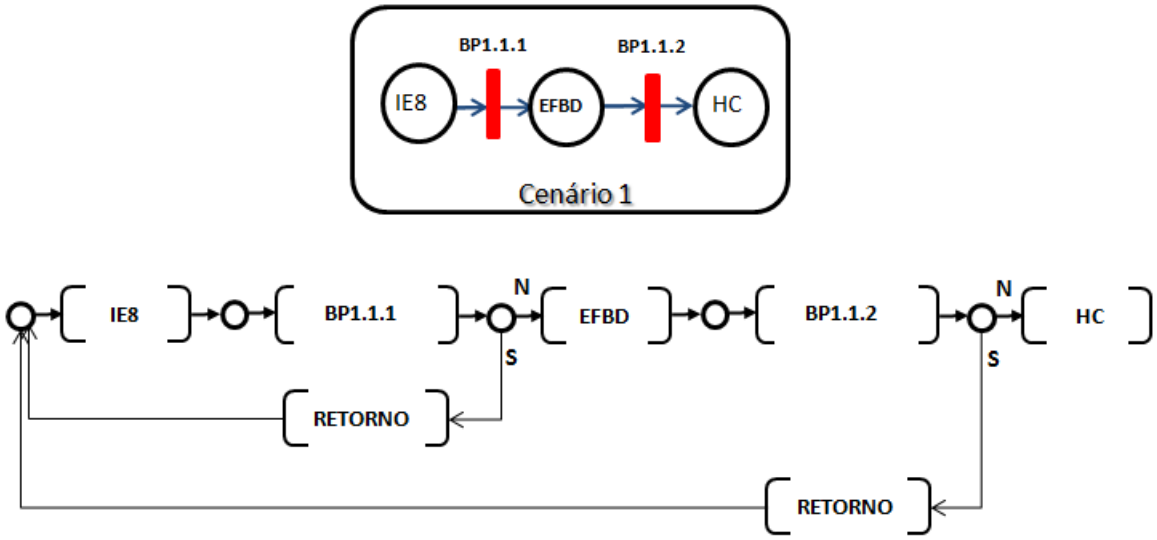


Fonte: próprio autor

- **Modelagem dos cenários críticos e barreiras em PFS**

Com base na Figura 62, a Figura 65 mostra o cenário crítico 1 e o seu modelo em PFS correspondente.

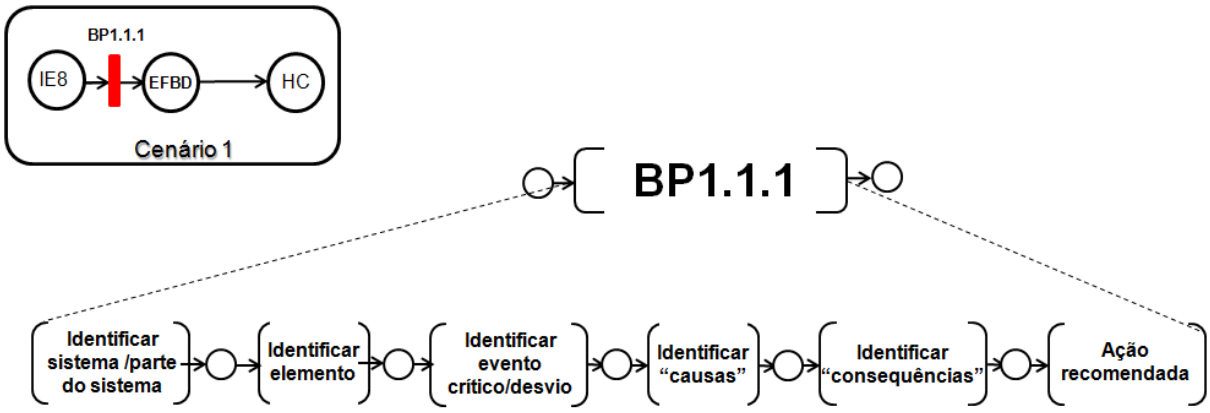
Figura 65 – Modelo de prevenção do cenário crítico 1 em PFS



Fonte: próprio autor

A partir do conceito de refinamentos sucessivos cada `atividade` associada a cada barreira de prevenção é refinada. As Figura 66 e Figura 67 mostram o refinamento das BP1.1.1 e BP1.1.2. Nas Tabela 6 e Tabela 7, estão as informações de cada barreira do mesmo cenário.

Figura 66 – Refinamento da BP1.1.1



Fonte: próprio autor

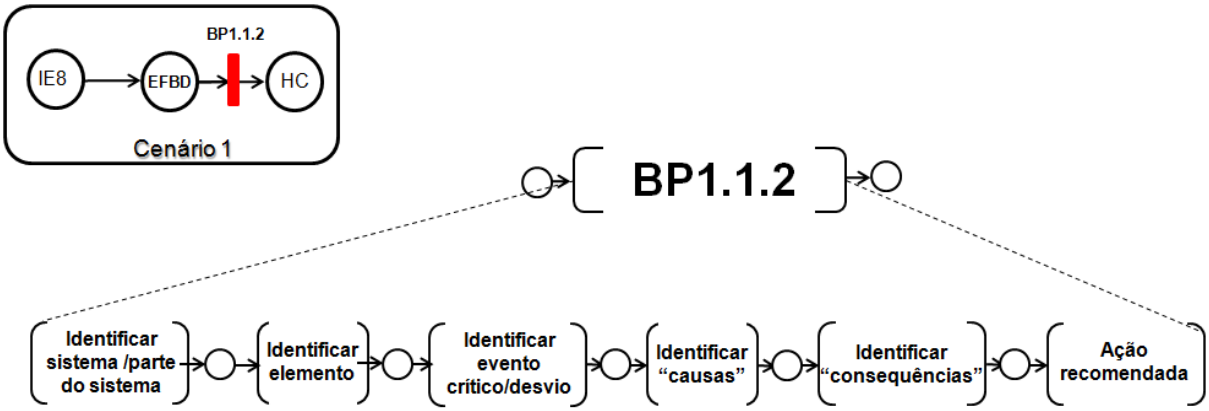
Tabela 6 – Informações da BP1.1.1

Barreira	BP1.1.1
Sistema/parte do sistema	Torre de isomerização (ISOM)
Elemento	Válvulas de alívio RV-1,2 e 3
Evento crítico/ desvio	Falha no fechamento das válvulas

Causa(s)	Desgaste mecânico ou falha no atuador das mesmas
Consequência(s)	Excesso de alimentação de refinado no tanque de *blowdown*
Ações recomendadas	a) Instalar sensores de posição (aberta / fechada) nas válvulas b) Diagnosticar e sinalizar falha de posição fechada das válvulas
Equipamento(s)	a) SIS b) IHM
Sensor(es)	a) Chaves fim de curso de válvula aberta (ZSH-1 / ZSH-2 e ZSH-3) b) Chaves fim de curso de válvula fechada (ZSL-1 / ZSL-2 e ZSL-3)
Atuador(es)	não se aplica

Fonte: próprio autor

Figura 67 – Refinamento da BP1.1.2



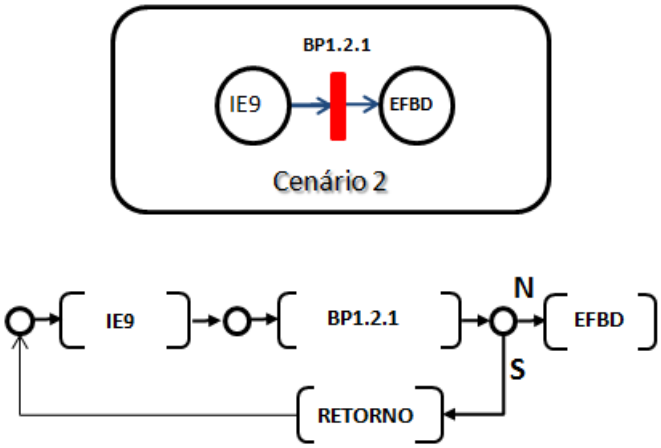
Fonte: próprio autor

Tabela 7 – Informações da BP1.1.2

Barreira	BP1.1.2
Sistema/parte do sistema	Tanque de *blowdown*
Elemento	Refinado
Evento crítico/ desvio	Excesso de alimentação de refinado
Causa(s)	Falha da barreira de prevenção BP1.1.1
Consequência(s)	Provável lançamento de vapores de hidrocarboneto na atmosfera
Ações recomendadas	a) Instalar três sensores de nível alto no tanque de *blowdown* b) Diagnosticar e sinalizar alarme de nível alto no tanque de *blowdown,* via algoritmo de votação "2oo3" c) Degenerar a unidade de isomerização de forma controlada
Equipamento(s)	a) SIS b) IHM
Sensor(es)	3 (três) sensores de nível
Atuador(es)	Comandos de "parada" de forma controlada dos elementos da unidade de isomerização

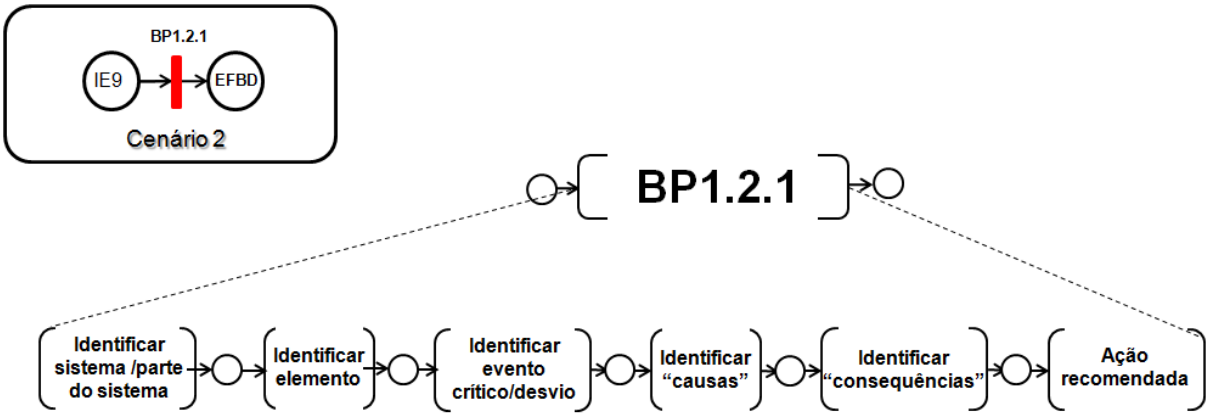
Ainda com base na Figura 62, a Figura 68 ilustra o modelo de prevenção do cenário crítico 2 em PFS. A Figura 69 mostra o refinamento da BP1.2.1 e a Tabela 8, as informações desta barreira.

Figura 68 – Modelo de prevenção do cenário crítico 2 em PFS



Fonte: próprio autor

Figura 69 – Refinamento da BP1.2.1



Fonte: próprio autor

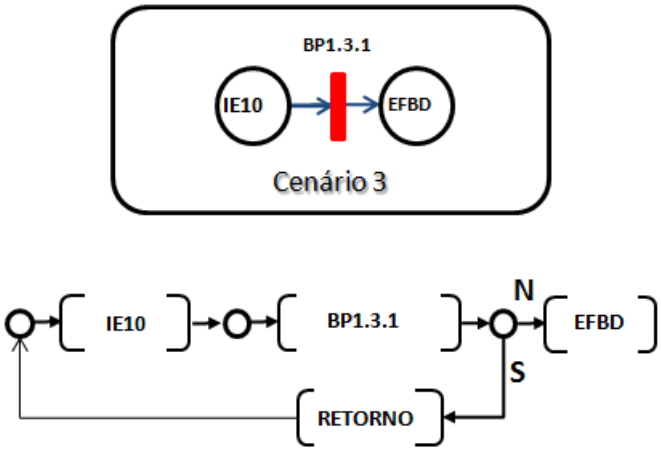
Tabela 8 – Informações da BP1.2.1

Barreira	BP1.2.1
Sistema/parte do sistema	Tanque de *blowdown*
Elemento	Válvula V-6
Evento crítico/ desvio	Falha na abertura da válvula V-6
Causa(s)	Desgaste mecânico ou falha no atuador da válvula V-6
Consequência(s)	Elevação do nível de refinado no tanque
Ações recomendadas	a) Instalar sensores de posição (aberta / fechada) na válvula V-6 b) Diagnosticar e sinalizar falha de posição aberta da válvula V-6

Equipamento(s)	a) SIS b) IHM
Sensor(es)	a) Chave fim de curso de válvula aberta (ZSH-6) b) Chave fim de curso de válvula fechada (ZSL-6)
Atuador(es)	não se aplica

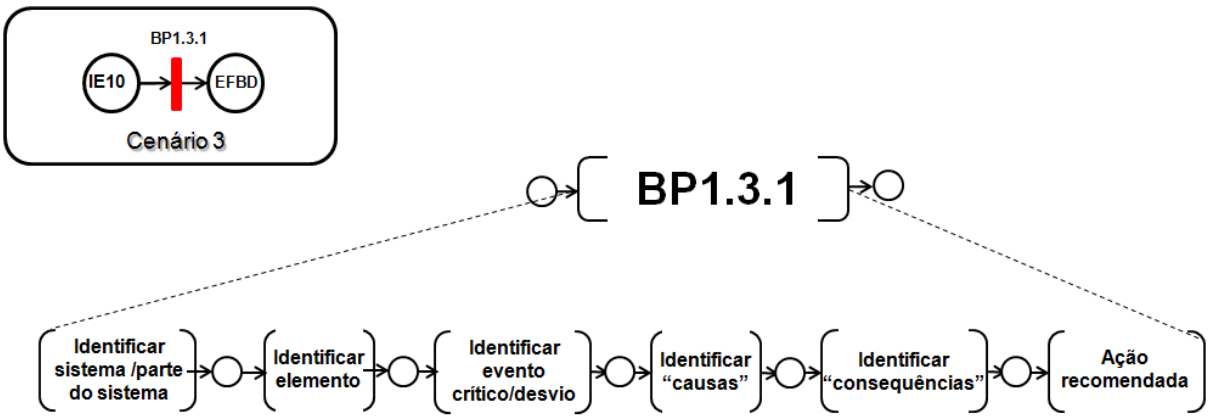
A Figura 70 mostra o modelo de prevenção do cenário crítico 3 em PFS. A Figura 71 mostra o refinamento da BP1.3.1 e a Tabela 9, as informações desta barreira.

Figura 70 – Modelo de prevenção do cenário crítico 3 em PFS



Fonte: próprio autor

Figura 71 – Refinamento da BP1.3.1



Fonte: próprio autor

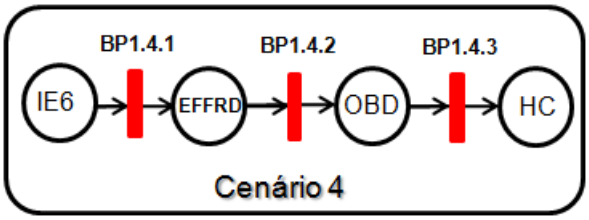
Tabela 9 – Informações da BP1.3.1

Barreira	BP1.3.1
Sistema/parte do sistema	Tanque de *blowdown*
Elemento	Sensor de nível de refinado no tanque de *blowdown*
Evento crítico/ desvio	Falha de alarme de nível alto de refinado no tanque de *blowdown*

Causa(s)	a) Falha do instrumento (sensor) b) Erro na calibração do instrumento c) Falha na alimentação do instrumento
Consequência(s)	Elevação do nível de refinado no tanque
Ações recomendadas	a) Instalar três sensores de nível alto de refinado no tanque b) Diagnosticar e sinalizar alarme de nível alto via algoritmo de votação “2oo3”
Equipamento(s)	a) SIS b) IHM
Sensor(es)	3 (três) sensores de nível
Atuador(es)	não se aplica

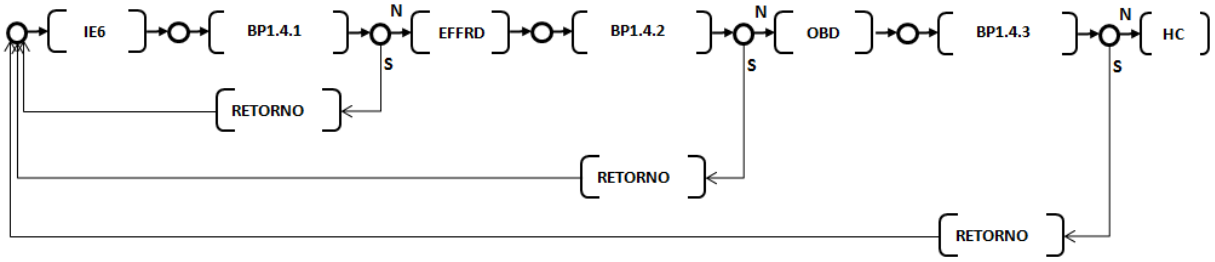
A Figura 72 ilustra o diagrama de barreiras do cenário crítico 4, e a Figura 73 ilustra o modelo de prevenção do mesmo cenário em PFS. As Figura 74, Figura 75 e Figura 76, mostram o refinamento de BP1.4.1, BP1.4.2 e BP1.4.3, respectivamente; e as Tabela 10, Tabela 11 e Tabela 12, as informações de cada barreira.

Figura 72 – Diagramas de barreiras do cenário crítico 4



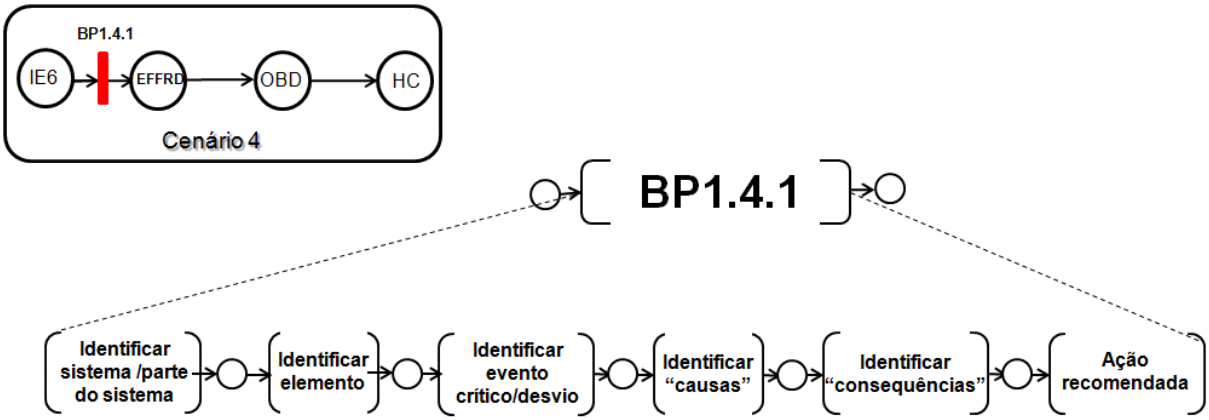
Fonte: próprio autor

Figura 73 – Modelo de prevenção do cenário crítico 4 em PFS



Fonte: próprio autor

Figura 74 – Refinamento da BP1.4.1

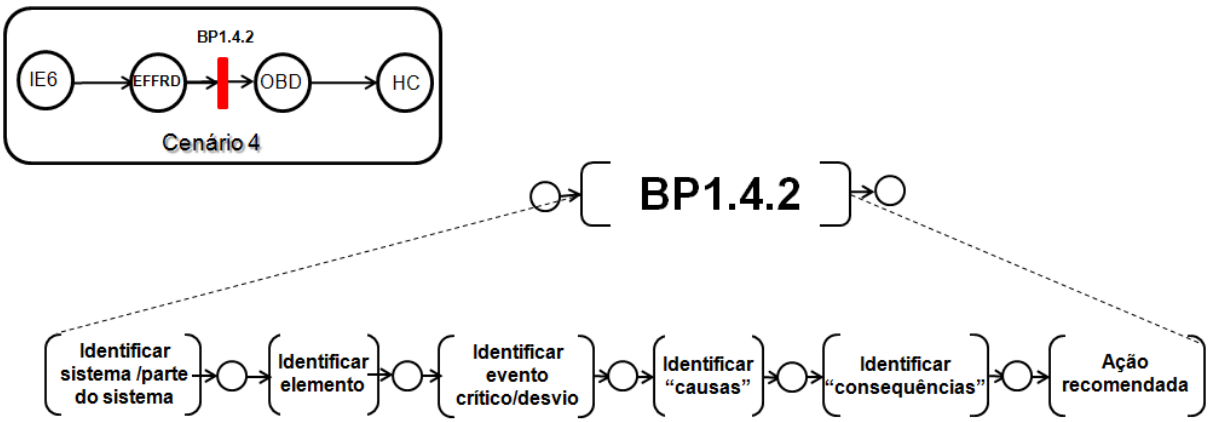


Fonte: próprio autor

Tabela 10 – Informações da BP1.4.1

Barreira	BP1.4.1
Sistema/parte do sistema	Tanque de refluxo
Elemento	Válvula de alívio RV-4
Evento crítico/ desvio	Falha no fechamento da válvula RV-4 e falta de sinalização para o(s) operador(es)
Causa(s)	Desgaste mecânico ou falha no atuador da válvula RV-4
Consequência(s)	Excesso de alimentação de refinado do tanque de refluxo
Ações recomendadas	a) Instalar sensores de posição (aberta / fechada) na válvula RV-4 b) Diagnosticar e sinalizar falha de posição fechada da válvula RV-4
Equipamento(s)	a) SIS b) IHM
Sensor(es)	a) Chave fim de curso de válvula aberta (ZSH-4) b) Chave fim de curso de válvula fechada (ZSL-4)
Atuador(es)	não se aplica

Figura 75 – Refinamento da BP1.4.2

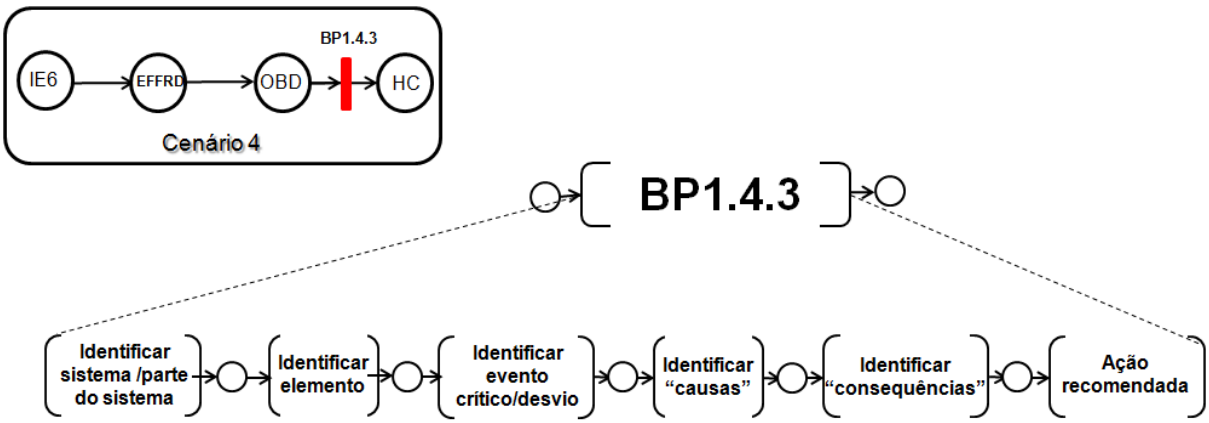


Fonte: próprio autor

Tabela 11 – Informações da BP1.4.2

Barreira	BP1.4.2
Sistema/parte do sistema	Tanque de *blowdown*
Elemento	Refinado
Evento crítico/ desvio	Excesso de alimentação de refinado no tanque de refluxo e falta de sinalização para o(s) operador(es).
Causa(s)	Falha da barreira de prevenção BP1.4.1
Consequência(s)	Nível de refinado acima do nível máximo permitido dentro do tanque de *blowdown*
Ações recomendadas	a) Instalar três sensores de nível alto de refinado no tanque b) Diagnosticar e sinalizar alarme de nível alto via algoritmo de votação “2oo3”
Equipamento(s)	a) SIS b) IHM
Sensor(es)	03 (três) sensores de nível denominados de LSH1, LSH2 e LSH3.
Atuador(es)	não se aplica

Figura 76 – Refinamento da BP1.4.3



Fonte: próprio autor

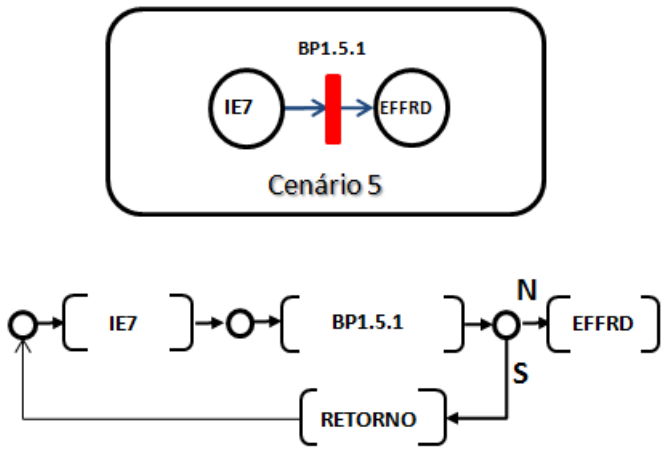
Tabela 12 – Informações da BP1.4.3

Barreira	BP1.4.3
Sistema/parte do sistema	Tanque de *blowdown*
Elemento	Refinado
Evento crítico/ desvio	Nível de refinado acima do nível máximo permitido dentro do tanque de blowdown
Causa(s)	Falha da barreira de prevenção BP1.4.2
Consequência(s)	Provável lançamento de vapores de hidrocarboneto na atmosfera
Ações recomendadas	a) Instalar três sensores de nivel alto do tanque de blowdown b) Diagnosticar e sinalizar alarme de nivel alto via algoritmo de votação “2003”.

	c) Degenerar de forma controlada a unidade de ISOM.
Equipamento(s)	a) SIS b) IHM
Sensor(es)	03 (três) sensores de nível denominados de LSHH1, LSHH2 e LSHH3.
Atuador(es)	Comandos de “parada” de forma controlada dos elementos da unidade de isomerização

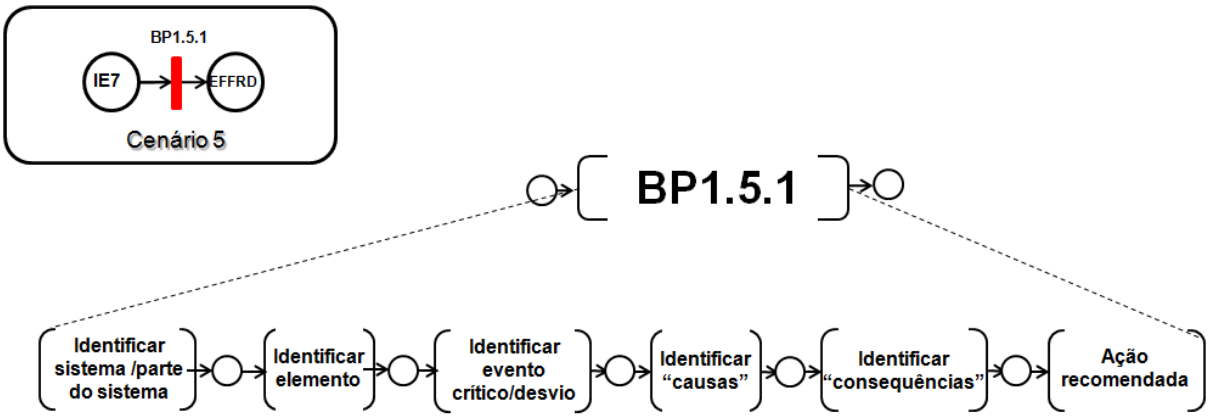
A Figura 77 mostra o modelo de prevenção do cenário crítico 5 em PFS. A Figura 78 mostra o refinamento da BP1.5.1 e a Tabela 13 as informações desta barreira.

Figura 77 – Modelo de prevenção do cenário crítico 5 em PFS



Fonte: próprio autor

Figura 78 – Refinamento da BP1.5.1



Fonte: próprio autor

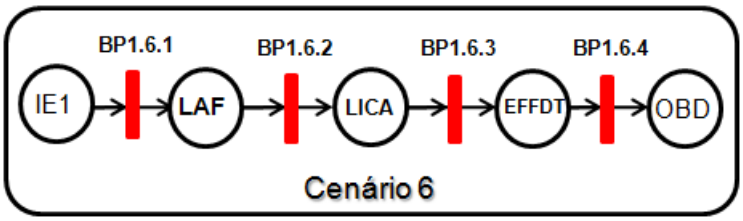
Tabela 13 – Informações da BP1.5.1

Barreira	BP1.5.1
Sistema/parte do sistema	Tanque de refluxo
Elemento	Bomba de refluxo
Evento crítico/ desvio	Falha da bomba de refluxo
Causa(s)	a) Falha no sistema de alimentação elétrica do motor-bomba

	b) Falha mecânica
Consequência(s)	Excesso de alimentação do tanque de refluxo
Ações recomendadas	a) Instalar sensores na bomba b) Diagnosticar e sinalizar falha da bomba de refluxo
Equipamento(s)	a) SIS b) IHM
Sensor(es)	Sensor de falha da bomba
Atuador(es)	não se aplica

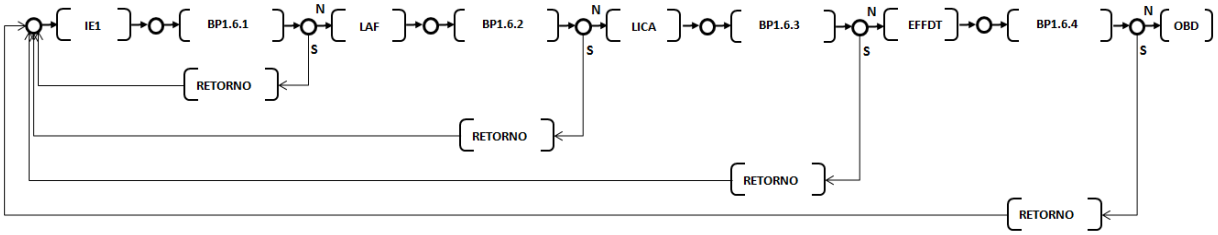
A Figura 79 ilustra o diagrama de barreiras do cenário crítico 6, e a Figura 80 ilustra o modelo de prevenção do mesmo cenário em PFS. As Figura 81, Figura 82, Figura 83 e Figura 84 mostram os refinamentos de BP1.6.1, BP1.6.2, BP1.6.3 e BP1.6.4, respectivamente, e as Tabela 14, Tabela 15, Tabela 16 e Tabela 17 as informações relacionadas a cada barreira.

Figura 79 – Diagrama de barreiras do cenário crítico 6



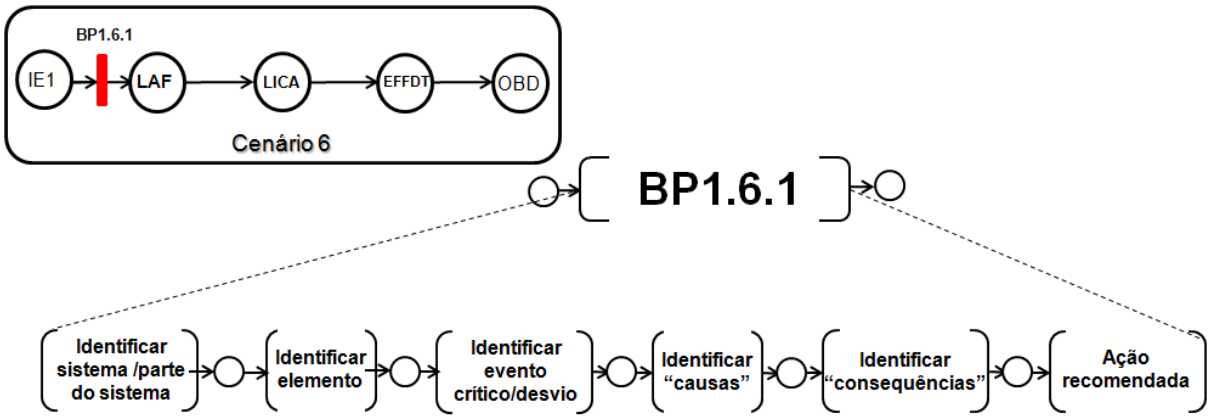
Fonte: próprio autor

Figura 80 – Modelo de prevenção do cenário crítico 6 em PFS



Fonte: próprio autor

Figura 81 – Refinamento da BP1.6.1

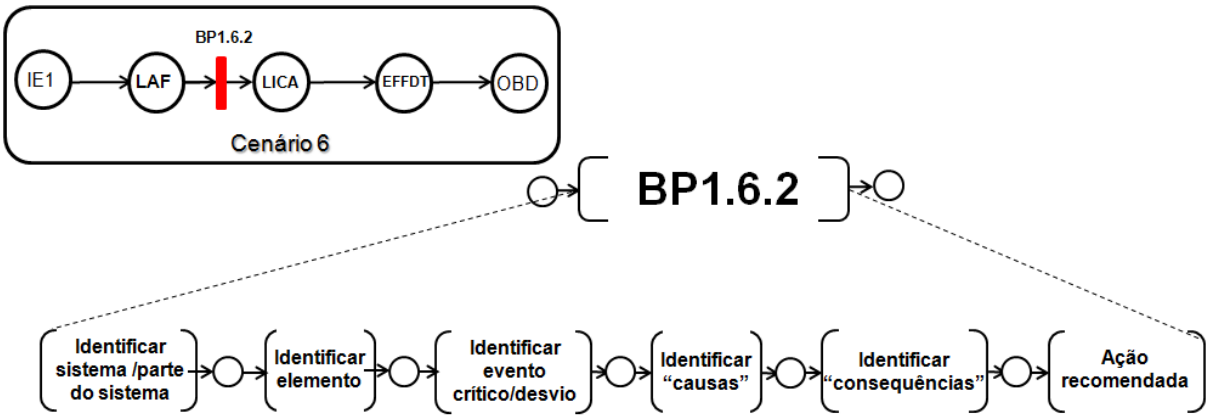


Fonte: próprio autor

Tabela 14 – Informações da BP1.6.1

Barreira	BP1.6.1
Sistema/parte do sistema	Torre de isomerização (ISOM)
Elemento	Sensor 1 de nível alto de refinado na torre de isomerização
Evento crítico/ desvio	Falha do sensor 1
Causa(s)	a) Falha do instrumento (sensor 1) b) Erro na calibração do instrumento 1 c) Falha na alimentação do instrumento 1
Consequência(s)	Falha de alarme de nível
Ações recomendadas	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
Equipamento(s)	a) SIS b) IHM
Sensor(es)	não se aplica
Atuador(es)	não se aplica

Figura 82 – Refinamento da BP1.6.2



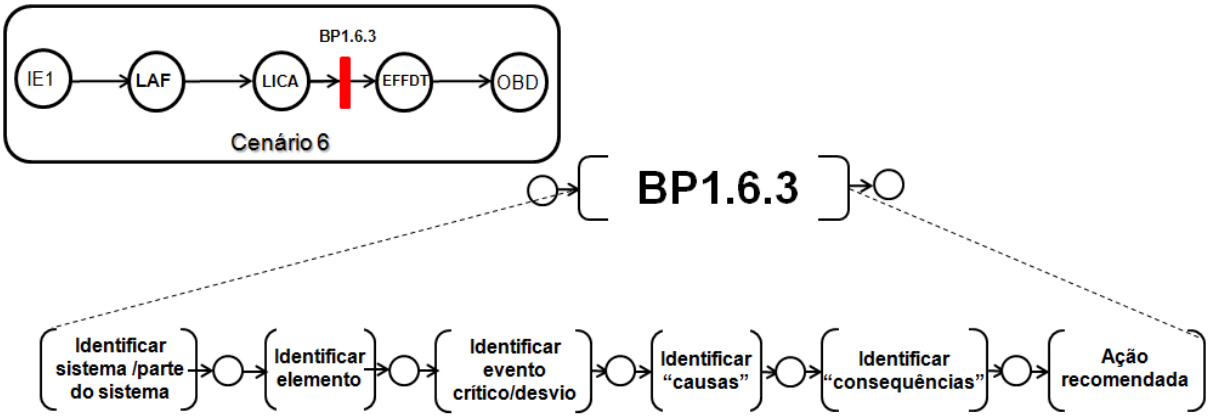
Fonte: próprio autor

Tabela 15 – Informações da BP1.6.2

Barreira	BP1.6.2
Sistema/parte do sistema	Torre de isomerização (ISOM)
Elemento	Sensor de nível alto de refinado na torre de isomerização
Evento crítico/ desvio	Falha de alarme de nível alto
Causa(s)	Falha da barreira de prevenção BP1.6.1
Consequência(s)	Falhas LICA
Ações	Fechar automaticamente a válvula de alimentação de refinado na torre ISOM

recomendadas	
Equipamento(s)	a) SIS b) IHM
Sensor(es)	não se aplica
Atuador(es)	Atuador da válvula de alimentação de refinado na torre ISOM

Figura 83 – Refinamento da BP1.6.3.

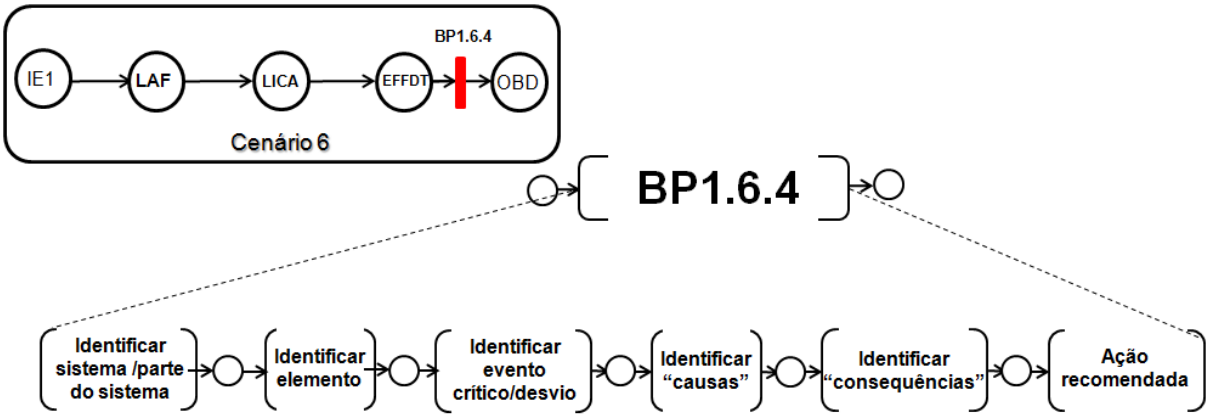


Fonte: próprio autor

Tabela 16 – Informações da BP1.6.3

Barreira	BP1.6.3
Sistema/parte do sistema	Torre de isomerização (ISOM)
Elemento	Sensor de nível alto de refinado na torre de isomerização
Evento crítico/ desvio	Falhas LICA
Causa(s)	Falha da barreira de prevenção BP1.6.2
Consequência(s)	Excesso de alimentação na torre de ISOM
Ações recomendadas	Degenerar de forma controlada a torre de ISOM
Equipamento(s)	a) SIS b) IHM
Sensor(es)	não se aplica
Atuador(es)	Comandos de "parada" de forma controlada da torre de isomerização (ISOM)

Figura 84 – Refinamento da BP1.6.4



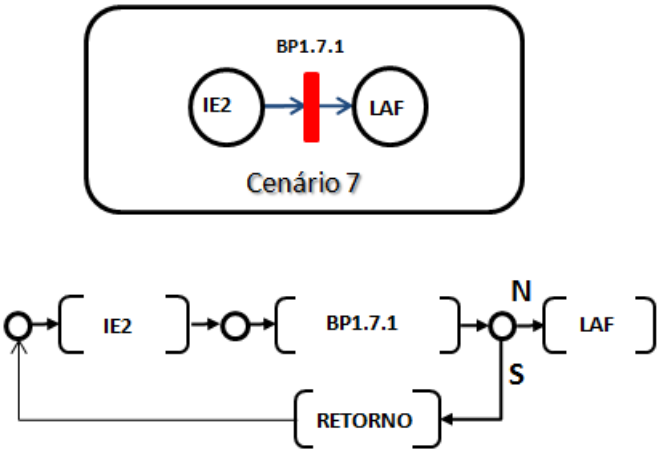
Fonte: próprio autor

Tabela 17 – Informações da BP1.6.4.

Barreira	BP1.6.4
Sistema/parte do sistema	Torre de isomerização (ISOM)
Elemento	Refinado
Evento crítico/ desvio	Excesso de alimentação da torre de ISOM
Causa(s)	Falha da barreira de prevenção BP1.6.3
Consequência(s)	Nível de refinado acima do nível máximo permitido dentro do tanque de *blowdown*
Ações recomendadas	Degenerar de forma controlada a unidade de isomerização
Equipamento(s)	a) SIS b) IHM
Sensor(es)	não se aplica
Atuador(es)	Comandos de "parada" de forma controlada dos elementos da unidade de isomerização

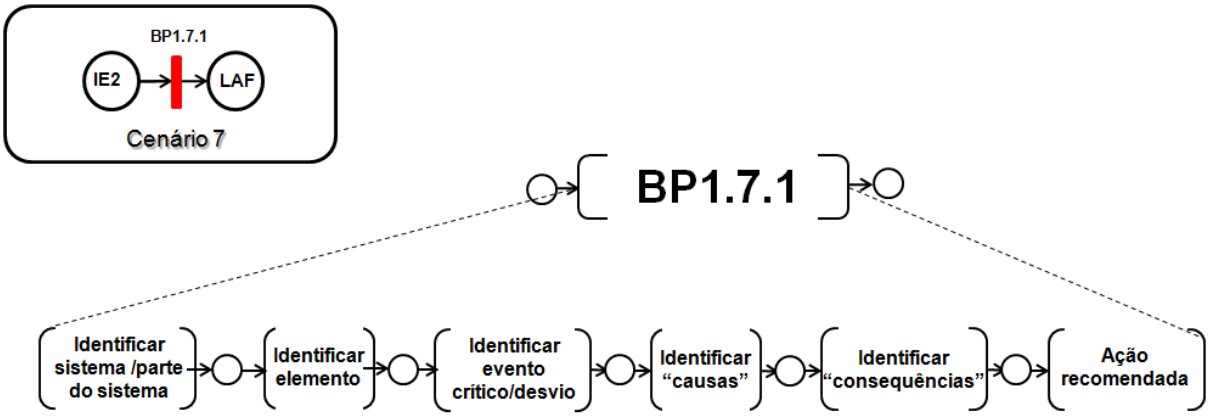
A Figura 85 mostra o modelo de prevenção do cenário crítico 7. A Figura 86 mostra o refinamento da BP1.7.1 e a Tabela 18 as informações desta barreira.

Figura 85 – Modelo de prevenção do cenário crítico 7 em PFS



Fonte: próprio autor

Figura 86 – Refinamento da BP1.7.1



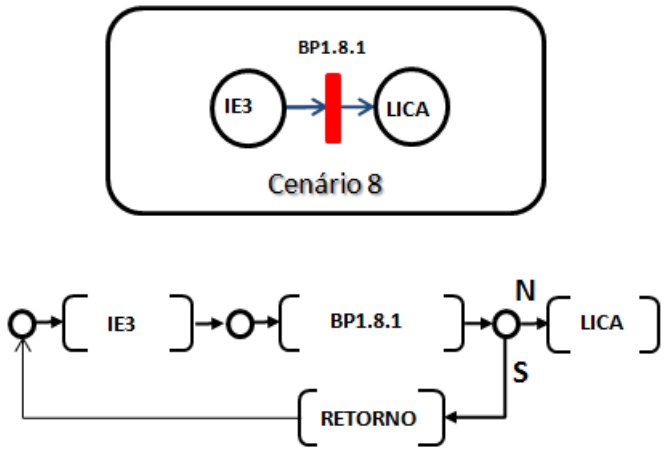
Fonte: próprio autor

Tabela 18 – Informações da BP1.7.1

Barreira	BP1.7.1
Sistema/parte do sistema	Torre de isomerização (ISOM)
Elemento	Sensor 2 de nível alto de refinado na torre de isomerização
Evento crítico/ desvio	Falha do sensor 2
Causa(s)	a) Falha do instrumento (sensor 2) b) Erro na calibração do instrumento 2 c) Falha na alimentação do instrumento 2
Consequência(s)	Falha de alarme de nível
Ações recomendadas	a) Diagnosticar e sinalizar falha do sensor 2 b) Diagnosticar e sinalizar erro de calibração do sensor 2 c) Diagnosticar e sinalizar falha na alimentação do sensor 2
Equipamento(s)	a) SIS b) IHM
Sensor(es)	não se aplica
Atuador(es)	não se aplica

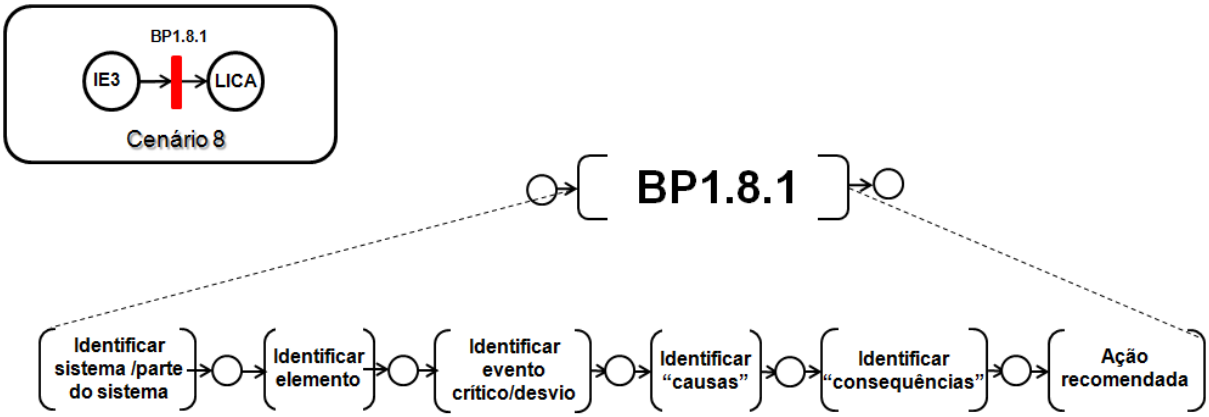
A Figura 87 mostra o modelo de prevenção do cenário crítico 8 em PFS. A Figura 88 mostra o refinamento da BP1.8.1 e a Tabela 19 as informações desta barreira.

Figura 87 – Modelo de prevenção do cenário crítico 8 em PFS



Fonte: próprio autor

Figura 88 – Refinamento da BP1.8.1



Fonte: próprio autor

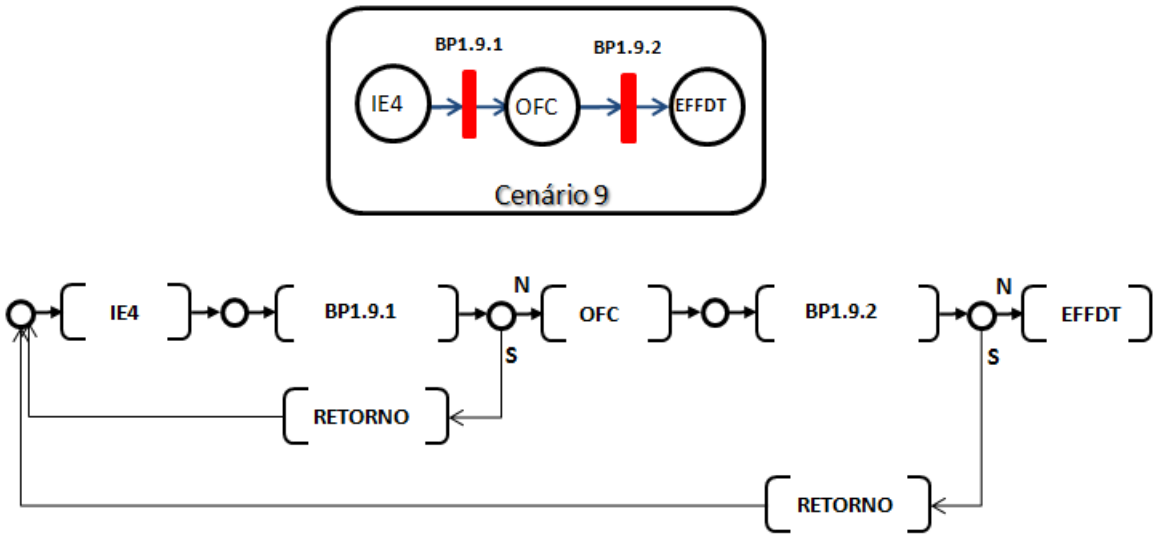
Tabela 19 – Informações da BP1.8.1

Barreira	BP1.8.1
Sistema/parte do sistema	Torre de isomerização (ISOM)
Elemento	Transmisor de nível (LT-1)
Evento crítico/ desvio	Falha na leitura do transmissor de nível (LT-1)
Causa(s)	a) Erro na calibração do transmisor b) Falha no sistema de alimentação elétrica do transmissor
Consequência(s)	Falhas LICA
Ações recomendadas	a) Diagnosticar e sinalizar erro na calibração do transmisor b) Diagnosticar e sinalizar falha no sistema de alimentação elétrica do transmisor c) Fechar automaticamente a válvula de alimentação de refinado na torre de ISOM

Equipamento(s)	a) SIS b) IHM
Sensor(es)	Transmisor de nível (LT-1)
Atuador(es)	Atuador da válvula de alimentação de refinado na torre ISOM

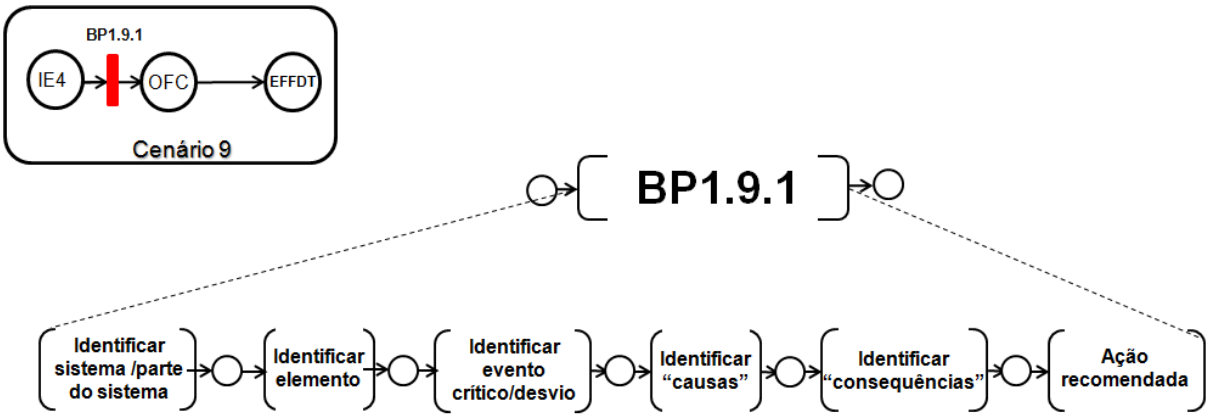
A Figura 89 mostra o modelo de prevenção do cenário crítico 9 em PFS. As Figura 90 e Figura 91 mostram os refinamentos de BP1.9.1 e BP1.9.2, respectivamente e as Tabela 20 e Tabela 21 as informações relacionadas a cada barreira.

Figura 89 – Modelo de prevenção do cenário crítico 9 em PFS



Fonte: próprio autor

Figura 90 – Refinamento da BP1.9.1

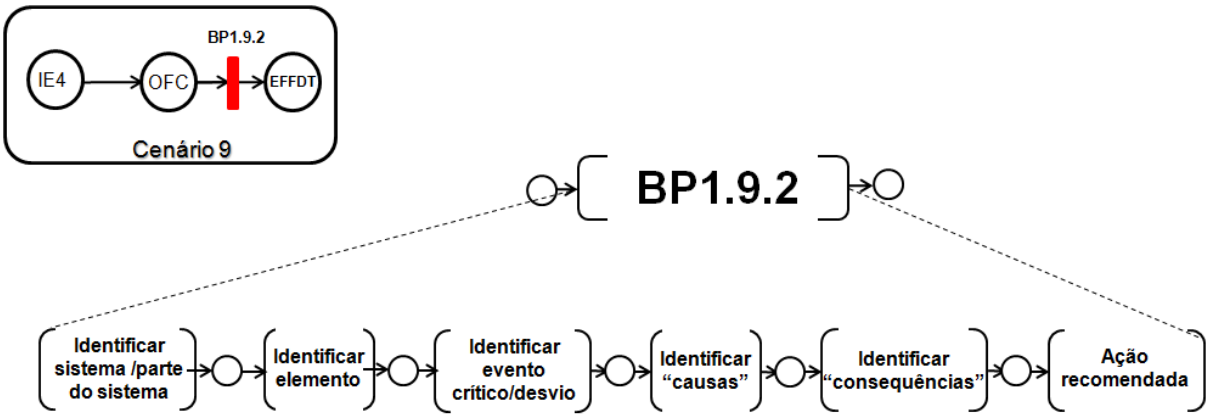


Fonte: próprio autor

Tabela 20 – Informações da BP1.9.1

Barreira	BP1.9.1
Sistema/parte do sistema	Sala de controle da unidade de isomerização
Elemento	Sensor 1 de nível alto de refinado na torre de isomerização
Evento crítico/ desvio	Alarme de nível alto 1 ignorado pelo operador
Causa(s)	a) Falta de gestão de riscos b) Falta de treinamento do(s) operador(es)
Consequência(s)	Falhas na operação da unidade de isomerização
Ações recomendadas	a) Fechar automaticamente a válvula de alimentação da torre de ISOM b) Planejar e implementar um sistema de gestão de riscos c) Planejar e implementar treinamentos de operação da unidade de isomerização e riscos
Equipamento(s)	a) SIS b) IHM
Sensor(es)	Sensor 1 de nível na torre de isomerização
Atuador(es)	Atuador da válvula de alimentação de refinado na torre ISOM

Figura 91 – Refinamento da BP1.9.2



Fonte: próprio autor

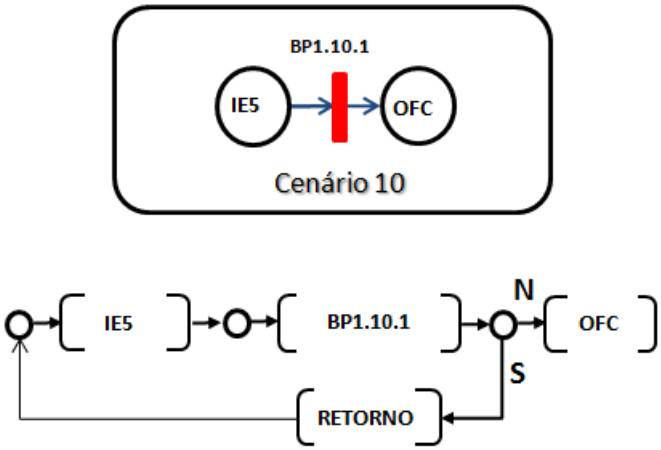
Tabela 21 – Informações da BP1.9.2

Barreira	BP1.9.2
Sistema/parte do sistema	Sala de controle da unidade de isomerização
Elemento	Nível de refinado na torre
Evento crítico/ desvio	Falhas na operação da unidade de isomerização
Causa(s)	Falha da barreira de prevenção BP1.9.1
Consequência(s)	Excesso de alimentação da torre de ISOM
Ações recomendadas	Fechar automaticamente a válvula de alimentação de refinado na torre de ISOM

Equipamento(s)	a) SIS b) IHM
Sensor(es)	não se aplica
Atuador(es)	Atuador da válvula de alimentação de refinado na torre ISOM

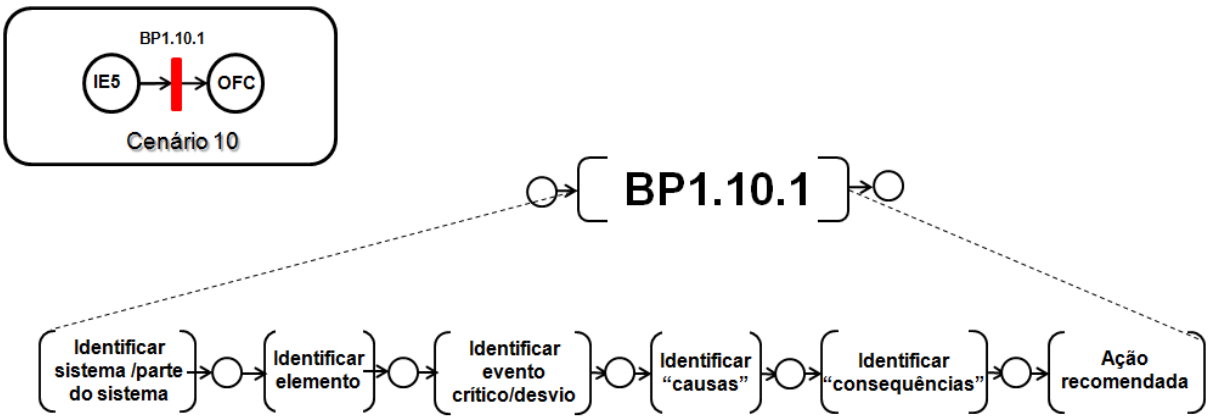
A Figura 92 mostra o modelo de prevenção do cenário crítico 10 em PFS. A Figura 93 mostra o refinamento da BP1.10.1 e a Tabela 22 as informações desta barreira.

Figura 92 – Modelo de prevenção do cenário crítico 10 em PFS



Fonte: próprio autor

Figura 93 – Refinamento da BP1.10.1



Fonte: próprio autor

Tabela 22 – Informações da BP1.10.1

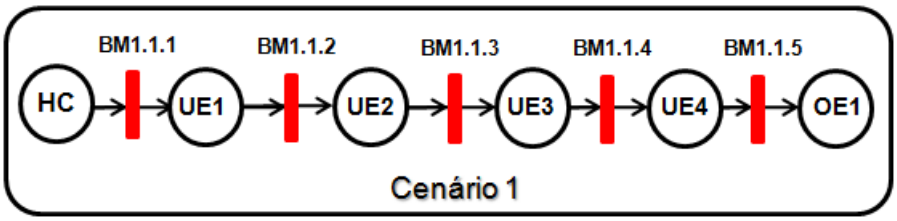
Barreira	BP1.10.1
Sistema/parte do sistema	Sala de controle da unidade de isomerização
Elemento	Sensor de temperatura de refinado dentro da torre de isomerização
Evento crítico/	Alarme de temperatura alta de refinado dentro da torre de ISOM ignorada pelo operador

desvio	
Causa(s)	a) Falha na gestão de riscos b) Falta de treinamento do(s) operador(es)
Consequência(s)	Falhas na operação da unidade de isomerização
Ações recomendadas	a) Fechar automaticamente a válvula de alimentação da torre de ISOM b) Abrir válvula inferior da torre de ISOM para redução do nível e temperatura c) Ligar bomba inferior d) Planejar e implementar um sistema de gestão de riscos e) Planejar e implementar treinamentos de operação da unidade de isomerização e riscos
Equipamento(s)	a) SIS b) IHM
Sensor(es)	Sensor de temperatura
Atuador(es)	a) Atuador da válvula de alimentação de refinado na torre ISOM b) Atuador da válvula inferior da torre de ISOM c) Contator de partida/parada da bomba inferior

Ainda na `atividade` de modelagem dos cenários críticos e barreiras em PFS e com base na Figura 64, são mostrados a seguir, os modelos de mitigação dos cenários críticos 1 a 6; dado o mesmo evento topo (HC).

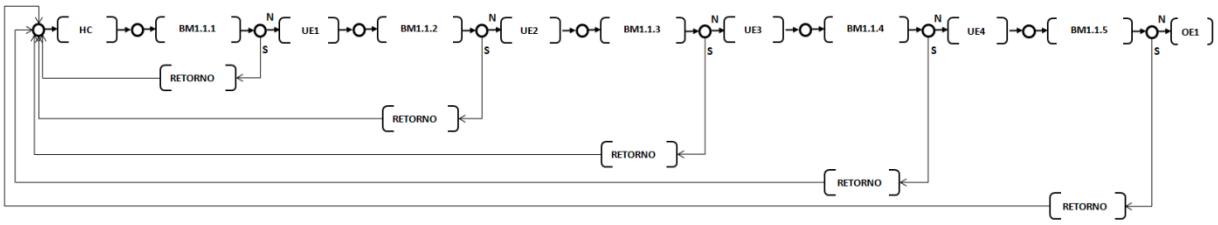
A Figura 94 ilustra o diagrama de barreiras do cenário crítico 1, e a Figura 95 o modelo de mitigação do mesmo cenário em PFS. A seguir, as Figura 96 a Figura 100 mostram os refinamentos de BM1.1.1 a BM1.1.5 respectivamente, e as Tabela 23 a Tabela 27, as informações relacionadas a cada barreira do mesmo cenário.

Figura 94 – Diagrama de barreiras do cenário crítico 1



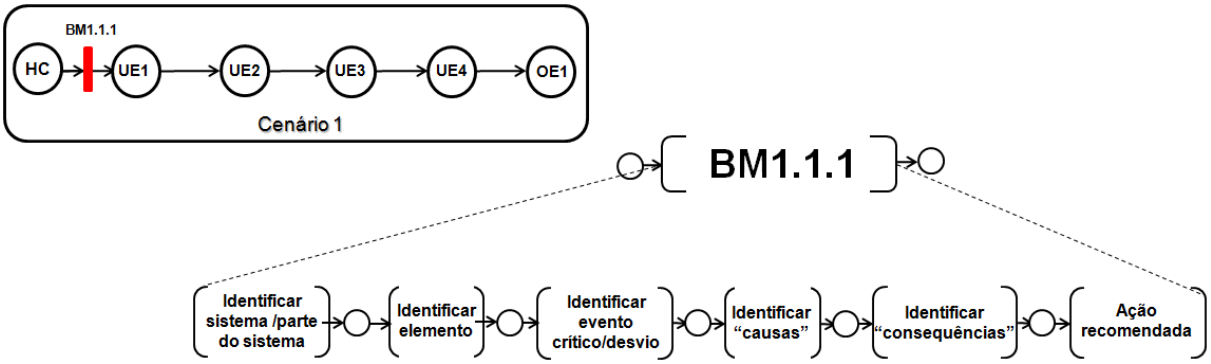
Fonte: próprio autor

Figura 95 – Modelo de mitigação do cenário crítico 1 em PFS



Fonte: próprio autor

Figura 96 – Refinamento da BM1.1.1

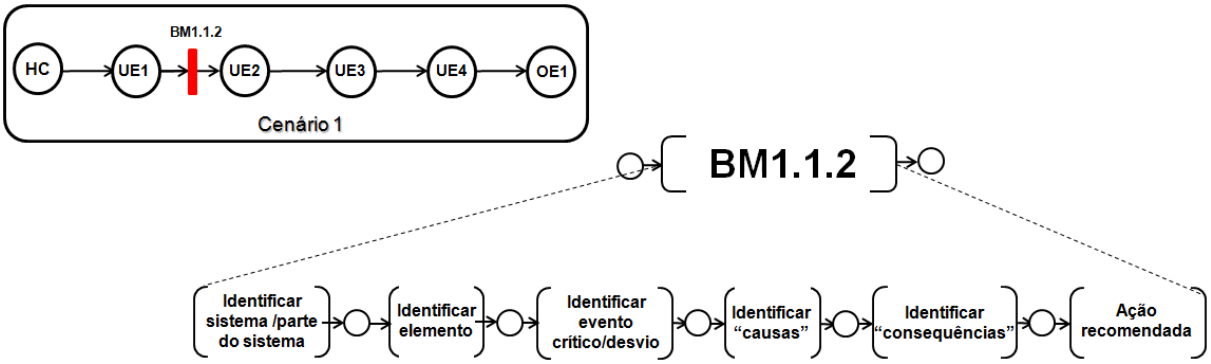


Fonte: próprio autor

Tabela 23 – Informações da BM1.1.1

Barreira	BM1.1.1
Sistema/parte do sistema	Unidade de Isomerização
Elemento	Tanque de *blowdown*
Evento crítico/ desvio	Lançamento de hidrocarboneto altamente inflamável
Causa(s)	Falha da barreira de prevenção BP1.4.3
Consequência(s)	Formação de nuvem de vapor de hidrocarboneto altamente inflamável
Ações recomendadas	a) Instalação de um sistema para queima dos gases de hidrocarbonetos na chaminé do tanque de *blowdown* (*flare system*) ou b) Instalar sensores de detecção de gás hidrocarboneto c) Diagnosticar e sinalizar alarme de presença de gás na chaminé do tanque de *blowdown* via algoritmo de votação "2oo3"
Equipamento(s)	a) SIS b) IHM
Sensor(es)	03 (três) sensores de gás
Atuador(es)	não se aplica

Figura 97 – Refinamento da BM1.1.2

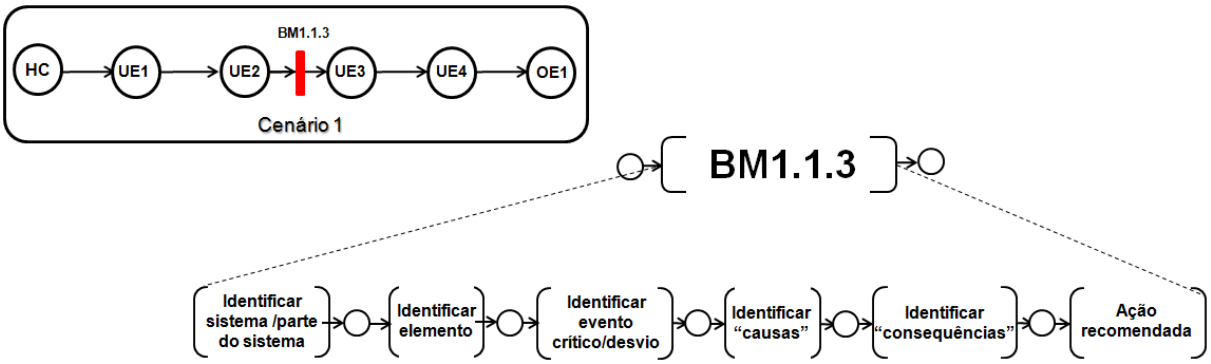


Fonte: próprio autor

Tabela 24 – Informações da BM1.1.2

Barreira	BM1.1.2
Sistema/parte do sistema	Unidade de Isomerização
Elemento	Tanque de *blowdown*
Evento crítico/ desvio	Formação de nuvem de vapor de hidrocarboneto altamente inflamável
Causa(s)	Falha na barreira BM1.1.1
Consequência(s)	Movimentação da nuvem de vapor
Ações recomendadas	a) Alarmar sinal de evacuação da unidade de isomerização b) Alarmar sinal para acionamento da brigada de incêndio
Equipamento(s)	a) SIS b) IHM
Sensor(es)	não se aplica
Atuador(es)	a) Buzina para alarme sonoro de evacuação da unidade de ISOM; b) Buzina para alarme de socorro

Figura 98 – Refinamento da BM1.1.3

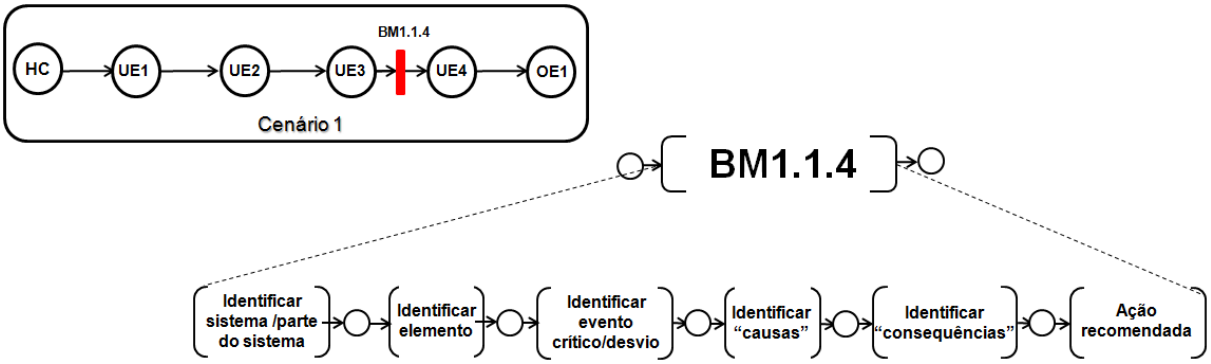


Fonte: próprio autor

Tabela 25 – Informações da BM1.1.3

Barreira	BM1.1.3
Sistema/parte do sistema	Unidade de Isomerização
Elemento	não se aplica
Evento crítico/ desvio	Movimentação de nuvem de vapor
Causa(s)	Falha da barreira BM1.1.2
Consequência(s)	Movimentação da nuvem de vapor para local com provável fonte de ignição
Ações recomendadas	a) Degenerar de forma controlada os equipamentos das unidades próximas à unidade de isomerização
Equipamento(s)	a) SIS b) IHM
Sensor(es)	não se aplica
Atuador(es)	Comandos via SIS para outros PES responsáveis pela degeneração controlada dos equipamentos das unidades próximas à unidade de isomerização

Figura 99 – Refinamento da BM1.1.4

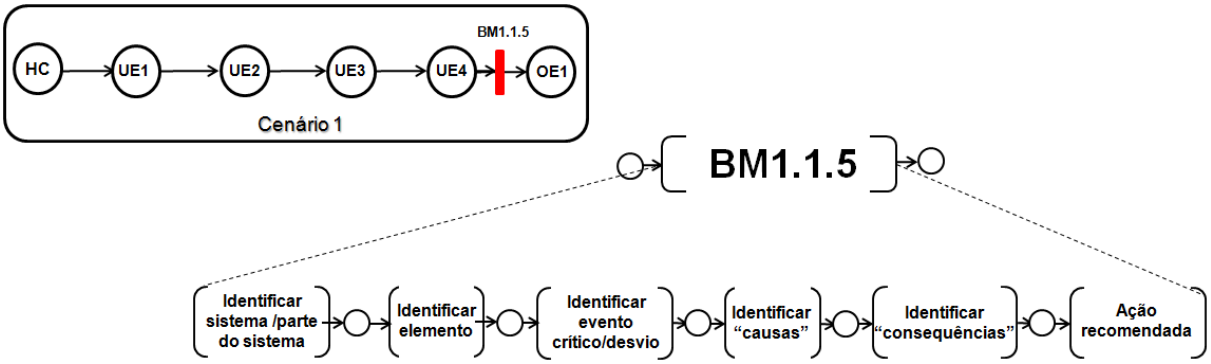


Fonte: próprio autor

Tabela 26 – Informações da BM1.1.4

Barreira	BM1.1.4
Sistema/parte do sistema	Unidade de Isomerização
Elemento	não se aplica
Evento crítico/ desvio	Ignição
Causa(s)	Falha da BM1.1.3
Consequência(s)	Nuvem de vapor e explosão (VCE) provocado por fonte de ignição
Ações recomendadas	a) Impedir entrada e/ou circulação de caminhões / carros na área de isomerização
Equipamento(s)	a) IHM
Sensor(es)	Câmeras
Atuador(es)	não se aplica

Figura 100 – Refinamento da BM1.1.5



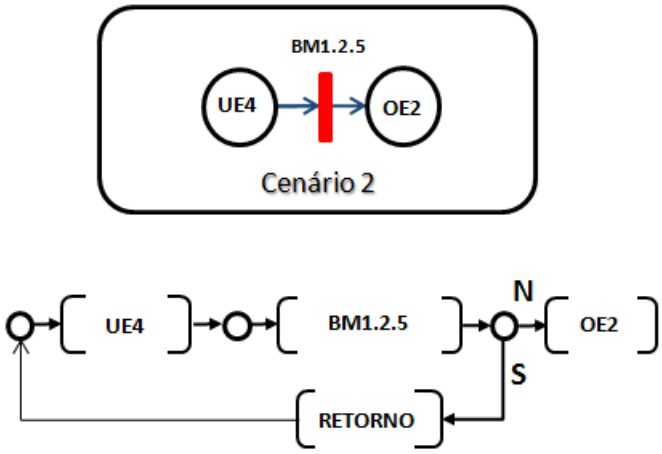
Fonte: próprio autor

Tabela 27 – Informações da BM1.1.5

Barreira	BM1.1.5
Sistema/parte do sistema	Unidade de Isomerização
Elemento	não se aplica
Evento crítico/ desvio	Nuvem de vapor e explosão (VCE) provocado por fonte de ignição
Causa(s)	Falha da barreira BM1.1.4
Consequência(s)	Nuvem de vapor e explosão
Ações recomendadas	a) Combater incêndio; b) Evacuar pessoas para local seguro;
Equipamento(s)	Equipamentos de combate a incêndio
Sensor(es)	não se aplica
Atuador(es)	não se aplica

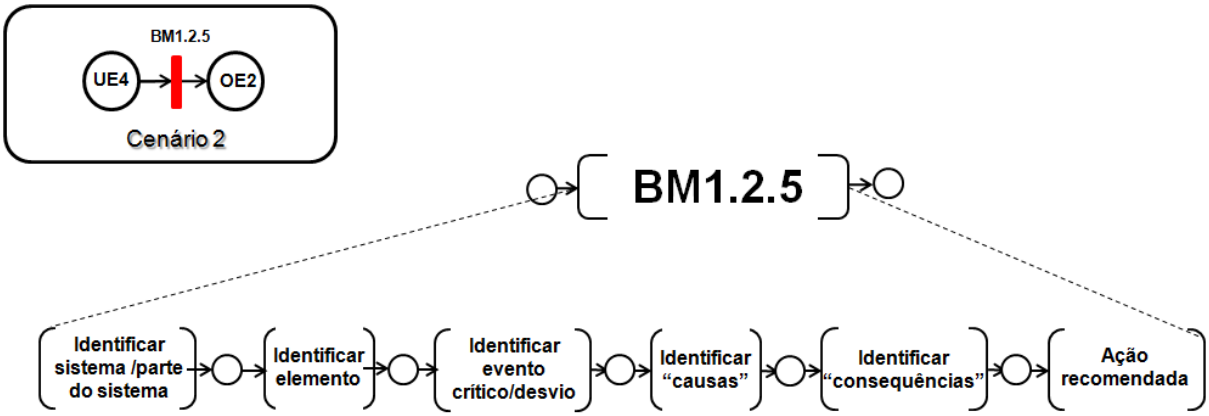
A Figura 101 ilustra o modelo de mitigação do cenário crítico 2. A Figura 102 ilustra o refinamento da BM1.2.5 e a Tabela 28 as informações desta barreira.

Figura 101 – Modelo de mitigação do cenário crítico 2 em PFS



Fonte: próprio autor

Figura 102 – Refinamento da BM1.2.5



Fonte: próprio autor

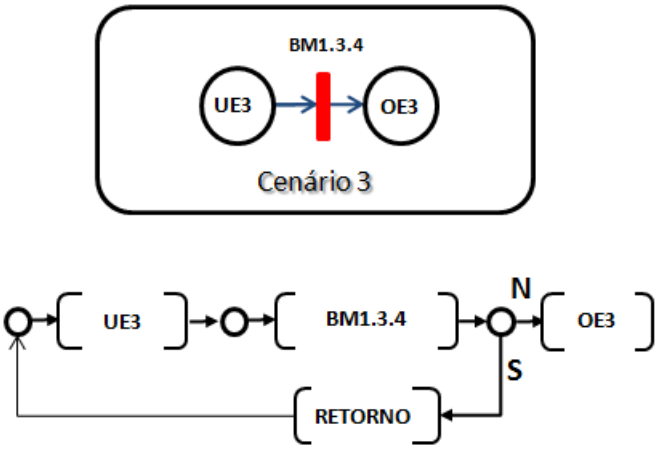
Tabela 28 – Informações da BM1.2.5

Barreira	BM1.2.5
Sistema/parte do sistema	Unidade de Isomerização
Elemento	não se aplica
Evento crítico/ desvio	Nuvem de vapor e explosão (VCE) provocado por fonte de ignição
Causa(s)	Falha da barreira BM1.1.4
Consequência(s)	Incêndio
Ações recomendadas	a) Combater incêndio; b) Evacuar pessoas para local seguro;
Equipamento(s)	Equipamentos de combate a incêndio
Sensor(es)	não se aplica
Atuador(es)	não se aplica

Fonte: próprio autor

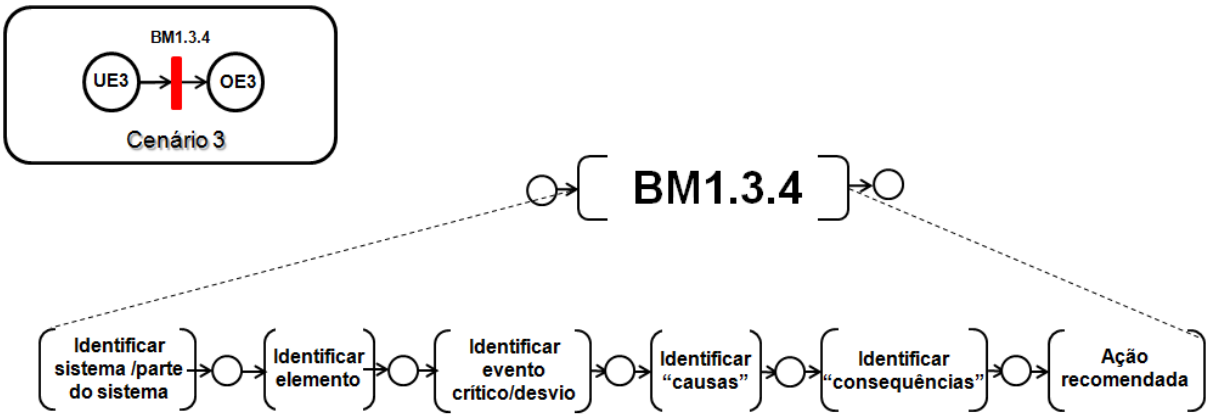
A Figura 103 ilustra o modelo de mitigação do cenário crítico 3 em PFS. A Figura 104 ilustra o refinamento da BM1.3.4 e a Tabela 29 as informações desta barreira.

Figura 103 – Modelo de mitigação do cenário crítico 3 em PFS



Fonte: próprio autor

Figura 104 – Refinamento da BM1.3.4



Fonte: próprio autor

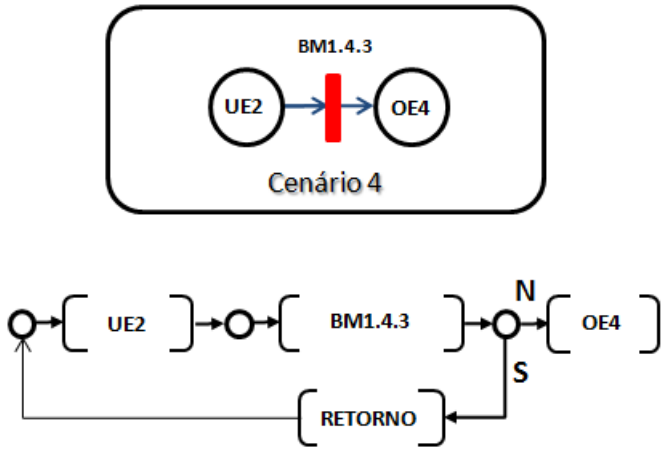
Tabela 29 – Informações da BM1.3.4

Barreira	BM1.3.4
Sistema/parte do sistema	Unidade de Isomerização
Elemento	não se aplica
Evento crítico/ desvio	Ignição
Causa(s)	Falha da barreira BM1.1.3
Consequência(s)	Nuvem de vapor de hidrocarboneto
Ações recomendadas	a) Instalar câmeras; b) Impedir entrada e/ou circulação de caminhões / carros na área de isomerização c) Degenerar de forma controlada os equipamentos de unidades vizinhas à unidade de ISOM
Equipamento(s)	a) SIS b) IHM

Sensor(es)	Câmeras
Atuador(es)	Comandos via SIS para outros PES responsáveis pela degeneração controlada dos equipamentos das unidades próximas à unidade de isomerização

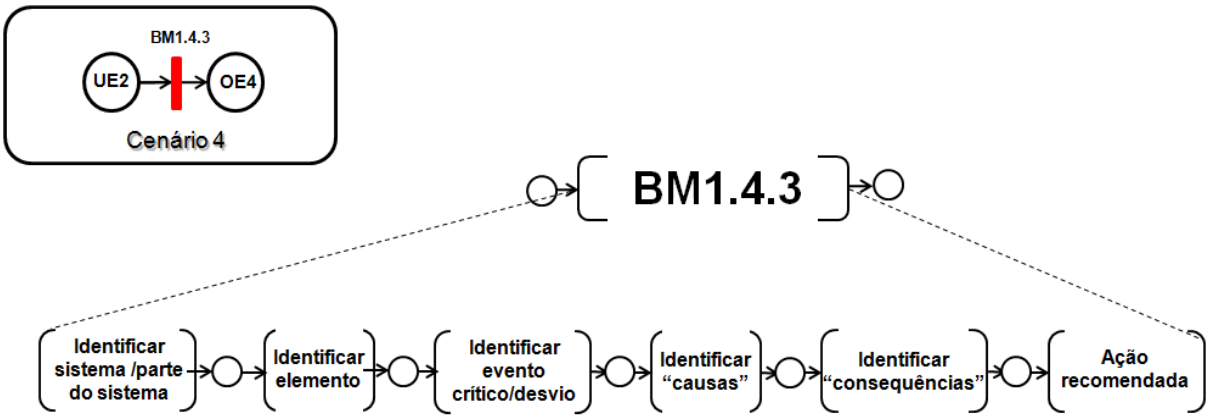
A Figura 105 ilustra o modelo de mitigação do cenário crítico 4 em PFS. A Figura 106 ilustra o refinamento de BM1.4.3 e a Tabela 30 as informações desta barreira.

Figura 105 – Modelo de mitigação do cenário crítico 4 em PFS



Fonte: próprio autor

Figura 106 – Refinamento da BM1.4.3



Fonte: próprio autor

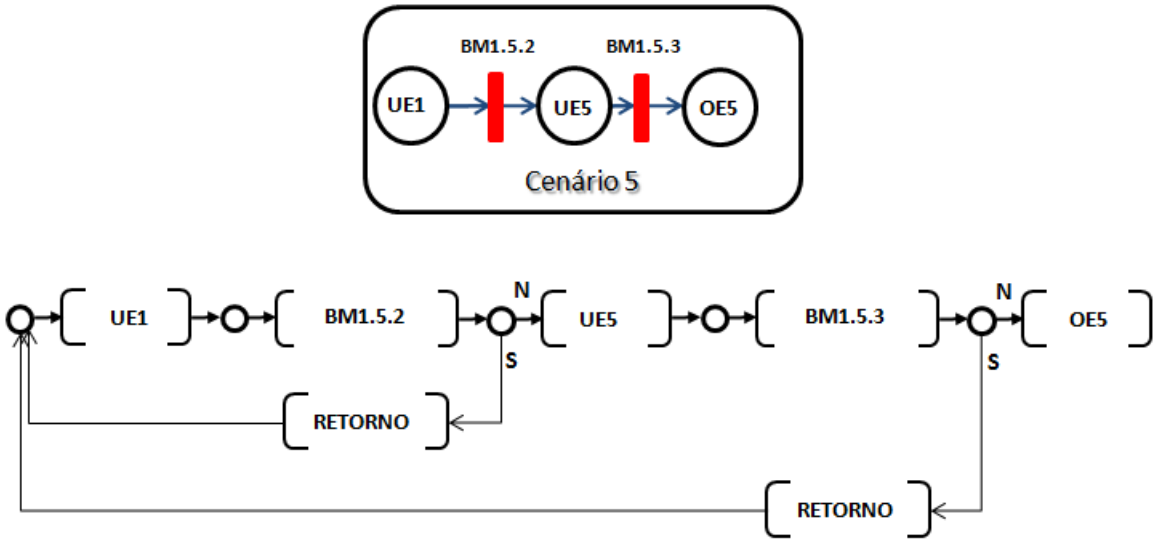
Tabela 30 – Informações da BM1.4.3

Barreira	BM1.4.3
Sistema/parte do sistema	Unidade de isomerização
Elemento	não se aplica
Evento crítico/ desvio	Movimentação de nuvem de vapor de hidrocarboneto (HC) altamente inflamável

Causa(s)	Falha da barreira BM1.1.2
Consequência(s)	Nuvem de vapor de HC sobre unidade de ISOM
Ações recomendadas	Degeneração de forma controlada dos equipamentos da unidade de ISOM.
Equipamento(s)	a) SIS b) IHM
Sensor(es)	Câmeras
Atuador(es)	Comandos de “parada” de forma controlada dos elementos da unidade de isomerização

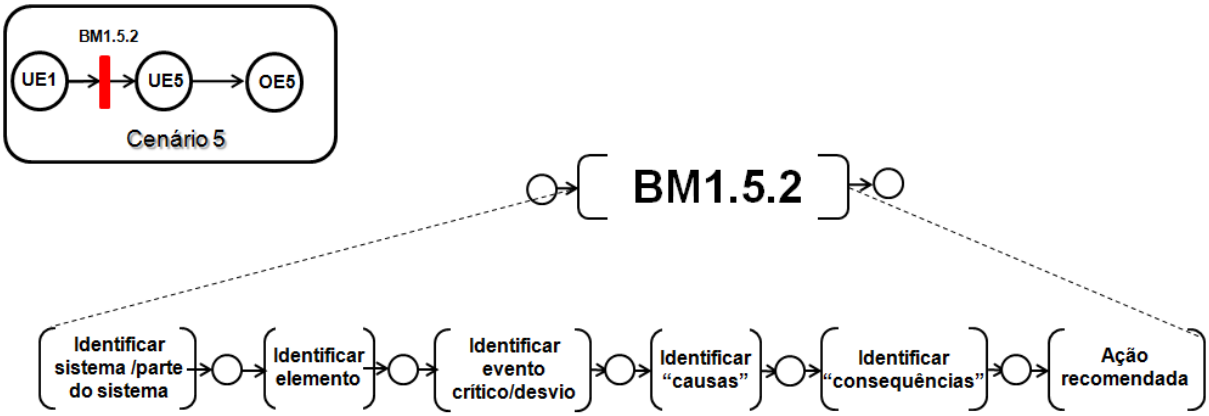
A Figura 107 ilustra o modelo de mitigação do cenário crítico 5 em PFS. As Figura 108 e Figura 109 ilustram os refinamentos das BM1.5.2 e BM1.5.3, respectivamente e as Tabela 31 e Tabela 32 as informações relacionadas a cada barreira.

Figura 107 – Modelo de mitigação do cenário crítico 5 em PFS



Fonte: próprio autor

Figura 108 – Refinamento da BM1.5.2

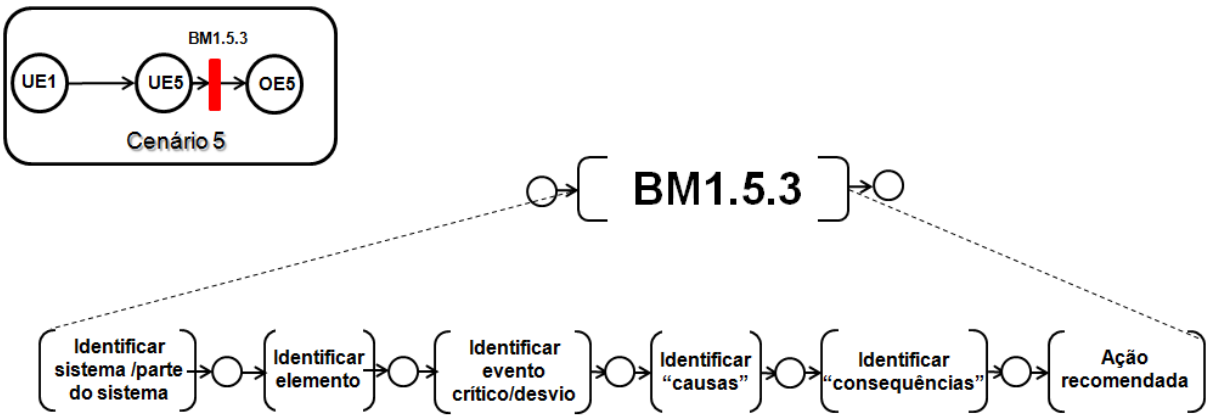


Fonte: próprio autor

Tabela 31 – Informações da BM1.5.2

Barreira	BM1.5.2
Sistema/parte do sistema	Unidade de Isomerização
Elemento	não se aplica
Evento crítico/ desvio	Formação de nuvem de vapor de hidrocarboneto altamente inflamável
Causa(s)	Falha na barreira BM1.1.1
Consequência(s)	Incêndio e explosão
Ações recomendadas	a) Alarmar sinal de evacuação da unidade de isomerização b) Alarmar sinal para acionamento da brigada de incêndio
Equipamento(s)	a) SIS b) IHM
Sensor(es)	não se aplica
Atuador(es)	a) Buzina para alarme sonoro de evacuação da unidade de ISOM; b) Buzina para alarme de socorro

Figura 109 – Refinamento da BM1.5.3



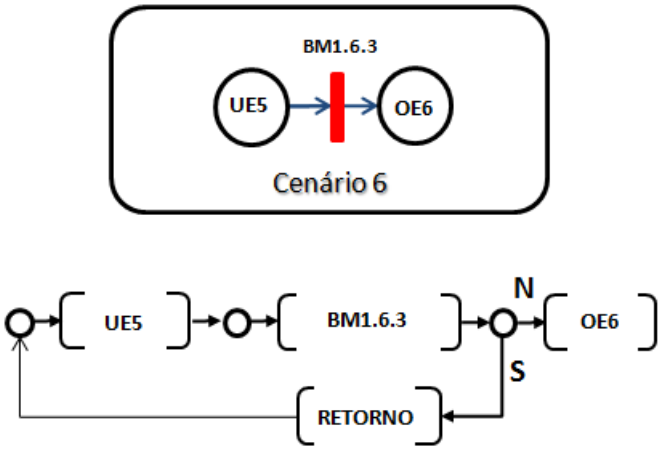
Fonte: próprio autor

Tabela 32 – Informações da BM1.5.3

Barreira	BM1.5.3
Sistema/parte do sistema	Unidade de Isomerização
Elemento	não se aplica
Evento crítico/ desvio	Incêndio e explosão
Causa(s)	Falha da barreira BM1.5.2
Consequência(s)	Piscina de fogo
Ações recomendadas	a) Alarmar sinal de evacuação da unidade de isomerização b) Alarmar sinal para acionamento da brigada de incêndio
Equipamento(s)	a) SIS b) IHM
Sensor(es)	não se aplica
Atuador(es)	a) Buzina para alarme sonoro de evacuação da unidade de ISOM; b) Buzina para alarme de socorro

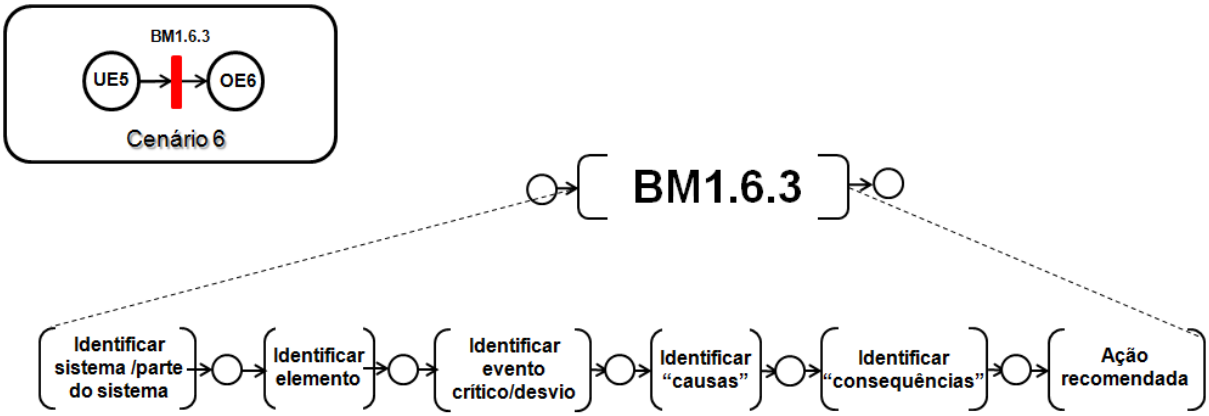
A Figura 110 ilustra o modelo de mitigação do cenário crítico 6 em PFS. A Figura 111 ilustra o refinamento da BM1.6.3 e a Tabela 33 as informações desta barreira.

Figura 110 – Modelo de mitigação do cenário crítico 6 em PFS



Fonte: próprio autor

Figura 111 – Refinamento da BM1.6.3



Fonte: próprio autor

Tabela 33 – Informações da BM1.6.3

Barreira	BM1.6.3
Sistema/parte do sistema	Unidade de Isomerização
Elemento	não se aplica
Evento crítico/ desvio	Incêndio e explosão
Causa(s)	Falha da barreira BM1.5.2
Consequência(s)	Piscina de Hidrocarboneto
Ações recomendadas	a) Alarmar sinal de evacuação da unidade de isomerização b) Alarmar sinal para acionamento da brigada de incêndio
Equipamento(s)	a) SIS b) IHM
Sensor(es)	não se aplica
Atuador(es)	a) Buzina para alarme sonoro de evacuação da unidade de ISOM; b) Buzina para alarme de socorro

- **Preenchimento da Tabela de HAZOP**

Nesta atividade, as informações das barreiras de prevenção e mitigação, obtidas para todos os cenários críticos modelados, são utilizadas para o preenchimento da Tabela de HAZOP. Os resultados desta etapa, ou seja, as Tabelas de HAZOP são mostradas no Apêndice E deste trabalho.

4.1.1.4 Fase 4 – Geração dos algoritmos de defesa de prevenção e mitigação de falhas críticas

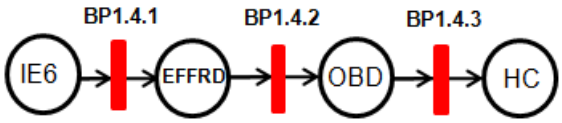
O cenário completo deste acidente para o evento topo HC (hidrocarboneto altamente inflamável) é representado via diagrama de barreiras na Figura 62

(diagrama de barreiras de prevenção) e na Figura 64 (diagrama de barreiras de mitigação).

A aplicação do procedimento proposto é apresentada abaixo.

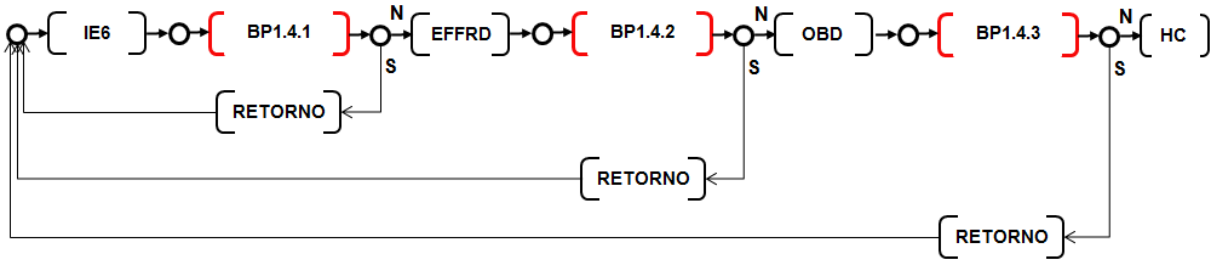
Passo 1: Considerando a AF do cenário completo, listar os modelos em PFS de todos os cenários críticos com as respectivas barreiras. Na Figura 112 é ilustrado como exemplo, o diagrama de barreiras de prevenção para o cenário crítico 4 e na Figura 113 é ilustrado o grafo PFS correspondente.

Figura 112 – Diagrama de barreiras de prevenção para o cenário crítico 4



Fonte: próprio autor

Figura 113 – Cenário crítico 4 em PFS

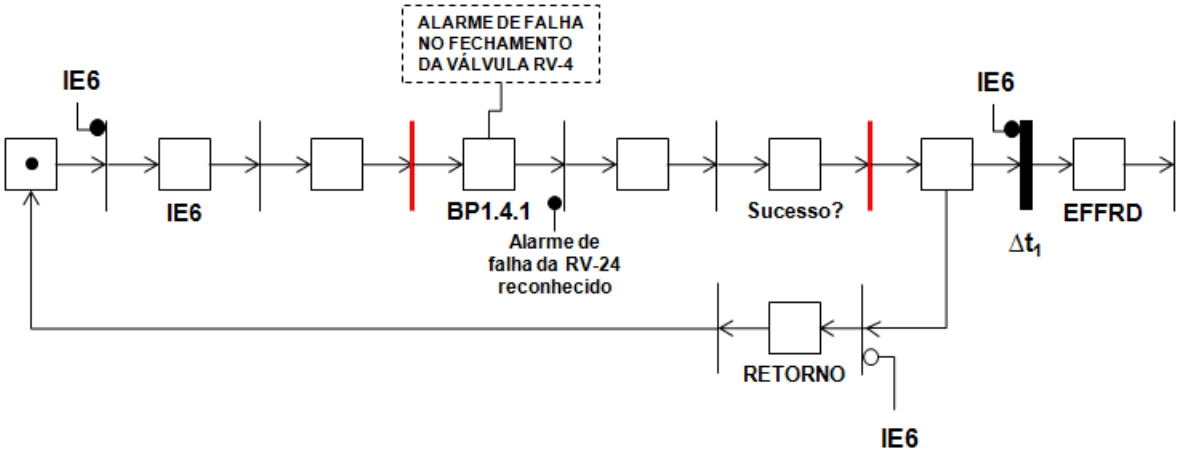


Fonte: próprio autor

Passo 2: Para cada barreira de prevenção, representada no modelo em PFS como uma `atividade`, detalhar o algoritmo de defesa para tratamento dos eventos iniciadores/críticos usando um modelo MFG. As ações a serem executadas pelas barreiras de prevenção são baseadas no HAZOP (ver Apêndice E).

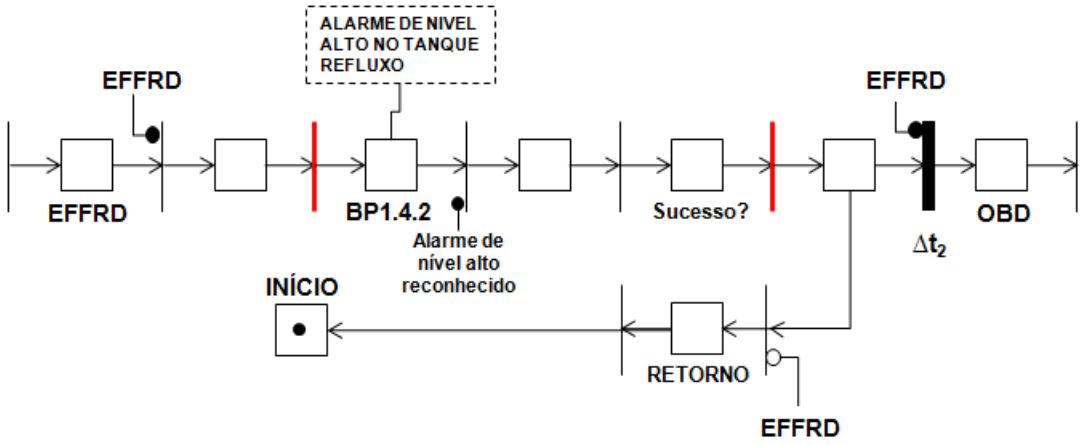
Para exemplificar este passo, no caso do cenário crítico 4, os modelos em MFG resultantes para as barreiras de prevenção: BP1.4.1, BP1.4.2 e BP1.4.3 são ilustrados nas Figura 114, Figura 115 e Figura 116, respectivamente.

Figura 114 – Modelo MFG da barreira de prevenção BP1.4.1



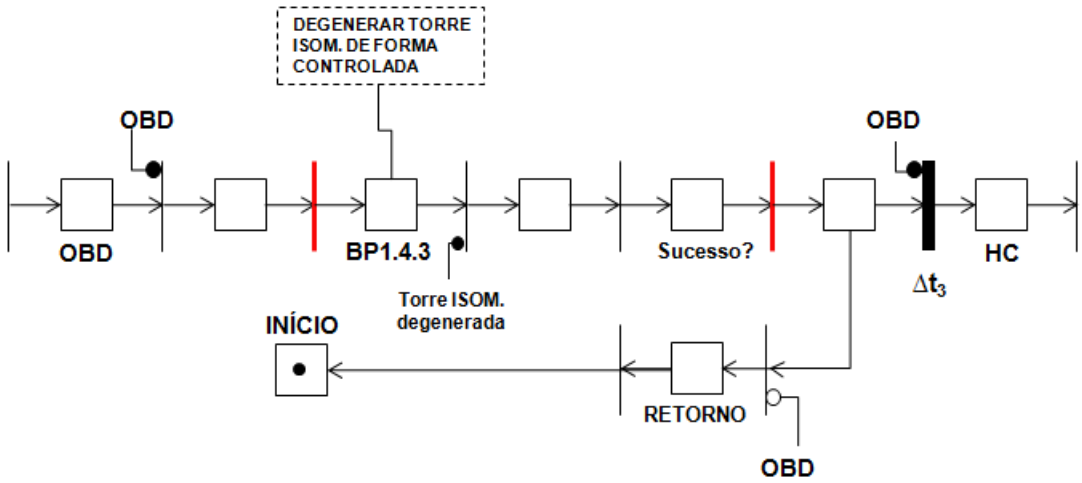
Fonte: próprio autor

Figura 115 – Modelo MFG da barreira de prevenção BP1.4.2



Fonte: próprio autor

Figura 116 – Modelo MFG da barreira de prevenção BP1.4.3

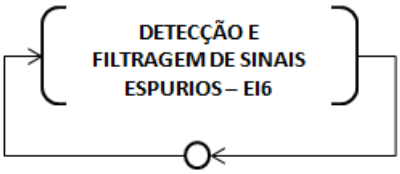


Fonte: próprio autor

As transições temporizadas Δt_1, Δt_2 e Δt_3, ilustradas nos grafos acima, correspondem ao atraso de tempo tolerável de execução das barreiras BP1.4.1, BP1.4.2 e BP1.4.3, respectivamente. Este tempo está associado com os tempos de resposta dos dispositivos de atuação.

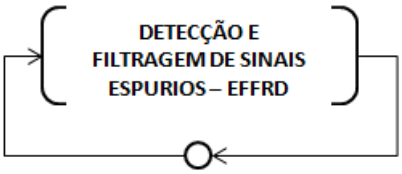
Passo 3: Construir o modelo PFS correspondente à detecção e diagnóstico de cada evento iniciador/crítico relacionado com o cenário crítico de prevenção considerado. No caso do cenário crítico 4 ilustrado na Figura 113, o evento iniciador é denominado de IE6 e os eventos críticos são: EFFRD e OBD. As Figura 117, Figura 118 e Figura 119, ilustram os modelos PFS correspondentes.

Figura 117 – Modelo PFS de detecção e diagnóstico do evento iniciador IE6



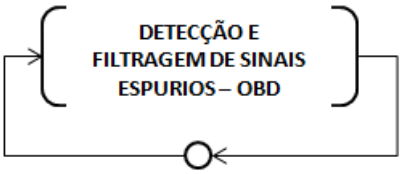
Fonte: próprio autor

Figura 118 – Modelo PFS de detecção e diagnóstico do evento crítico EFFRD



Fonte: próprio autor

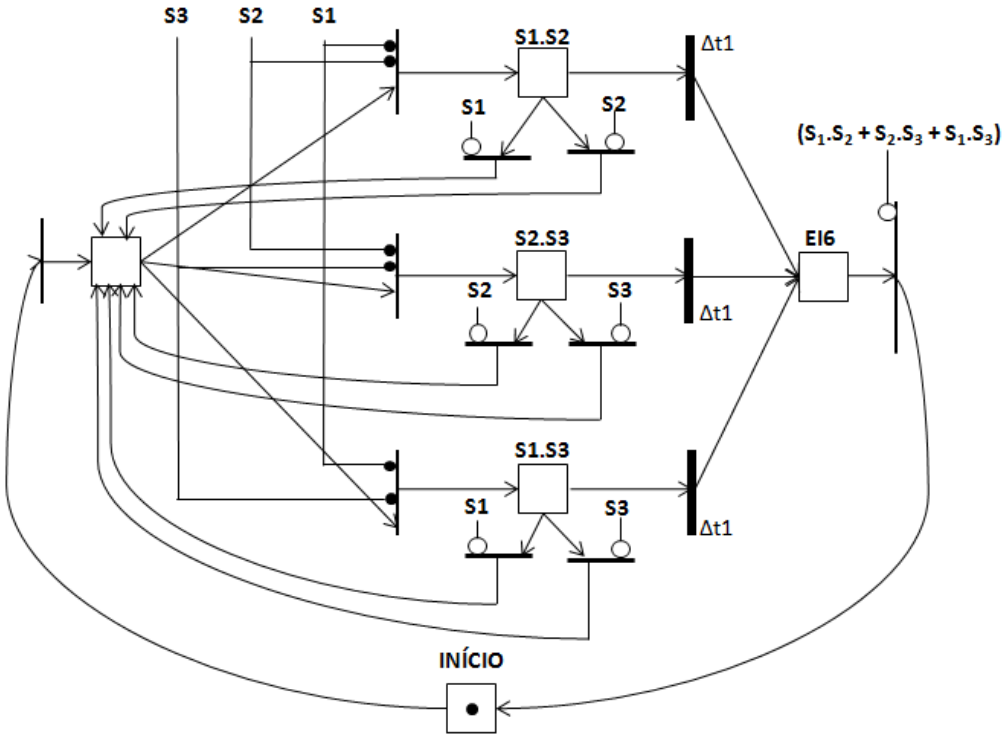
Figura 119 – Modelo PFS de detecção e diagnóstico do evento crítico OBD



Fonte: próprio autor

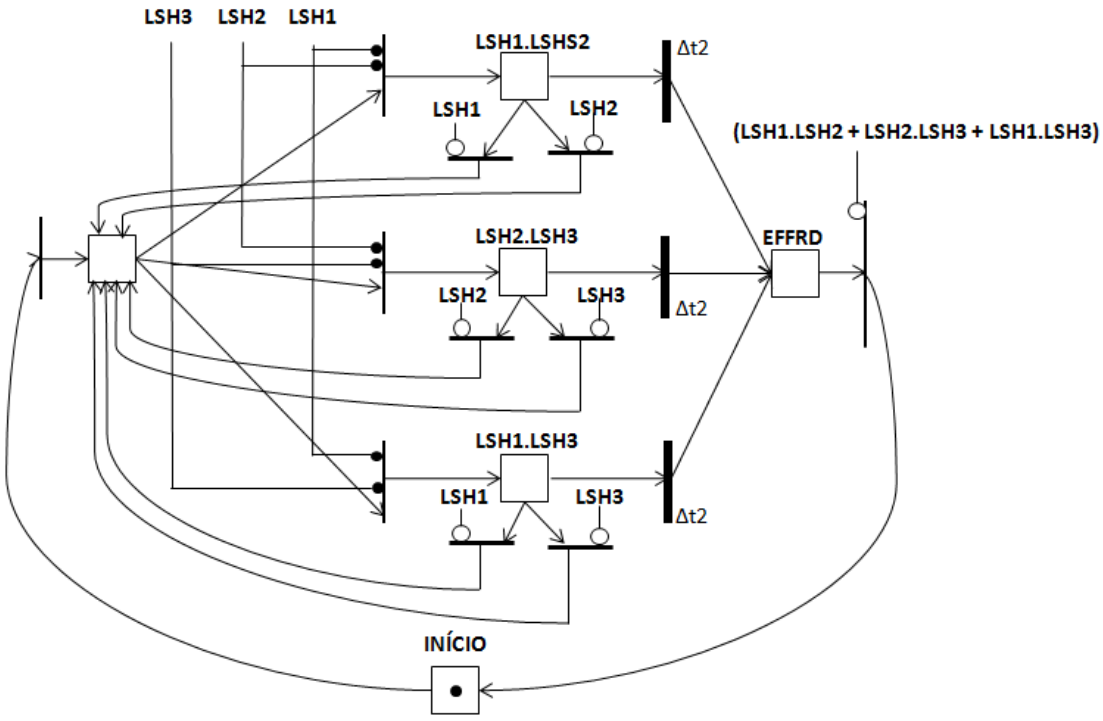
Passo 4: Refinar a `atividade` de detecção e filtragem de sinais espúrios de cada evento iniciador/crítico, em um modelo MFG correspondente. Os sensores a serem considerados para cada evento iniciador, crítico e/ou indesejado, são baseados no HAZOP (ver Apêndice E). As Figura 120, Figura 121 e Figura 122 ilustram os modelos MFGs correspondentes.

Figura 120 – Modelo MFG – detecção e filtragem de sinais espúrios – IE6



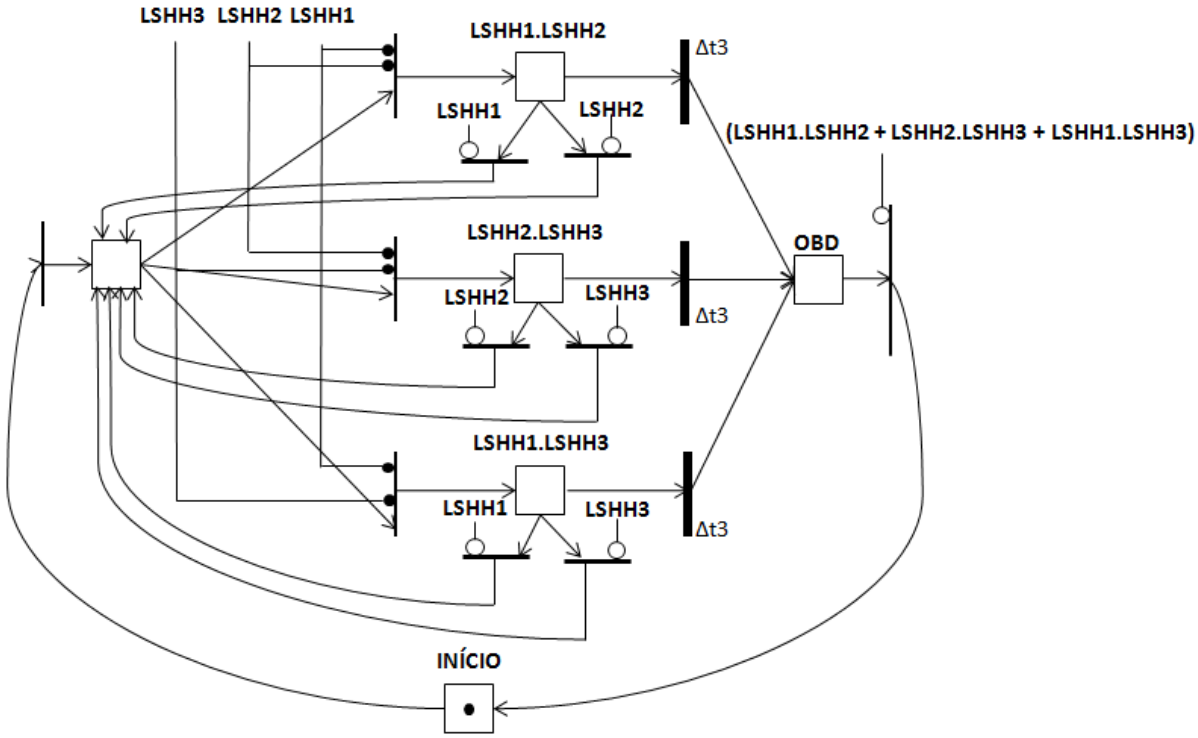
Fonte: próprio autor

Figura 121 – Modelo MFG – detecção e filtragem de sinais espúrios - EFFRD



Fonte: próprio autor

Figura 122 – Modelo MFG – detecção e filtragem de sinais espúrios - OBD



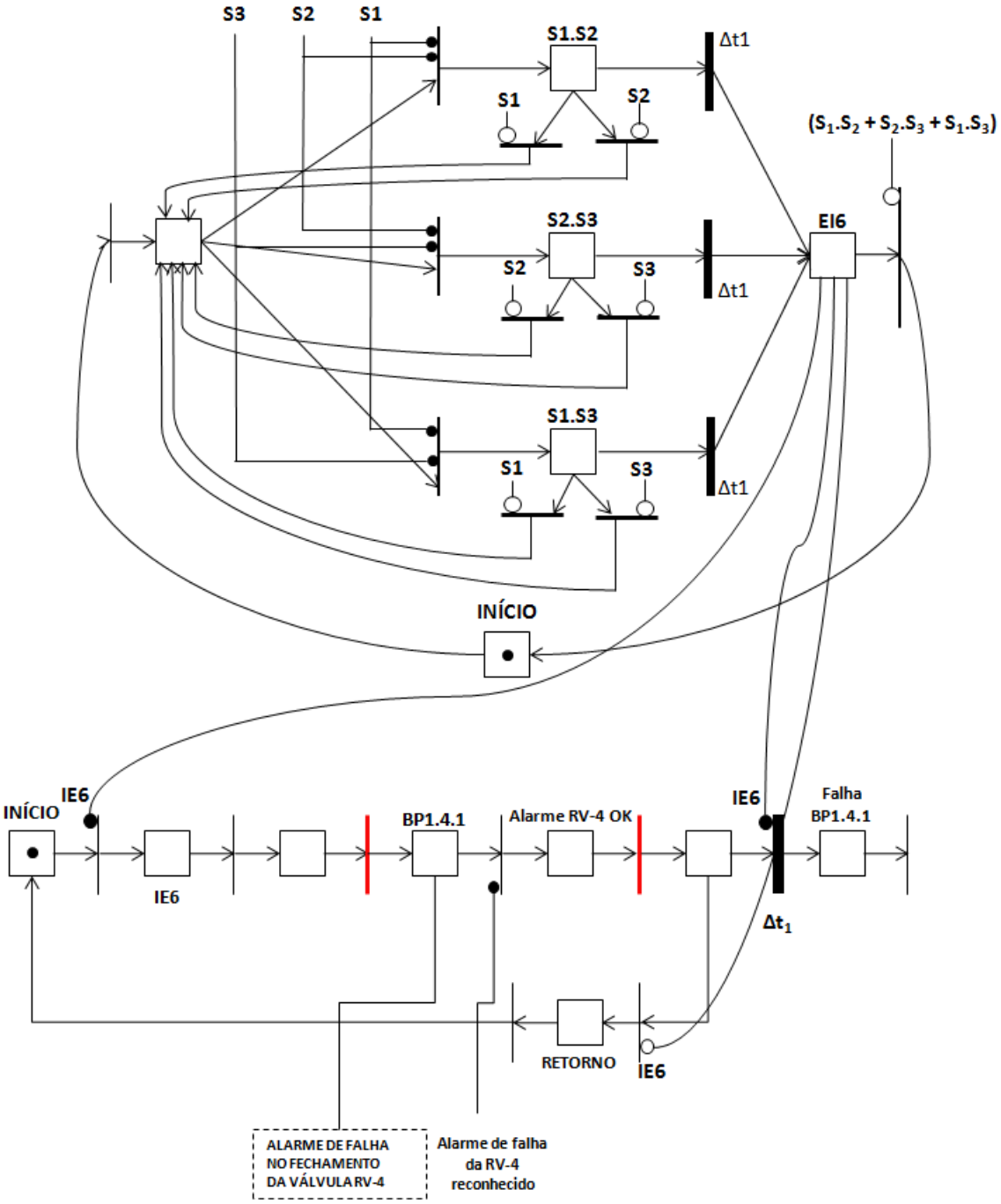
Fonte: próprio autor

Cada modelo MFG representa o modelo de um diagnosticador local exigido para cada evento iniciador/crítico que possa surgir durante a operação de uma planta de um SCr. Desta forma assegura-se a propriedade de diagnosticabilidade segura(PAOLI e LAFORTUNE, 2005), que exige a existência de um diagnosticador local para cada evento crítico do sistema. A detecção e diagnóstico de cada evento iniciador/crítico, representado nos modelos acima, considera a existência de três sensores redundantes, a fim de aumentar a confiabilidade geral do sistema de controle. O algoritmo de diagnóstico representado, corresponde à lógica de votação 2oo3 (do termo inglês *2 out of 3*), ou seja, se pelo menos dois sensores indicarem nível alto, a saída é considerada como sendo de nível alto, caso contrário, a saída é considerada como sendo de nível baixo. As transições temporizadas Δt_1, Δt_2 e Δt_3, correspondem ao tempo de atraso máximo para a detecção do evento crítico pelo diagnosticador local. Este tempo está associado com os tempos de atraso dos dispositivos de sensoriamento.

Passo 5: Integrar os modelos MFG de detecção e filtragem de eventos iniciadores/críticos com os modelos MFG correspondentes ao tratamento destes eventos via barreiras de segurança. As Figura 123, Figura 124 e Figura 125, ilustram

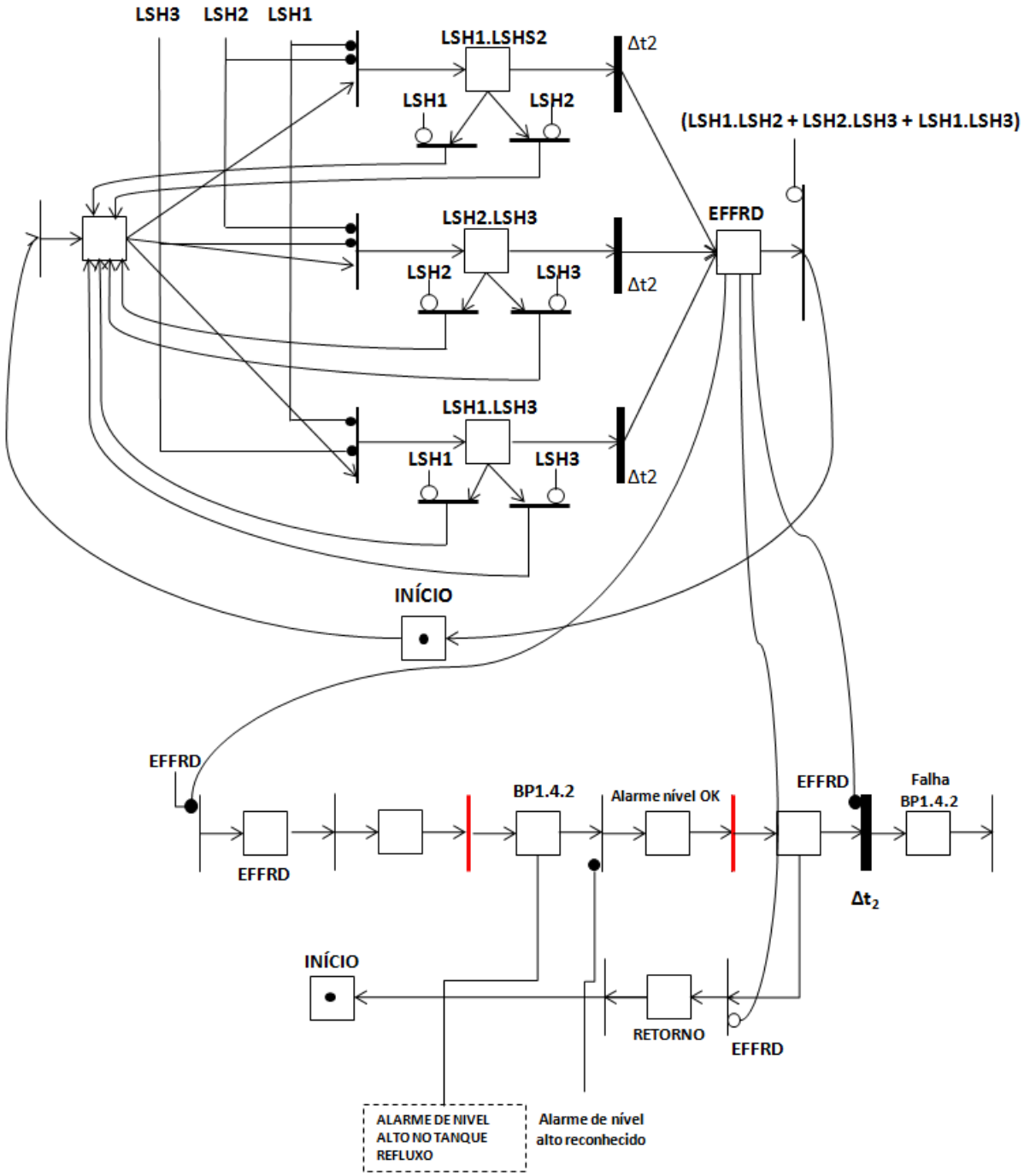
os grafos MFG correspondentes à detecção, filtragem e tratamento dos eventos IE6, EFFRD e OBD, respectivamente.

Figura 123 – Grafo MFG de detecção, filtragem e tratamento do evento IE6



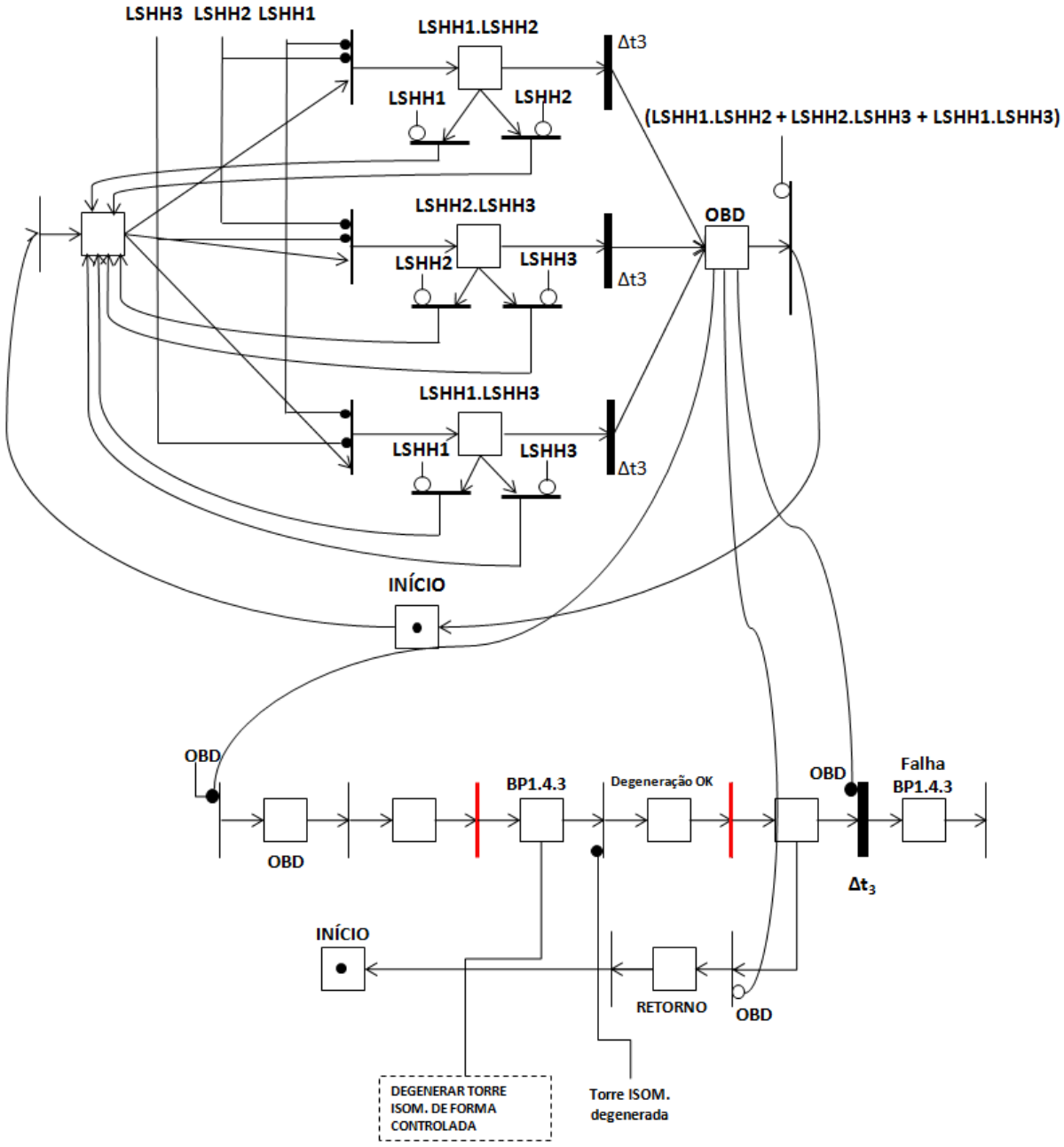
Fonte: próprio autor

Figura 124 – Grafo MFG de detecção, filtragem e tratamento do evento EFFRD



Fonte: próprio autor

Figura 125 – Grafo MFG de detecção, filtragem e tratamento do evento OBD



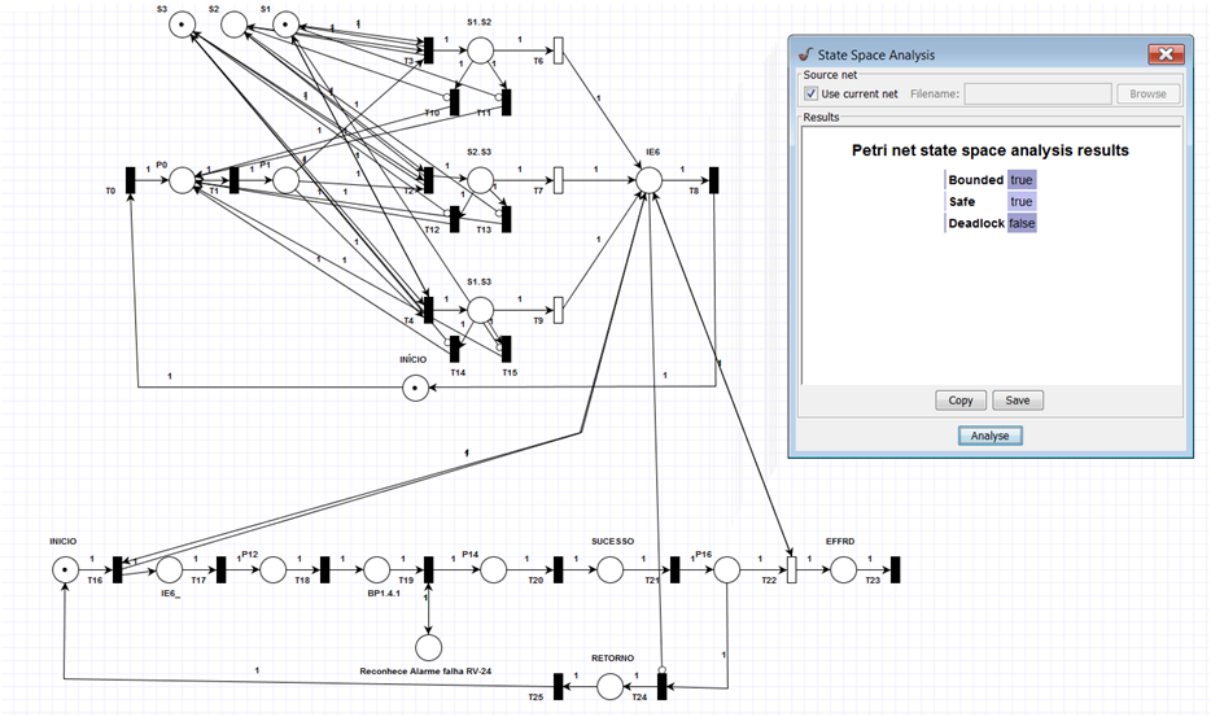
Fonte: próprio autor

Passo 6: Verificar as propriedades de segurança e vivacidade de cada grafo de detecção, diagnóstico e tratamento dos eventos.

Neste exemplo, as propriedades de segurança e vivacidade dos modelos foram verificadas com uso da ferramenta PIPE v.4.5[18]. A Figura 126 apresenta como exemplo a verificação do modelo MFG do processo de detecção, diagnóstico e tratamento do evento IE6.

[18] http://pipe2.sourceforge.net/. Acesso em 23/12/2016

Figura 126 – Verificação das propriedades do modelo MFG de detecção, diagnóstico e tratamento do evento iniciador IE6

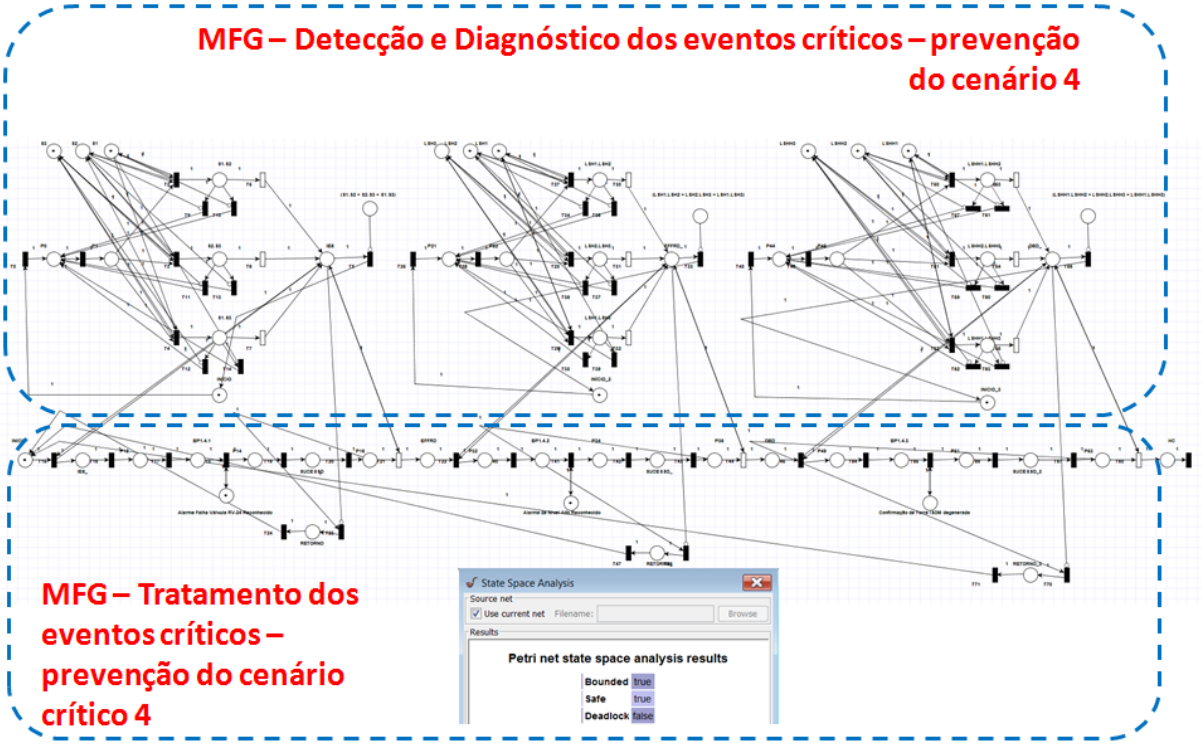


Fonte: próprio autor

Passo 7 – Integrar os modelos de detecção, filtragem e tratamento de cada evento pertinente aos cenários críticos. Neste exemplo, o algoritmo de defesa de prevenção da falha crítica HC derivado do cenário crítico 4 é ilustrado na Figura 130.

Passo 8 - Verificar as propriedades de segurança e vivacidade do modelo resultante. Neste exemplo, as propriedades foram verificadas com o uso da ferramenta PIPE v.4.5. A Figura 127 mostra um exemplo da verificação do modelo MFG sendo conduzida no PIPE.

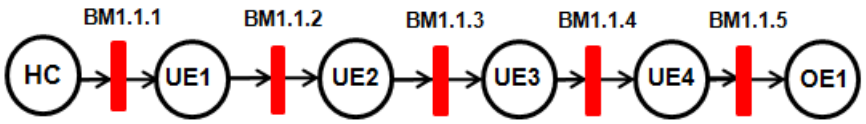
Figura 127 – Verificação das propriedades de segurança e vivacidade do modelo derivado do cenário crítico 4



Fonte: próprio autor

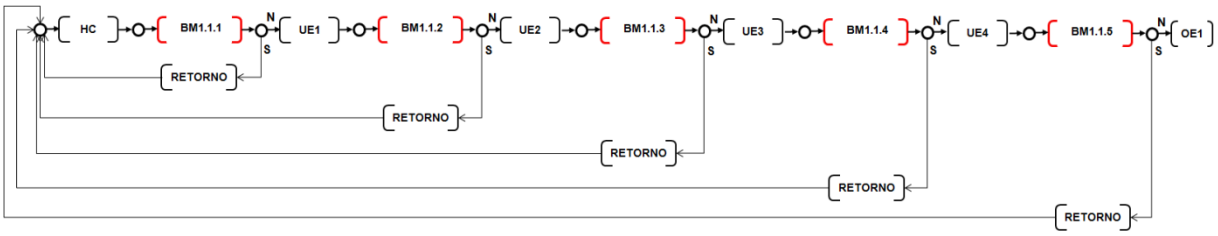
Passos 9 a 16 - Considerando agora a AE do cenário completo, modelou-se em PFS todos os cenários críticos representados por diagramas de barreiras. Na Figura 128, por exemplo, é ilustrado o diagrama de barreiras de mitigação para o cenário crítico 1 e na Figura 129 é ilustrado o modelo em PFS correspondente.

Figura 128 – Diagrama de barreiras de mitigação para o cenário crítico 1



Fonte: próprio autor

Figura 129 – Mitigação do cenário crítico 1 em PFS

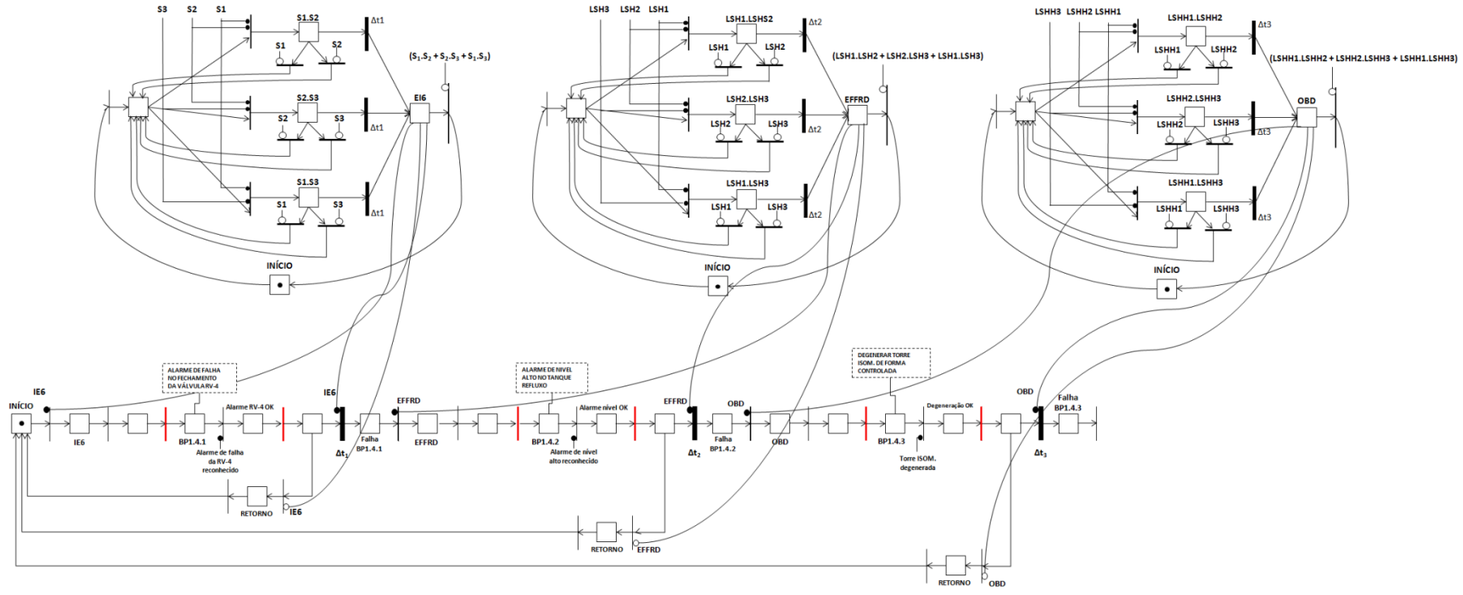


Fonte: próprio autor

Desenvolveu-se a modelagem dos algoritmos de defesa de prevenção da falha crítica, para cada um dos modelos de mitigação do cenários críticos 1 a 6, obtendo-se como resultado o algoritmo de defesa de mitigação da falha crítica HC. Na Figura 131 tem-se como exemplo o modelo MFG referente ao algoritmo de defesa de mitigação da falha crítica HC derivado do cenário crítico 1.

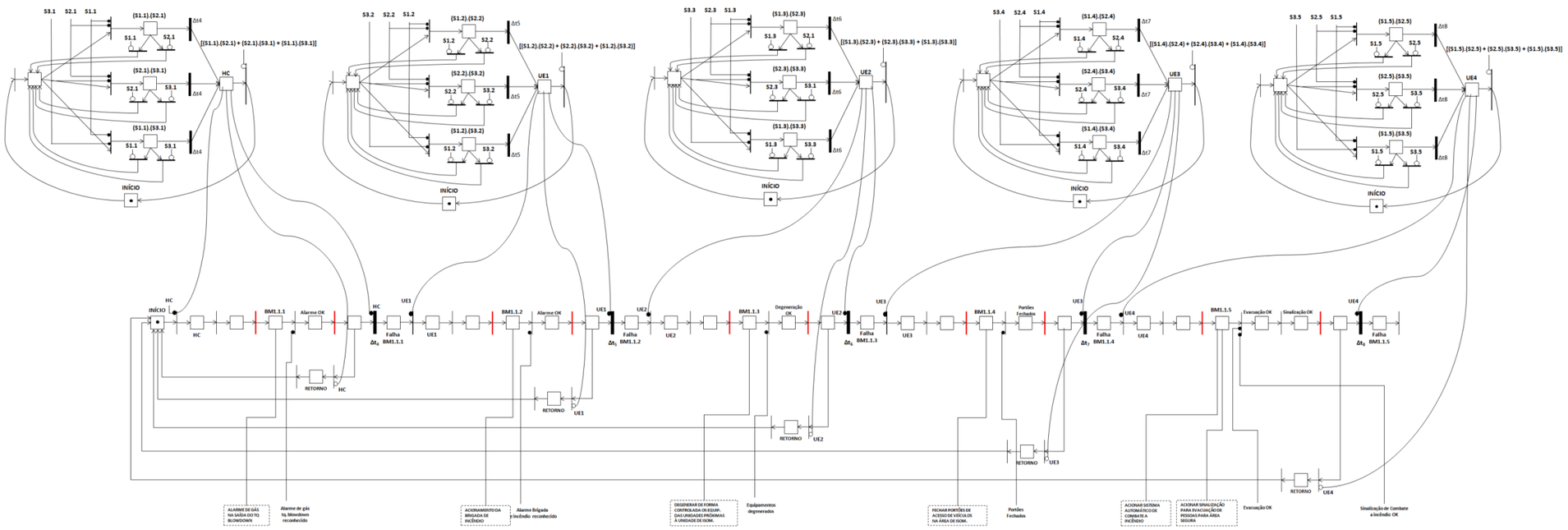
Os modelos MFG resultantes que representam os algoritmos de defesa de prevenção e mitigação da falha crítica HC, podem ser convertidos para um programa de controle numa linguagem IEC 61131-3 (ex: *Sequential Function Chart* (SFC), *Ladder Diagram* (LD)), para controladores programáveis de segurança (SIS).

Figura 130 – Algoritmo de defesa para a prevenção da falha crítica HC derivado do cenário crítico 4



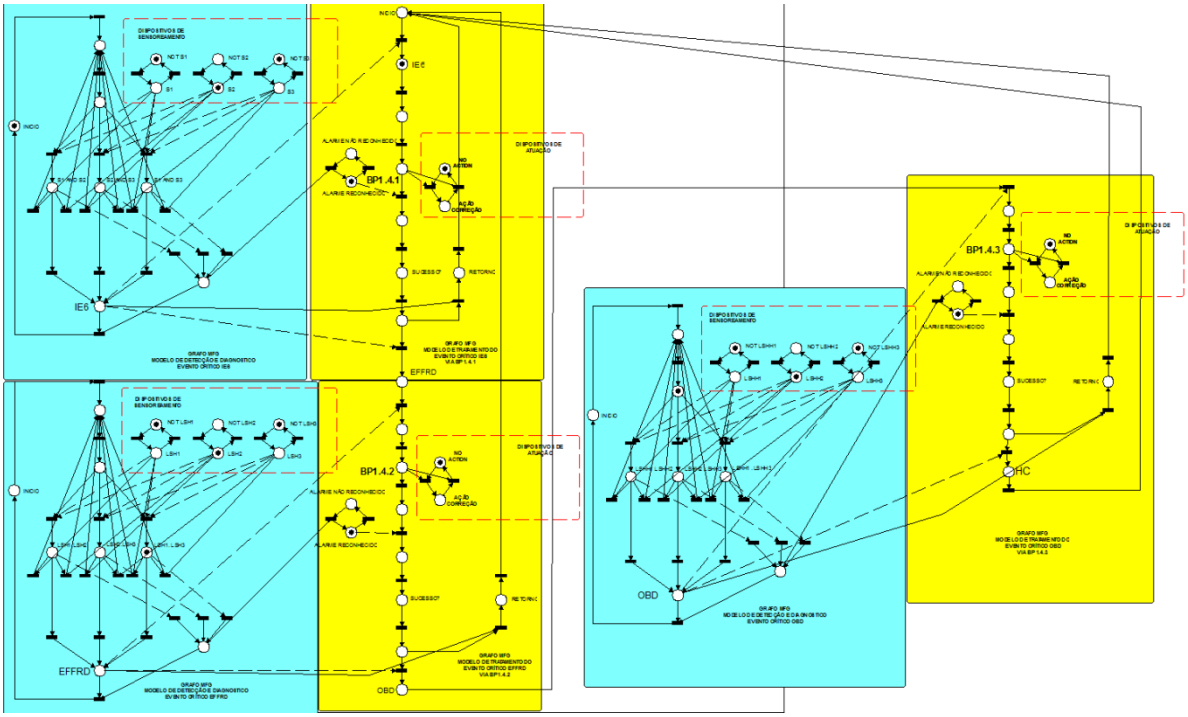
Fonte: próprio autor

Figura 131 – Algoritmo de defesa para a mitigação da falha crítica HC derivado do cenário crítico 1



É importante ressaltar, que antes de elaborar os algoritmos de defesa (IEC 61131-3), é recomendável também verificar a propriedade de reiniciabilidade dos modelos resultantes(SQUILLANTE JR, 2011). Esta propriedade pode ser verificada com o uso da ferramenta HPSIM[19]. A Figura 132 ilustra o uso do HPSim para a verificação da propriedade de reiniciabilidade para o modelo de detecção, filtragem e tratamento de eventos críticos para a prevenção do cenário crítico 4.

Figura 132 – Verificação da propriedade de reiniciabilidade do modelo de prevenção do cenário crítico 4



Fonte: próprio autor

[19] http://www.winpesim.de/default.html, acessado em 23/12/2016.

4.2 DISCUSSÃO DOS RESULTADOS

O *framework* proposto para a síntese de SCSP foi aplicado em dois exemplos de aplicação investigados da literatura.

O primeiro exemplo de aplicação é descrito neste capítulo e trata de um cenário de acidente ocorrido na unidade de isomerização (ISOM) da refinaria da *British Petroleum* (BP), na cidade do Texas nos Estados Unidos. O cenário refere-se ao incêndio seguido de explosão que ocorreu durante a repartida da unidade de ISOM da refinaria e os dados foram obtidos de (BAKOLAS e SALEH, 2011) e (FERDOUS, KHAN, *et al.*, 2013).

O segundo exemplo de aplicação que está descrito no Apêndice D deste trabalho, trata de um cenário de acidente que ocorreu num sistema de carregamento de hidrocarbonetos na forma líquida, em um caminhão tanque. O cenário refere-se ao incêndio e explosão do caminhão tanque e os dados foram obtidos do trabalho de (BADREDDINE e BEN AMOR, 2013).

Os bancos de dados de treinamentos BDT_{AF} e BDT_{AE}, para os dois exemplos de aplicação, consideram dados faltantes ou incompletos, e foram obtidos de forma sistemática realizando-se os procedimentos descritos nos Apêndices A e B. Adicionalmente, os bancos de dados BDT_{AF} e BDT_{AE}, apresentam cada um, 20% (vinte por cento) de dados faltantes. Esta porcentagem foi adotada neste trabalho, com base no resultado do estudo de fiabilidade de construção artificial de modelos de acidentes baseado em duas abordagens probabilísticas: (i) imputação de dados e (ii) aprendizagem de estrutura de redes Bayesianas e que é apresentado com maiores detalhes no Apêndice C.

Nos casos onde a porcentagem de dados faltantes, em bancos de dados de treinamento, for maior que 20%, a fiabilidade dos modelos de acidentes construídos não é garantida. Neste contexto é sugerida a utilização de uma abordagem baseada em restrições, e nesse caso, será necessário incluir o conhecimento de especialistas; uma vez que os modelos serão utilizados para tomadas de decisões na elaboração e implementação de estratégias de prevenção e mitigação de eventos e falhas críticas.

Um dos resultados obtidos com a aplicação do *framework* proposto, são modelos de acidentes obtidos a partir de bancos de dados com dados faltantes

gerados de forma artificial. Os dois modelos de acidentes mostrados nas Figura 58 para o exemplo 1 e Figura 152 para o exemplo 2, foram comparados com os respectivos diagramas de *bowtie* obtidos da literatura, para cada exemplo de aplicação, e os resultados foram positivos, mostrando que os modelos são equivalentes.

Adicionalmente, com a aplicação do *framework*, os seguintes resultados foram obtidos:

(a) Identificação das barreiras de prevenção e mitigação de falhas críticas. Desta forma fica claro como os diagramas de barreiras podem ser usados como ferramenta para a gestão da segurança da planta / processo, conforme previsto em (DUIJM, 2009),

(b) Desenvolvimento de modelos baseados na formalização da rede de Petri, para descrição de cenários críticos, considerando a existência de barreiras de prevenção e mitigação. A técnica PFS permite a modelagem de sistemas segundo uma abordagem hierárquica, com base em refinamentos sucessivos, para construção de modelos funcionais de forma progressiva e estruturada, de tal forma que as propriedades dos modelos obtidos que descrevem o comportamento dinâmico desses sistemas podem ser verificadas e validadas utilizando ferramentas computacionais adequadas(PESSOA, 2015).

(c) Considerando que cada barreira corresponde a uma `atividade` no PFS, composta por uma sequência de `subatividades` que utilizam recursos humanos e físicos, ao refinarmos estas, obtêm-se as informações necessárias para o preenchimento da tabela de HAZOP obedecendo a critérios da norma (IEC 61882, 2003).

(d) Sistematização da integração dos modelos de acidentes com o HAZOP para identificar todos os eventos críticos que precederam a ocorrência do evento topo (ET) e eventos indesejados que sucederam a ocorrência do ET, desta forma, a rastreabilidade dos eventos durante a dinâmica do acidente é incorporada ao HAZOP, permitindo que o princípio de defesa em profundidade e a propriedade de diagnosticabilidade segura sejam considerados no projetos de SCSP.

(e) Modelagem de algoritmos de defesa de prevenção e mitigação de falhas críticas. Os modelos obtidos são consistentes com o princípio de defesa em

profundidade e com a propriedade de diagnosticabilidade segura. As propriedades de vivacidade e segurança podem ser verificadas e os modelos podem ser convertidos de forma isomórfica para programas em linguagem de programação (IEC 61508, 2010) e implementados em dispositivos de realização de controle em SIS.

A fase 3 do *framework*, não substitue a técnica clássica de identificação de riscos (ex: HAZOP), ao contrário, os resultados obtidos a partir dessa etapa deverão ser integrados com as técnicas clássicas; corroborando nas atividades pertinentes à primeira etapa do ciclo de projeto de sistemas de controle relacionados à segurança (IEC 61508, 2010) (IEC 61511, 2003); pois consideram além dos eventos críticos definidos por especialistas – durante a atividade de HAZOP, a relação entre os eventos previamente conhecidos pelos especialistas com os eventos parcialmente observados, tornando o processo de identificação e análise de riscos o mais próximo da realidade.

De forma geral, pode-se concluir a partir da verificação do *framework* com base em dois exemplos de aplicação, que a metodologia proposta atende aos objetivos descritos no início deste trabalho. Entretanto, vale ressaltar que alguns pontos ainda não foram resolvidos:

(a) O *framework* proposto para a síntese do SCSP – via abordagem probabilística, não considera fatores gerenciais e/ou corporativos como causas do ET, sendo estes fatores, de extrema relevância para a ocorrência dos chamados “acidentes patogênicos”.

(b) O estudo de fiabilidade de construção artificial de modelos de acidentes, considerando a natureza dos bancos de dados com dados incompletos, não considerou outros mecanismos de ausência de dados, como por exemplo, MAR e NMAR.

(c) O estudo de fiabilidade de construção artificial de modelos de acidentes, considerando técnicas de imputação de dados, não considerou a técnica de aprendizagem de parâmetros das redes Bayesianas, sendo esta abordagem fundamental para a análise quantitativa de riscos.

(d) O *framework* proposto não aborda a questão de gestão e manutenabilidade das barreiras de segurança, sendo esta questão fundamental para se garantir níveis de segurança definidos na concepção de SCSP.

5 CONCLUSÕES

Este trabalho apresenta uma metodologia para o projeto de sistemas de controle baseados no conceito de segurança funcional nas indústrias de processos, definindo sua arquitetura de controle, uma extensão da classificação de barreiras de segurança com foco no uso de barreiras reativas, e um *framework* para a síntese do SCSP baseado em modelos de acidentes que descrevem a evolução de eventos críticos “observados” e “parcialmente observados”.

A arquitetura do SCSP endereça:

(i) o conceito de sistema seguro(HOLLNAGEL, 2007) integrando as abordagens de prevenção e mitigação de eventos iniciadores, críticos e/ou indesejados;

(ii) a aderência às normas de segurança (IEC 61508, 2010) e (IEC 61511, 2003);

(iii) a aderência ao princípio de defesa em profundidade, permitindo que mecanismos de defesa de prevenção e mitigação sejam definidos e executados por módulos de controle do SCSP. Os mecanismos de defesa de prevenção e mitigação considerados neste trabalho, são baseados num novo sistema de barreiras denominadas de reativas, e que consideram a substituição da atuação humana pela tecnologia (SIS), tendo cada barreira, autonomia suficiente para realizar as funções de segurança (ex: detecção, diagnóstico e ação), contra os eventos iniciadores, críticos e/ou indesejados; e

(iv) a aderência à propriedade de diagnosticabilidade segura, pois considera os dispositivos de sensoriamento para cada módulo de controle (ex: prevenção, mitigação e supervisão) do SCSP, assim como, dispositivos de sensoriamento do SCBP; necessários à detecção e diagnóstico de todos os eventos iniciadores, críticos e/ou indesejados que são identificados, usando a abordagem de modelos de acidentes.

O *framework* para a síntese do SCSP, endereça:

(i) sistemática para a elaboração da Tabela de HAZOP a partir da elicitação de especialistas,

(ii) descrição de processos de evolução de eventos críticos e/ou indesejados, a partir de modelos de acidentes obtidos via bancos de dados incompletos ou

com dados faltantes, permitindo a rastreabilidade e diagnosticabilidade de todos os eventos iniciadores e críticos precedentes à falha crítica, assim como, todos os eventos e consequências indesejadas após a ocorrência da falha crítica, se os mecanismos de defesa de prevenção falharem. A descrição de processos de evolução destes eventos é aderente à propriedade de diagnosticabilidade segura; e

(iii) integração de modelos de acidentes gerados, com as técnicas clássicas de identificação e análise de riscos (ex. HAZOP). As técnicas usadas para gerar este *framework* foram: (a) imputação de dados, (b) aprendizagem de estruturas de redes Bayesianas, (c) método de *bowtie*, e (d) PFS para a sistematização dos métodos propostos, e para a representação em alto nível de cenários de acidentes, utilizados para a descrição de atividades e recursos a serem consideradas no estudo de HAZOP, e

(iv) a modelagem, verificação e validação de algoritmos de defesa para a prevenção e mitigação de falhas críticas (ET), dado um cenário crítico. Os algoritmos desenvolvidos podem posteriormente ser convertidos para programas de controle de segurança em qualquer linguagem de programação prescrita pela IEC61131-3 em consonância com a IEC61508/IEC61511.

As ferramentas como *Hugin Educational*®, *UnBBayes*, MICE e plataforma computacional R, também são consideradas para análise, implementação e validação do método.

A solução proposta:

(i) trata a questão de acidentes patogênicos(BAKOLAS e SALEH, 2011), que de acordo com a análise de relatórios de investigação de acidentes, apontam para eventos críticos e/ou indesejáveis não observados ou ocultos, durante o processo de evolução destes eventos;

(ii) propõe uma mudança de paradigma no desenvolvimento de requisitos para projetos de sistemas de controle relacionados à segurança, pois considera em seus requisitos, modelos de acidentes que descrevem de forma estruturada o processo de evolução de eventos críticos e/ou indesejados, estando em consonância com a propriedade de diagnosticabilidade segura(PAOLI e LAFORTUNE, 2005);

(iii) propõe um novo método para modelagem de acidentes utilizando a técnica de *bowtie*. O método utiliza abordagem probabilística e considera bancos de dados reais encontrados nas indústrias de processos. Estes bancos de dados são incompletos, ou com dados faltantes(LAKSHMINARAYAN, HARP e SAMAD, 1999); que neste trabalho, endereçam eventos iniciadores, críticos e/ou indesejados parcialmente observados, durante o processo de evolução destes eventos. Adicionalmente, no Apêndice C deste relatório, é apresentada uma síntese do estudo de fiabilidade de modelos de acidentes aprendidos via imputação múltipla de dados e abordagem bayesiana, considerando bancos de dados incompletos ou com dados faltantes. Os resultados pertinentes a este estudo podem ser encontrados no próprio apêndice.

(iv) um modelo que descreve o acidente, dado um risco (ex: falha crítica), permitindo identificar, de forma bem definida, as barreiras de prevenção e mitigação dos eventos críticos/indesejados, a partir de um formalismo denominado diagrama de barreiras(DUIJM, 2009). Estes diagramas podem ser utilizados como ferramentas para a gestão da segurança dos mecanismos de defesas da planta/processo e que são aderentes ao ciclo de vida de projetos de sistemas relacionados à segurança(IEC 61508, 2010)(IEC 61511, 2003).

(v) um método para modelagem dos algoritmos de defesa de prevenção e mitigação de falhas críticas, dado um determinado cenário crítico, usando a metodologia PFS/MFG (ver Anexo A).

(vi) O uso do formalismo de diagramas de barreiras, permitiu desenhar um processo de degeneração que será tratado localmente, por cada mecanismo de defesa (ex: barreira de prevenção/mitigação); diminuindo o dano do processo todo. Espera-se que com este processo de degeneração controlada, os danos do processo sejam minimizados, abreviando o período necessário para a regeneração de cada parte do processo/planta.

5.1 TRABALHOS FUTUROS

(a) Uma sistemática para integração de modelos de acidentes obtidos artificialmente, com causas de natureza gerencial e/ou organizacional – obtidos a partir de relatórios de acidentes, permitindo integrar o sistema de barreiras reativas, propostas neste trabalho, com outros sistemas de barreiras propostos por Sklet (2006), convergindo para a uma arquitetura de colaboração considerando diferentes sistemas de barreiras, concebendo sistemas de segurança mais eficazes.

(b) Estender o estudo de fiabilidade de construção artificial de modelos de acidentes, considerando a natureza intrínseca de bancos de dados com dados incompletos, a partir de outros mecanismos de ausência de dados, como por exemplo, MAR e NMAR.

(c) Estender o estudo de fiabilidade de construção artificial de modelos de acidentes, via técnicas de imputação de dados, considerando as técnicas de aprendizagem de parâmetros de redes Bayesianas, permitindo a realização de análises quantitativas de riscos a partir de bancos de dados incompletos.

(d) Elaborar uma sistemática para a gestão e manutenabilidade da segurança funcional a partir dos diagramas de barreiras de segurança gerados, a fim de garantir níveis de segurança pertinentes e que foram definidos na concepção de SCSP.

(e) Dado o processo de degeneração local, representado via diagrama de barreiras e modelo PFS correspondente, elaborar uma sistemática para: (i) avaliar qualitativamente os riscos a partir do conhecimento da quantidade de energia despendida no processo de degeneração controlada, e (ii) medir a quantidade de energia necessária para regenerar cada parte da planta/processo, como ferramenta para a gestão e manutenabilidade do SCSP. Uma possibilidade a ser investigada seria a aplicação de diagrama *bonds-graph* neste contexto de problema.

REFERÊNCIAS BIBLIOGRÁFICAS

ANDERSEN, H.; CASAL, J.; DANDRIEUX, A.; DEBRAY, B.; DE DIANOUS, V.; DUIJM, N.J. **ARAMIS - user guide**. [S.l.]. 2004. (EVG1-CT-2001-0036).

ARAKAKI, J.; MIYAGI, P.E.; VILLANI, E.; BASTIDAS-GUSTIN, G.D; MIYAGI, M.M.; KISIL, M. **Integração de Atividades e Serviços em Edificios Inteligentes - Aplicação da Metodologia PFS/MFG**. In: ENEGEP XVIII Encontro Nacional de Engenharia de Produção. Niterói, R.J.: ABEPRO. 1998. p. CD-ROM.

BADREDDINE, A.; BEN AMOR, N. A Bayesian approach to construct bow tie diagrams for risk evaluation. **Process Safety an Environmental Protection**, v. 91, p. 159-171, 2013.

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.

BOBBIO, A; PORTINALE, L.; MINICHINO, M.; E.CIANCAMERLA. **Improving the analysis of dependable systems by mapping fault trees into Bayesian networks**. Reliability Engineering and System Safety. Rome, Italy: [s.n.]. 2001. p. 249-260.

BRAUER, W.; REISIG, W. **Carl Adam Petri and "petri nets"**. Informatik-Spektrum. [S.l.]: v.29, n.5. 2006. p. 369-374.

BUUREN, S. V.; OUDSHOORN, K. G. MICE: Multivariate Imputation by Chained Equations in R. **Journal of Statistical Software**, v. 45, n. Issue 3, p. 1-67, 2011.

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.

CARDOSO, J.; VALETTE, R. **Redes de Petri**. CDU 681.31:519.1. ed. Florianópolis - SC: UFSC, 1997.

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).

CASTILHO, E.; GUTIÉRREZ, J.; HADI, A. **Expert Systems and Probabilistic Network Models**. New York: Springer, 1997.

CAVALHEIRO, A. C. M. **Sistema de controle para diagnóstico e tratamento de falhas em dispositivos de assistência ventricular**. Tese de Doutorado - Escola Politécnica da Universidade de São Paulo. São Paulo. 2013.

CHOW, C.; LIU, C. **Approximating discrete probability distributions with dependence trees**. IEEE Transactions on Information Theory. [S.l.]: [s.n.]. 1968. p. 462-467.

COCKSHOTT, J. E. Probability bow-ties a transparent risk management tool. **Process Saf. Environ. Protect.**, n. 83, p. 307-316, 2005.

DALY, R.; SHEN, Q.; AITKEN, S. Learning Bayesian networks: approaches and issues. **The Knowledge Engineering Review**, v. 26:2, n. Cambridge University Press, p. 99-157, 2011. ISSN doi: 10.1017/S0269888910000251.

DARWICHE, A. What are Bayesian networks and why are their applications growing across all fields? **Communications of the ACM**, v. 53, p. 80-90, 2010.

DELVOSALLE, C. et al. ARAMIS project: a comprehensive methodology for the identification of reference accident scenarios in process industries. **J. Hazard Mater**, n. 130, p. 200-219, 2006.

DIANOUS, V.; FIEVEZ, C. ARAMIS project: a more explicit demonstration of risk control through the use of bow-tie diagrams and the evaluation of safety barrier performance. **J. Hazard Mater**, n. 130, p. 220-223, 2006.

DUIJM, N. J. Safety-barrier diagram as a safety management tool. **Reliability Engineering and System Safety**, Roskilde, Denmark, 2009. 332-341.

DUIJM, N. J. et al. **Evaluating and managing safety barriers in major hazard plants**. Berlin, Germany. 2004.

ENDERS, C. K. **Applied Missing Data Analysis**. New York: Guilford Press, v. 72, 2010.

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.

FERDOUS, R. et al. Analyzing system safety and risks under uncertainty using a bow-tie diagram: An innovative approach. **Process Safety and Environmental Protection**, v. 9I, p. 1-18, 2013.

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.

FERRAREZI, R. C. et al. **Framework para o Desenvolvimento de Programas de Controles de SIS baseado na norma IEC 61511**. Congresso Nacional de Matemática Aplicada à Indústria - CNMAI. [S.l.]: [s.n.]. 2014b.

FLOREA, G.; DOBRESCU, R. Risk and Hazard Control the new process control paradigm. **Communications, Circuits and Educational Technologies**, v. ISBN: 978-1-61804-231-6, p. 141-149, 2011.

FRIEDMAN, N. **Learning Belief Networks in the Presence of Missing Values and Hidden Variables**. Proceedings of the Fourteenth International Conference on Machine Learning. San Francisco - USA: [s.n.]. 1997. p. 125-133.

FRIEDMAN, N. **The Bayesian Structural EM algorithm**. In Proceedings of the Fourteenth Conference on Uncertainty in Artificial Intelligence. UAI-98: [s.n.]. 1998. p. 129-138.

GROOSSENS, L.; HOURTOLOU, D. **What is a barrier?** ARAMIS-working document. [S.l.]. 2003.

GROOVER, M. **Automação Industrial e Sistemas de Manufatura**. 3ª Edição. ed. São Paulo: Pearson Education do Brasil, 2011. ISBN ISBN 978-85-7605-871-7.

HADDON, W. J. The basic strategies for reducing damage from hazards of all kinds. **Hazard Prevention**, September-October 1990. 8-12.

HALE, A. **Note on barriers and delivery systems**. In PRISM conference. Athens: [s.n.]. 2003.

HARARY, F. **Graph theory**. 281p. ed. Massachusetts - United States: Addison-Wesley Publishing Company. Inc., 1969.

HARREL JR, F. E. **Regression modeling strategies with applications to linear models, logistic regression and survival analysis**. New York: Springer - Verlag, 2001.

HENLEY, F.; KUMAMOTO, H. **Reliability Engineering and Risk Assessment**. Englewood Cliffs, NJ: Prentice Hall, 1981.

HOEPFER, V. M.; SALEH, J. H.; MARAIS, K. B. On the value of redundancy subject to common-cause failures: toward the resolution of an on-going debate. **Reliability Engineering & System Safety**, v. 94, p. 1904-1916, Dezembro 2009. ISSN DOI 10.1016.

HOLAND, P. **Offshore blowouts:** Causes and control. Houston: Gulf Publ. Co., 1997.

HOLLNAGEL, E. **Barrier and accident prevention**. Ashgate, UK: Hampshire, 2004.

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

HORTON, N. J.; LIPSITZ, S. R. Multiple Imputation in Practice: Comparison of Software Packages for Regression Models with Missing Variables. **The American Statistician**, v. 55, n. 3, p. 244-254, 2001.

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

IEC 61508. **Functional Safety of Electrical/Electronic/Programmable electronic Safety-related Systems**. [S.l.]: [s.n.], 2010.

IEC 61511. **Functional Safety - Safety Instrumented Systems for the Process Industry**. [S.l.]: [s.n.], 2003.

IEC 61882. **HAZARD AND OPERABILITY STUDIES (HAZOP studies):** application guide. London: [s.n.], 2003.

INSTITUTE of Industrial & Systems Engineers, 2016. Disponivel em: <http://www.iienet2.org/details.aspx?id=282>. Acesso em: 28 ago. 2016.

ISA-S5.1-1984. **Instrumentation Symbols and Identification**. Instrument Society of America. North Carolina. 2009.

JENSEN, K. **Coloured Petri Nets:** Basic Concepts, Analysis Methods and Practical Use. Berlin: [s.n.]. 1992.

JUNQUEIRA, F.; MIYAGI, P. E. **A new method for the hierarchical modelling of productive systems**. Information Technology for Balanced Manufacturing Systems. [S.l.]: Springer. 2006. p. 479-488.

KANESHIRO, P. J. E. A. **Modeling of collision resolution algorithm in Lonworks networks**. Proceedings of ASME International Mechanical Engineering Congress and Exposition. [S.l.]: v.9. 2008. p. 743-749.

KECKLUND, L.J.; EDLAND, A.; WEDIN, P.; SVENSON, O. Safety barrier function analysis in a process industry: A nuclear power application. **International Journal of Industrial Ergonomics**, 1996. 275-284.

KHAKZAD, N.; KHAN, F.; AMYOTTE, P. **Safety analysis in process facilities:** Comparison of fault tree and network approaches. Reliability Engineering and System Safety. [S.l.]: [s.n.]. 2011. p. 925-932.

KJELLÉN, U. **Prevention of accidents through experience feedback**. [S.l.]: Taylor & Francis, 2000.

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.

LAKSHMINARAYAN, K.; HARP, S. A.; SAMAD, T. **Imputation of Missing Data in Industrial Databases**. pp. 259-275. ed. Netherlands: Kluwer Academic Publishers, v. 11, 1999.

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.

MADSEN, A. L. et al. **The Hugin Tool for Learning Bayesian Networks**. ECSQARU 2003, LNAI 2711. Berlin Heidelberg: Springer-Verlag. 2003. p. pp. 594-605.

MARKOWSKI, A. S.; MANNAN, M. S.; BIGOSZEWKA, A. Fuzzy logic for process safety analysis. **J. Loss Prev. Process Ind.** , v. 22, p. 695-702, 2009.

MAZZOLINI, M.; BRUSAFERRI, A.; 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.

MIYAGI, P. E. **Controle Programável:** Fundamentos de Controle de Sistemas a Eventos Discretos. 3ª Edição. ed. São Paulo: Blucher, 2007.

MORALES, R. A. G.; MELO, J. I. G.; MIYAGI, P. E. Diagnosis and Treatment of Faults in Productive Systems based on Bayesian Networks and Petri Net. **IEEE International Conference onAutomation Science and Engineering**, p. 357 - 362, 2007.

MURATA, T. Petri nets: Properties, analysis and applications. **Proceedings of IEEE**, v. 77, n. 4, p. 541–580, 1989.

NIVOLIANITOU, Z. S.; LEOPOULOS, V. N.; KONSTANTINIDOU, M. Comparison of techniques for accident scenario analysis in hazardous systems. **J. Loss Prevent. Process Ind.**, n. 17, p. 467-475, 2004.

NUNES, L. N. **Métodos de Imputação de dados aplicados na Área de Saúde**. Universidade Federal do Rio Grande do Sul. Porto Alegre, p. 120. 2007.

NUNES, L. N.; KLUCK, M. M.; FACHEL, J. M. G. Uso da imputação múltipla de dados faltantes: uma simulação utilizando dados epidemiológicos. **Cad. Saúde Pública**, Rio de Janeiro, v. 25, n. 2, p. 268-278, fev. 2009.

OCHOA LUNA, J. E. **Algoritmos EM para Aprendizagem de Redes Bayesianas a partir de Dados Incompletos**. Universidade Federal de Mato Grosso do Sul. [S.l.], p. 120. 2004.

OCHOA-LUNA, J. E.; ZANUSSO, M. B. **Revisited EM algorithms for Learning Bayesian Networks from Incomplete Data**. EEUU - Proceeding of the International MultiConference in Computer Science and Computer Engineering. Las Vegas - USA: [s.n.]. 2005. p. p.498.

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.

PERROW, C. **Normal accidents:** living with high-risk tecnologies. New York: Basic Books, 1984.

PESSOA, M. A. O. **Arquitetura de Sistema de Planejamento e Controle da Produção no contexto de Empresa Virtual**. Escola Politécnica da Universidade de São Paulo. São Paulo, p. 172. 2015.

PETERSON, J. L. **Petri Net Theory and the Modeling of Systems**. New Jersey: Prentice Hall Inc., 1981.

RATHNAYAKA, S.; KHAN, F.; AMYOTTE, P. SHIPP methodology: Predictive accident modeling approach. Part I: Methodology and model description. **Process Safety and Environmental Protection**, n. 89, p. 151-164, 2011.

RAUSAND, M.; HOYLAND, A. **System reliability theory:** Models, statistical methods, and applications. Hoboken: Wiley-Interscience, 2004.

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

REASON, J.; PARKER, D.; LAWTON, R. Organizational controls and safety: The varieties of rule-related behaviour. **Journal of Occupational and Organizational Psychology**, 1998. 289-304.

REISIG, W. **Petri nets:** an introduction. New York: Springer Verlag, 1985.

RIASCOS, L. A. M. **Metodologia para Detecção e Tratamento de Falhas em Sistemas de Manufatura através de rede de Petri**. Tese de Doutorado, Escola Politécnica da Universidade de São Paulo. São Paulo. 2002.

RIASCOS, L. A. M.; SIMOES, M. G.; MIYAGI, P. E. A Bayesian network fault diagnostic system for proton exchange membrane fuel cells. **Journal of Power Sources**, v. 165, n. 1, p. 267–278, 2007.

ROCHLIN, G. I.; LA PORTE, T. R.; ROBERTS, K. H. **The self-designing high reliability organization**. Naval War College. [S.l.]. 1998. (51(3):17).

ROUVROYE, J. L.; VAN DEN BLIEK, E. G. **Comparing safety analysis techniques.** Reliability Engineering and System Safety. [S.l.]: [s.n.]. 2002. p. 289-294.

RU, Y.; HADJICOSTIS, C. N. Fault diagnosis in discrete event systems modeled by Petri nets with outputs. **9th International Workshop on Discrete Event Systems**, Göteborg, p. 443-448, 2008.

RUBIN, D. B. **Inference and Missing Data**. Biometrika. [S.l.]: [s.n.]. 1976. p. 581-590.

RUBIN, D. B. **Multiple Imputation for Nonresponse in Surveys**. New York: John Wiley & Sons. 1987.

RUIJTER, A.; GULDENMUND, F. The bowtie method: A review. **Safety Science**, n. 88, p. 211-218, 18 March 2016.

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**, 2010. 1105-1116.

SAMPATH, M. et al. **Diagnosability of discrete-event systems**. IEEE Trans. on Automatic Control. [S.l.]: [s.n.]. 1995. p. 1555-1575.

SCHAFER, J. L.; GRAHAM, J. W. **Missing data:** Our view of the state of the art. Psychologial Methods. [S.l.]: [s.n.]. 2002. p. 147-177.

SCHUPP, B. **The safety modeling language. Advises tutorial in human error analisys, barriers and the safety modelling language**. Paderborn, Germany. 2004.

SILVA, M. K. C. D. **Imputação múltipla: comparação e eficiência em experimentos multiambientais**. Universidade de São Paulo - Escola Superior de Agricultura "Luiz de Queiroz". Piracicaba, p. 122. 2012.

SINGH, M. **Learning Bayesian Networks for Solving Real-World Problems**. PhD Thesys presented to the Faculties of the University of Pennsylvania. Pennsylvania - USA: [s.n.]. 1998. p. pp. 1-183.

SKLET, S. Comparison of some selected methods for accident investigation. **Journal of Hazardous Materials**, Trondheim, Norway, 13 April 2004. 29-37.

SKLET, S. Safety barriers: Definition, classification, and performance. **Journal of Loss Prevention in the Process Industries**, Trondheim, Norway, September 2006. 494-506.

SKLET, S. Safety barriers: Definition, classification, and performance. **Journal of Loss Prevention in the Process Industries**, Trondheim, Norway, September 2006. 494-506.

SQUILLANTE JR, R. **Diagnóstico e Tratamento de Falhas Críticas em Sistemas Instrumentados de Segurança**. Escola Politécnica da Universidade de São Paulo. São Paulo, p. 1-158. 2011.

SQUILLANTE JR, R. et al. Safety in Supervisory Control for Critical Systems. **IFIP International Federation for Information Processing (DoCEIS 2013)**, v. 394, p. 261-270, 2013.

SQUILLANTE JR, R. et al. **A Novel Safety Control Hierarchical Architecture for Prevention and Mitigation of Critical Faults in Process Industries based on Defense-in-depth, Reactive Systems and Safety-Diagnosability**. 15th IFAC Symposium on Information Control Problems in Manufacturing. Ottawa, Canada: [s.n.]. 2015. p. 1326-1331.

SUMMERS, A. E. Introduction to layers of protection analisys. **Journal of Hazard Materials**, 2003. 163-168.

TEAM, R. C. **R: A Language and Environment for Statistical Computing**. R Foundation for Statistical Computing. Vienna, Austria. 2016.

WAHLSTROM, B.; GUNSELL, L. **Reactor safety: a description and assessment of the Nordic safety work**. Riso forskningscenter. 1998.

WEBER, P. et al. **Overview on Bayesian networks applications for dependability, risk analisys and maintenance areas**. Engineering Applications of Artificial Intelligence. [S.l.]: Elsevier. 2012. p. 671-682.

ZHANG, P. Multiple imputation: Theory and method. **International Statistical Review**, v. 71, n. 3, p. 581-592, 2003.

ZURAWSKI, R.; ZHOU , M. **Petri nets and industrial applications:** a tutorial. IEEE Trans. on Industrial Eletronics. [S.l.]: [s.n.]. 1994. p. 567–583.

ANEXO A – METODOLOGIA PFS/MFG

Neste anexo, são apresentados os fundamentos da técnica de modelagem de sistemas discretos *Mark Flow Graph* (MFG) e os fundamentos da metodologia PFS/MFG.

A.1 FUNDAMENTOS DO MFG

O *Mark Flow Graph* (MFG) (MIYAGI, 2007) é uma rede interpretada(PETERSON, 1981) derivada das redes de Petri, desenvolvida para a modelagem e controle de SEDs. O MFG é composto basicamente pelos seguintes elementos estruturais ilustrados na Figura 133:

a) a `transição` que indica a ocorrência de eventos;

b) o `box` que representa as pré e pós-condições;

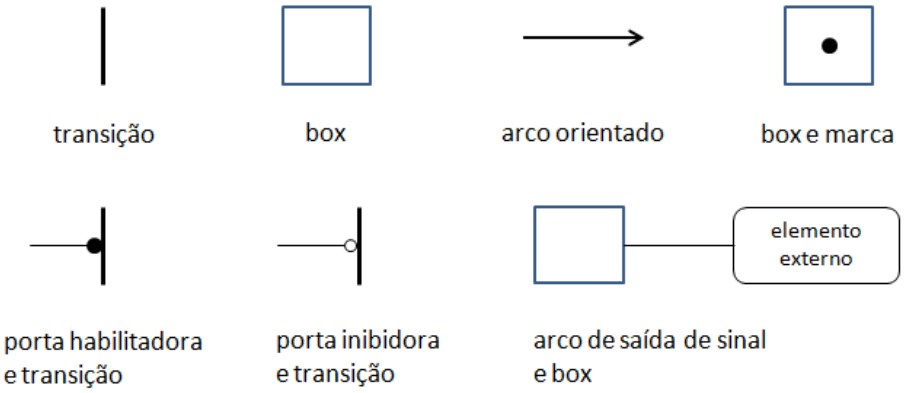
c) o `arco` orientado que estabelece uma relação causal entre o evento e a condição;

d) a `marca` que indica a manutenção de uma condição;

e) as `portas` que habilitam ou inibem a ocorrência dos eventos;

f) `arco` de sinal de saída que envia um sinal binário do `box` para os dispositivos externos do grafo, e é representado por uma linha que conecta estes dois elementos. Quando houver uma `marca` neste `box`, o sinal é “1”; quando não houver, é “0”.

Figura 133 – Elementos básicos do MFG



Fonte: (MIYAGI, 2007)

No processo de modelagem, os `boxes` representam as condições, estados ou operações associadas aos dispositivos, e as `transições` representam à mudança

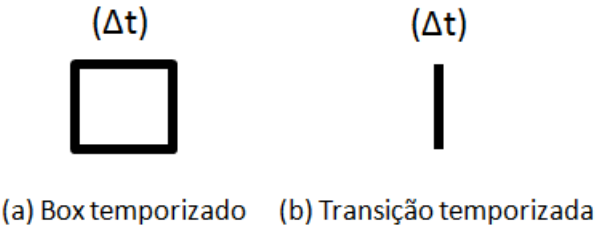
dos estados. O comportamento dinâmico do sistema que está sendo modelado, é indicado pela evolução das `marcas` no grafo, de acordo com uma regra predefinida de disparo das `transições` e que correspondem ao fluxo de informações no sistema real.

Para representar a interface do modelo do sistema com os dispositivos externos (ex: sensores, atuadores) do sistema real, existem dois elementos estruturais: os `arcos` de sinal de saída e as `portas` habilitadoras / inibidoras. No caso das `portas`, ainda há uma classificação em `portas` externas ou internas, dependendo da natureza do sinal de origem.

Quando o conceito de tempo é considerado na manutenção de estados e na ocorrência de eventos, como no caso de muitos sistemas reais, os seguintes elementos são introduzidos no MFG:

- `Box` *temporizado*: quando uma `marca` aparece neste tipo de `box`, a `transição` conectada em sua saída fica disparável somente após decorrido um intervalo de tempo (Δt), vide Figura 134a.
- `Transição` *temporizada*: uma vez que todas as condições de disparo estejam satisfeitas, esta `transição` só dispara após decorrido um intervalo de tempo (Δt), vide Figura 134b. Se durante este tempo, uma das condições deixa de ser satisfeita, a contagem do tempo é anulada. Será reiniciada somente após todas as condições estarem novamente satisfeitas.

Figura 134 – MFG com conceito de tempo



Fonte: (MIYAGI, 2007)

A.2 FUNDAMENTOS DA METODOLOGIA PFS/MFG

A metodologia PFS/MFG consiste na representação de um modelo conceitual do sistema, via grafos *Production Flow Schema* (PFS), e o seu detalhamento por meio dos grafos MFG(ARAKAKI, J.; MIYAGI, P.E.; VILLANI, E.; BASTIDAS-GUSTIN, G.D; MIYAGI, M.M.; KISIL, M., 1998). Todos os elementos que podem ser utilizados para

a criação de um modelo PFS já foram ilustrados na Figura 23, sendo eles: (a) `atividade`, representada pelo bloco com colchetes e com indicação de um nome descritivo desta atividade; (b) elemento `distribuidor` representado pela circunferência, e; (c) `arco` (fluxo de materiais e/ou informações) representado pela seta entre um elemento `distribuidor` e uma `atividade` ou entre uma `atividade` e um elemento `distribuidor`.

De acordo com a metodologia, os elementos do grafo PFS são então detalhados. Este detalhamento pode gerar subgrafos totalmente em PFS, ou subgrafos em MFG ou subgrafos híbridos (PFS/MFG) com alguns elementos em PFS e outros em MFG (vide Figura 135)(ARAKAKI, J.; MIYAGI, P.E.; VILLANI, E.; BASTIDAS-GUSTIN, G.D; MIYAGI, M.M.; KISIL, M., 1998).

O detalhamento para a implementação prática de sinais com o meio externo (atuadores, sensores, dispositivos de monitoração ou de comando) é necessariamente via grafos MFG.

De uma forma sistemática a metodologia consiste nos seguintes passos:

Passo 1 – Defina um modelo PFS para cada processo a ser modelado.

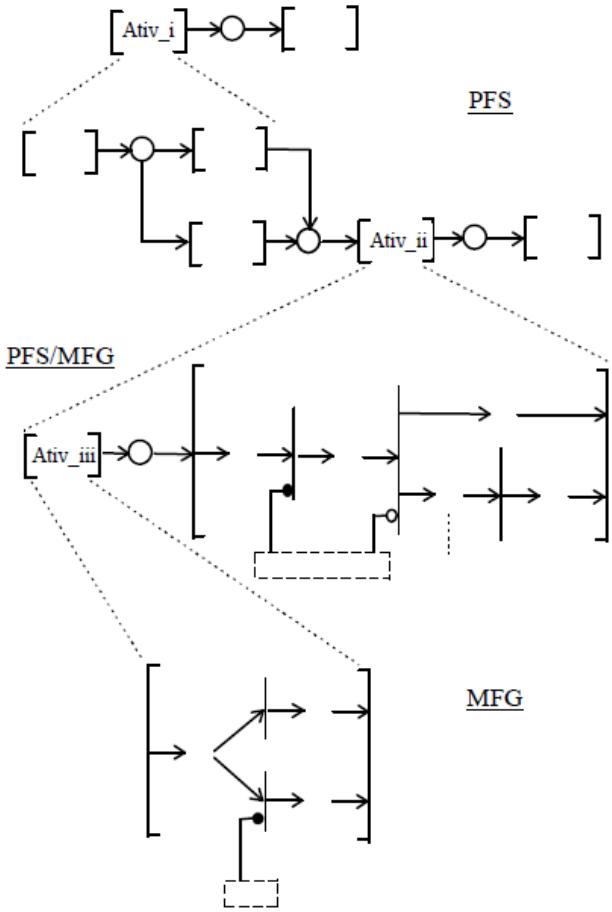
Passo 2 – Refine o processo por meio de um conjunto de `atividades` associadas às funções que necessitam serem realizadas.

Passo 3 – Refine cada função em um conjunto de `subatividades` de acordo com as operações pertinentes.

Passo 4 – Represente os recursos necessários para execução das `atividades`.

Passo 5 – Estabeleça a comunicação com os elementos externos por meio de `arcos` de sinal de saída e `portas` externas habilitadoras e inibidoras que se comunicam com os elementos finais do sistema de controle.

Figura 135 – Exemplo de um grafo PFS/MFG

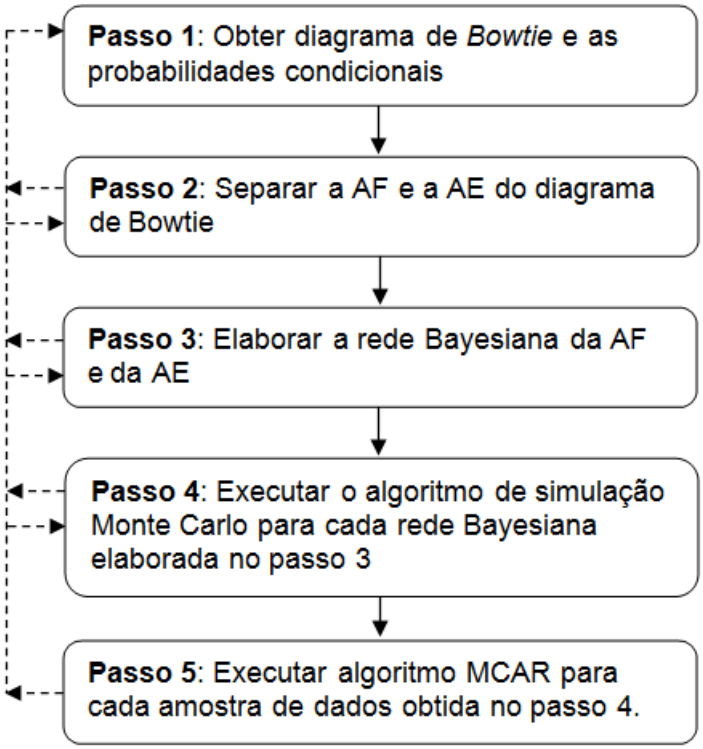


Fonte: (ARAKAKI, J.; MIYAGI, P.E.; VILLANI, E.; BASTIDAS-GUSTIN, G.D; MIYAGI, M.M.; KISIL, M., 1998)

APÊNDICE A – ELABORAÇÃO DE BANCOS DE DADOS BDTAF E BDTAE

Neste apêndice é proposto um procedimento probabilístico para obtenção dos bancos de dados de treinamentos BDT_{AF} e BDT_{AE} a partir dos diagramas de *bowtie*. Estes bancos de dados são utilizados nos exemplos de aplicação 1 e 2. Os bancos de dados BDT_{AF} e BDT_{AE}, possuem cada um, 20% de dados faltantes; endereçando os eventos críticos e/ou indesejados parcialmente observados. A Figura 136 mostra o procedimento.

Figura 136 – Procedimento para obtenção dos bancos de dados de treinamentos BDTAF e BDTAE



Fonte: próprio autor

No passo 1, obteve-se o diagrama de *bowtie* e o conjunto de probabilidades condicionais entre os nós do diagrama, a partir dos trabalhos de(FERDOUS, KHAN, *et al.*, 2013) para o exemplo de aplicação 1 e (BADREDDINE e BEN AMOR, 2013) para o exemplo de aplicação 2.

No passo 2, os diagramas de árvore de falha (AF) e árvore de eventos (AE), contidos no diagrama de *Bowtie*, foram separados.

No passo 3, elaborou-se as redes bayesianas da AF e da AE, com base nos diagramas de AF e AE e nas probabilidades condicionais entre os nós dos mesmos. A elaboração das redes bayesianas foi realizada por meio da ferramenta

computacional *Hugin Educational*®. Cada rede Bayesiana foi salva como um arquivo com extensão (.net) que é compatível com a ferramenta *UnBBayes.*

No passo 4, executou-se o algoritmo de simulação Monte Carlo (recurso disponível da ferramenta *UnBBayes*) para gerar amostras aleatórias de dados, baseadas na probabilidade conjunta das redes bayesianas. O algoritmo foi executado duas vezes, sendo que, na primeira vez foram consideradas como entrada de dados, a rede bayesiana da AF, e na segunda vez, a rede bayesiana da AE. Desta forma, foram obtidas duas amostras de dados aleatórios com dados completos; uma para cada rede bayesiana. A primeira amostra contém dados referentes às "causas" do ET e a segunda amostra contém dados referentes às "consequências" decorrentes do ET. A ferramenta computacional *UnBBayes*[20]- versão 4.21.15 foi utilizada para executar o algoritmo de simulação de Monte Carlo[21]. Antes de executar o algoritmo, os arquivos (.net) gerados no passo 3, foram importados para a ferramenta *UnBBayes,* permitindo desta forma, a execução do algoritmo de simulação.

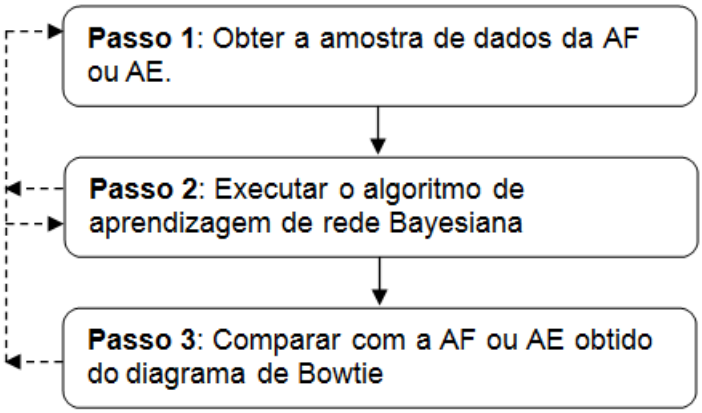
Finalmente no passo 5, foi aplicado o mecanismo de ausência de dados MCAR, para geração de dados faltantes de forma completamente aleatória, obtendo-se os bancos de dados de treinamento do diagrama de AF (BDT_{AF}) e do diagrama de AE (BDT_{AE}). O mecanismo foi implementado por meio de uma aplicação em *Visual Basic* (VBA) desenvolvida na ferramenta *Excel*® usando a função de aleatoriedade. A quantidade de dados faltantes é parametrizada na própria aplicação VBA. No Apêndice B são apresentados os algoritmos e as aplicações em VBA que foram desenvolvidos para gerar os dados faltantes de forma completamente aleatória usando o mecanismo MCAR; dadas as amostras de dados com dados completos, geradas artificialmente por meio da simulação de Monte Carlo.

A fim de validar se cada amostra de dados, obtida pelo passo 4 do procedimento proposto (Figura 136), é consistente com as redes bayesianas elaboradas no passo 3 do mesmo procedimento, é necessário proceder à validação das mesmas. A Figura 137 mostra os passos deste procedimento.

[20] https://sourceforge.net/projects/unbbayes/

[21] Em particular, todos os arquivos de código fonte referentes à funcionalidade Monte Carlo, estão presentes no seguinte diretório para consulta e download: https://sourceforge.net/p/unbbayes/code/HEAD/tree/trunk/UnBBayes/src/main/java/unbbayes/simulation/montecarlo/sampling/

Figura 137 – Procedimento para validação das amostras obtidas por simulação Monte Carlo



Fonte: próprio autor

No passo 1, cada amostra de dados (ex: amostra de dados da AF ou da AE) obtida, deve ser salva como um arquivo de texto (.txt).

No passo 2, utilizar cada amostra como entrada de dados para a execução do algoritmo de aprendizagem de estrutura bayesiana. Como resultado, obter-se-á a estrutura da rede bayesiana da amostra. O algoritmo de aprendizagem de estrutura bayesiana selecionado é o proposto por *Chow* e *Liu* (CHOW e LIU, 1968). A ferramenta usada para a execução do algoritmo de *Chow* e *Liu* foi a ferramenta *Hugin Educational*®.

Finalmente, o passo 3 orienta a comparação das redes bayesianas obtidas a partir do passo 2, com os diagramas de AF e AE obtidos do diagrama de *bowtie* original e usado como referência. Para os dois exemplos de aplicação do Capítulo 4, observou-se que para cada amostra obtida por simulação de Monte Carlo, a rede bayesiana aprendida foi semelhante, validando desta forma o procedimento proposto para geração aleatória de dados por simulação de Monte Carlo.

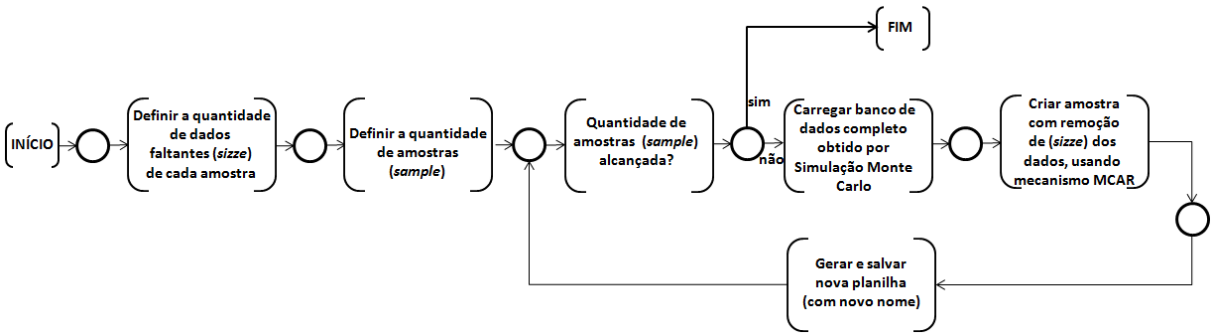
APÊNDICE B – ALGORITMO DE REMOÇÃO COMPLETAMENTE ALEATÓRIA DE DADOS (MCAR) DE BANCOS DE DADOS BDTAE E BDTAF

Neste apêndice são apresentados, o algoritmo e as aplicações que foram desenvolvidas para gerar os dados faltantes de forma completamente aleatória, usando o mecanismo *Missing Completely at Random* (MCAR). O algoritmo foi implementado por meio de uma aplicação em *Visual Basic* (VBA) desenvolvida usando a ferramenta *Excel*®. As amostras de dados utilizadas como entradas nos algoritmos foram geradas artificialmente por meio da simulação Monte Carlo.

O algoritmo é constituído por quatro partes: (1) rotina principal, (2) subrotina carregar dados, (3) subrotina criar amostra de dados com dados faltantes, e (4) sub-rotina salvar planilha com amostra de dados.

A Figura 138 mostra o algoritmo da parte (1) “rotina principal”, em PFS.

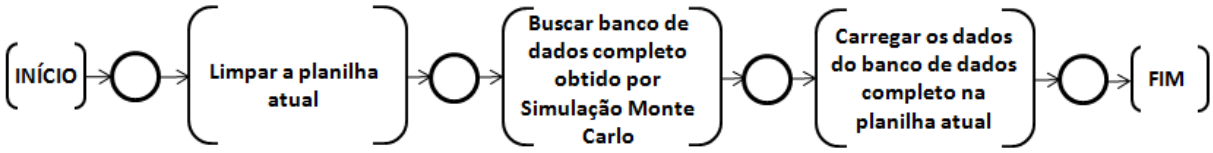
Figura 138 – Algoritmo da rotina principal em PFS



Fonte: próprio autor

A Figura 139 mostra o algoritmo da parte (2) subrotina “carregar dados”, em PFS.

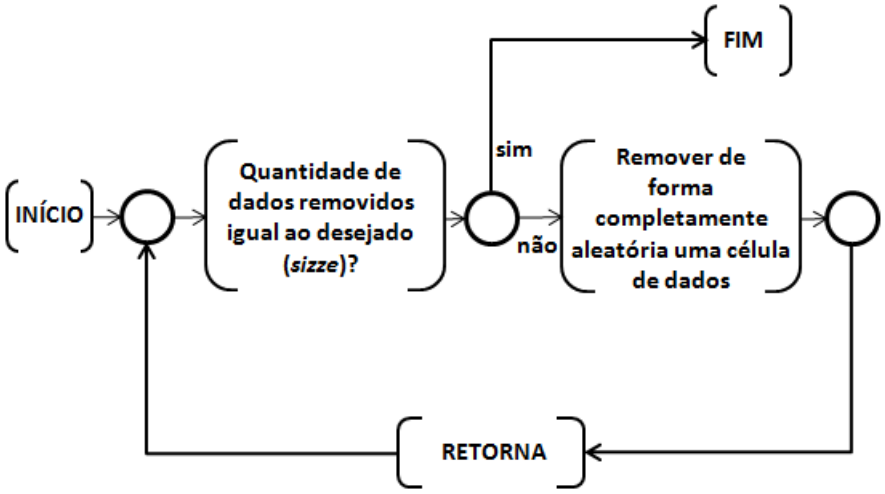
Figura 139 – Algoritmo da sub-rotina “carregar dados” em PFS



Fonte: próprio autor

A Figura 140 mostra o algoritmo da parte (3) subrotina “criar amostra de dados com dados faltantes”, em PFS.

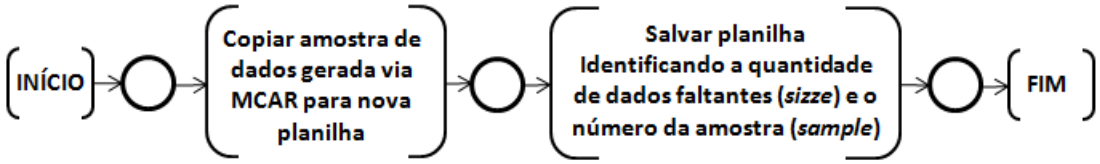
Figura 140 – Algoritmo da sub-rotina “criar amostra de dados com dados faltantes” em PFS



Fonte: próprio autor

Finalmente, a Figura 141 mostra o algoritmo da parte (4) sub-rotina “salvar planilha com amostra de dados”, em PFS.

Figura 141 – Algoritmo da sub-rotina “salvar planilha com amostra de dados” em PFS



Fonte: próprio autor

A seguir, apresenta-se os algoritmos acima descritos codificados em VBA.

```
Sub principal()
sizze = 922
    For sample = 1 to 5
                CarregarDados
                Call createsample(sizze, sample)
                Call Copiarecolaremnovaplanilha(sizze, sample)
    Next
 sizze = 1843
    For sample = 1 to 5
                CarregarDados
                Call createsample(sizze, sample)
                Call Copiarecolaremnovaplanilha(sizze, sample)
    Next
sizze = 2765
    For sample = 1 to 5
                CarregarDados
                Call createsample(sizze, sample)
                Call Copiarecolaremnovaplanilha(sizze, sample)
    Next
sizze = 3686
    For sample = 1 to 5
                CarregarDados
                Call createsample(sizze, sample)
                Call Copiarecolaremnovaplanilha(sizze, sample)
    Next
sizze = 4608
    For sample = 1 to 5
                CarregarDados
                Call createsample(sizze, sample)
                Call Copiarecolaremnovaplanilha(sizze, sample)
    Next
sizze = 5530
    For sample = 1 to 5
                CarregarDados
                Call createsample(sizze, sample)
                Call Copiarecolaremnovaplanilha(sizze, sample)
    Next
End Sub
```

```
Sub CarregarDados()

    Windows("MacroReinaldo").Activate
    Cells.Select
    Selection.QueryTable.Delete
    Selection.ClearContents
    Range("A1").Select

    With      ActiveSheet.QueryTables.Add(Connection:="TEXT;F:\BD_BPORIGINAL.csv"      _          ,
Destination:=Range("$A$1"))
        .Name = "BDTAF_BP_refinary_1"
        .FieldNames = True
        .RowNumbers = False
        .FillAdjacentFormulas = False
        .PreserveFormatting = True
        .RefreshOnFileOpen = False
        .RefreshStyle = xlInsertDeleteCells
        .SavePassword = False
        .SaveData = True
        .AdjustColumnWidth = True
        .RefreshPeriod = 0
        .TextFilePromptOnRefresh = False
        .TextFilePlatform = 437
        .TextFileStartRow = 1
        .TextFileParseType = xlDelimited
        .TextFileTextQualifier = xlTextQualifierDoubleQuote
        .TextFileConsecutiveDelimiter = False
        .TextFileTabDelimiter = True
        .TextFileSemicolonDelimiter = True
        .TextFileCommaDelimiter = False
        .TextFileSpaceDelimiter = False
        .TextFileColumnDataTypes =Array(1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1)
        .TextFileTrailingMinusNumbers = True
        .Refresh BackgroundQuery:=False
    End With

End Sub


Sub createsample(ByVal sizze As Integer, ByVal sample As Integer)
i = 0


Do While Not i = sizze
    Dim RNG As Range
    Set RNG = Range("A2:R1025")

    Dim randomCell As Long
        randomCell = Int(Rnd * RNG.Cells.Count) + sample

    With RNG.Cells(randomCell)
        .Select
        .Value = ""

    End With

i = Excel.WorksheetFunction.CountBlank(RNG)

Loop

End Sub
```

```
Sub Copiarecolaremnovaplanilha(ByVal sizze As Integer, ByVal sample As Integer)
'
' Copiarecolaremnovaplanilha Macro
'

    Range("A1:R1025").Select
    Selection.Copy
    Workbooks.Add
    ActiveSheet.Paste
    Application.CutCopyMode = False
    Range("S5").Select
    ChDir "F:\"
    ActiveWorkbook.SaveAs Filename:="F:\sample" & sample & "_" & sizze & ".csv", FileFormat:=
xlCSVMSDOS, CreateBackup:=False
    ActiveWorkbook.Save
    ActiveWorkbook.Close savechanges:=False

End Sub
```

APÊNDICE C – ESTUDO DE FIABILIDADE DE CONSTRUÇÃO DE MODELOS DE ACIDENTES A PARTIR DE BANCOS DE DADOS INCOMPLETOS/DADOS FALTANTES

Neste apêndice, é apresentada uma síntese do estudo de fiabilidade de modelos de acidentes aprendidos via imputação de dados e abordagem bayesiana, considerando bancos de dados incompletos ou com dados faltantes.

Este estudo foi elaborado com base nos dados obtidos do primeiro exemplo de aplicação que trata de um cenário de acidente ocorrido na unidade de isomerização da refinaria da *British Petroleum* (BP) na cidade de Texas nos Estados Unidos, em 23 de março de 2005.

C.1 INTRODUÇÃO

Modelos de acidentes, quando existirem, podem ser considerados elementos fundamentais para a elaboração do projeto de sistemas de controle relacionados à segurança e à implementação de estratégias de prevenção e mitigação de riscos. Estes modelos são elaborados com base nas abordagens: (i) conhecimento humano, e (ii) relatórios de investigação de acidentes. Entretanto, ambas as abordagens, dependem do conhecimento de especialistas e demandam tempo e custo.

Neste contexto, quando existirem bancos de dados com registros históricos de falhas, os mesmos podem ser usados para compor bancos de dados de treinamentos para aprendizagem de modelos causais, segundo abordagem bayesiana. Esta abordagem tem por objetivo reduzir ou eliminar a dependência de especialistas na construção de modelos de acidentes.

C.2 MOTIVAÇÃO

O problema da abordagem bayesiana é que a maioria dos algoritmos de aprendizagem de estruturas e parâmetros consideram bancos de dados completos. Adicionalmente, a maioria dos bancos de dados encontrados no cotidiano, possuem dados faltantes ou incompletos. Por outro lado, as ciências Estatística e Engenharia da Computação, têm contribuído para o desenvolvimento de algoritmos de imputação de dados, quando existirem bancos de dados com dados faltantes. Neste

contexto, surge uma questão: Podemos confiar em algoritmos de imputação de dados faltantes antes de proceder à modelagem de cenários de acidentes a partir de abordagem bayesiana? Este estudo pretende responder a esta questão.

C.3 OBJETIVO

Avaliar a sensibilidade dos modelos de cenários de acidentes, aprendidos via algoritmos de imputação de dados e aprendizagem bayesiana; considerando bancos de dados com dados faltantes.

C.4 METODOLOGIA

Para atender o objetivo descrito acima, é proposto um método constituído por oito passos que foram executados de maneira sistemática, conforme descrição abaixo:

Passo 1: Foi gerado de forma artificial, um banco de dados de treinamento da árvore de falhas (BDT_{AF}), de um suposto diagrama de *bowtie* encontrado em (FERDOUS, KHAN, *et al.*, 2013). O banco de dados possui dados completos e foi gerado a partir do método de Monte Carlo por meio da ferramenta *UnBBayes* – v.4.21.15.

Passo 2: O BDT_{AF} foi utilizado como base para aprendizagem da rede bayesiana, ou modelo estrutural ou gráfico acíclico orientado (GAO), que semanticamente representa a árvore de falhas (AF) do diagrama de *bowtie*. O algoritmo utilizado foi o *Chow-Liu tree* e a ferramenta utilizada foi *Hugin® Educational* - v.8.2. O GAO aprendido foi comparado com a AF do suposto diagrama de *Bowtie*, a fim de validar se o banco de dados de treinamento gerado no passo 1 é pertinente à AF.

Passo 3: Foram removidos de forma completamente aleatória - via mecanismo MCAR - 5%, 10%, 15%, 20%, 25% e 30% dos dados do BDT_{AF}, produzindo-se 5 amostras de bancos de dados de treinamento com dados faltantes para cada porcentagem adotada, ou seja, um total de 30 bancos de dados de treinamento com dados faltantes. O algoritmo que implementa o mecanismo MCAR é descrito no Apêndice A.

Passo 4: Cada amostra de dados obtida no passo 3 foi utilizada para aprendizagem dos GAOs, via algoritmo *Chow-Liu tree*, antes da imputação dos dados faltantes.

Passo 5: Cada GAO aprendido no passo 4, foi comparado com a AF do suposto diagrama de *bowtie*, adotado como referência, e eventuais discrepâncias[22] observadas foram registradas em uma tabela, que neste estudo são mostradas na Tabela 34.

Passo 6: Para cada banco de dados de treinamento com dados faltantes, obtido no passo 3, os dados faltantes foram imputados por meio do algoritmo MICE via método PMM. Durante o processo de imputação, o algoritmo MICE cria 5 bancos de dados imputados para cada amostra com dados faltantes; produzindo-se então 25 bancos de dados completos para cada amostra. Como foram criadas 5 amostras para cada porcentagem de dados faltantes (Passo 3), um total de 150 bancos de dados completos foram gerados para posterior análise. Na seção B.6 deste apêndice é mostrada uma parte do script utilizado para imputação de dados via MICE.

Passo 7: O algoritmo de *Chow-Liu tree* foi executado com base em cada banco de dados de treinamento obtido no passo 6, gerando modelos (GAOs) a partir de supostos bancos de dados completos.

Passo 8: Cada GAO gerado no passo 7, foi comparado com a AF do suposto diagrama de *bowtie*, adotado como referência, e eventuais discrepâncias observadas foram registradas em uma tabela, conforme ilustra a Tabela 35.

C.5 RESULTADOS

Os resultados deste estudo são mostrados nas Tabela 34 e Tabela 35.

Tabela 34 – Porcentagem de modelos estruturais (GAO) discrepantes antes do processo de imputação de dados

Quantidade de dados faltantes (%)	**Modelos estruturais (GAOs) aprendidos antes do processo de imputação de dados**					
	Amostra 1	Amostra 2	Amostra 3	Amostra 4	Amostra 5	Discrepância (%)
5	não	sim	sim	sim	não	60
10	sim	não	sim	não	sim	60
15	sim	sim	não	sim	sim	80
20	sim	não	não	não	não	20

[22] Entende-se por discrepância, qualquer desvio do GAO obtido pelas técnicas de imputação de dados e aprendizagem bayesiana, com relação aos `arcos` e os `nós` (eventos críticos), comparados com a AF pertencente ao diagrama de *bowtie*, tomada como referência.

25	sim	não	sim	sim	sim	80
30	sim	sim	sim	sim	sim	100

Legenda:

sim : modelo aprendido é discrepante da AF do modelo de *bowtie*

não: modelo aprendido não é discrepante com a AF do modelo de *bowtie*

Fonte: próprio autor

Tabela 35 – Porcentagem de modelos estruturais (GAO) discrepantes após o processo de imputação de dados

Quantidade de dados faltantes (%)	**Amostras**	**Modelos estruturais (GAOs) aprendidos após o processo de imputação de dados**					
		Imp1	Imp2	Imp3	Imp4	Imp5	Discrepância (%)
5	1	não	não	não	não	não	0
	2	não	não	não	não	não	
	3	não	não	não	não	não	
	4	não	não	não	não	não	
	5	não	não	não	não	não	
10	1	não	não	não	não	não	0
	2	não	não	não	não	não	
	3	não	não	não	não	não	
	4	não	não	não	não	não	
	5	não	não	não	não	não	
15	1	não	não	não	não	não	0
	2	não	não	não	não	não	
	3	não	não	não	não	não	
	4	não	não	não	não	não	
	5	não	não	não	não	não	
20	1	não	não	não	não	não	0
	2	não	não	não	não	não	
	3	não	não	não	não	não	
	4	não	não	não	não	não	
	5	não	não	não	não	não	
25	1	não	não	não	não	não	24
	2	não	não	não	não	não	
	3	não	sim	não	não	não	
	4	não	não	não	não	não	
	5	sim	sim	sim	sim	sim	
30	1	sim	sim	sim	não	sim	52
	2	sim	sim	não	sim	não	
	3	sim	não	não	não	não	
	4	sim	sim	sim	sim	não	
	5	não	não	não	não	sim	

Legenda:

sim : modelo aprendido é discrepante da AF do modelo de *bowtie*

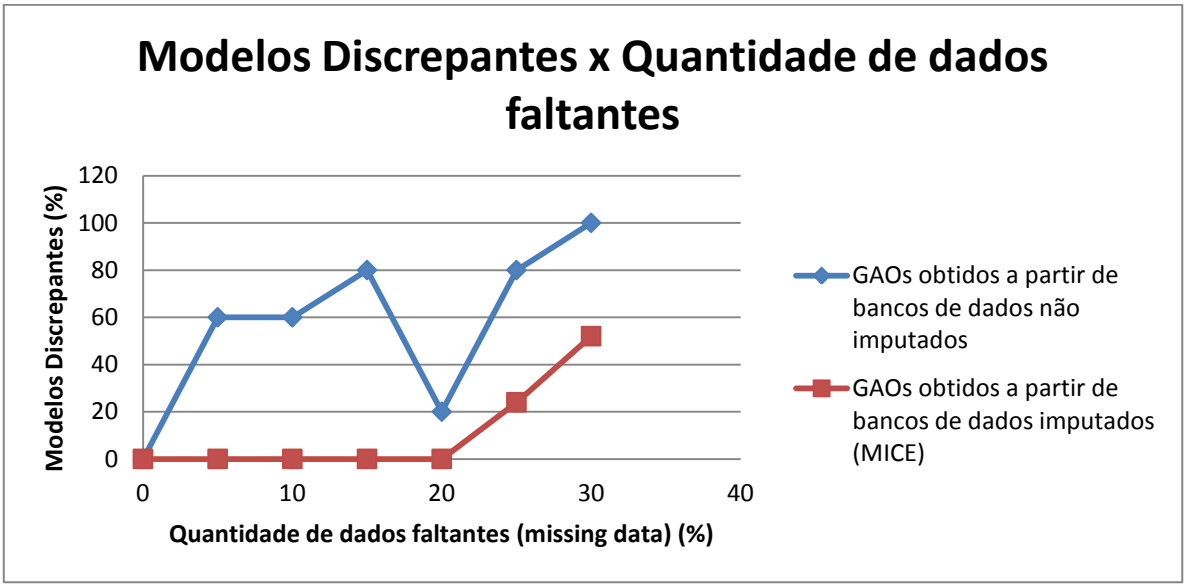
não: modelo aprendido não é discrepante com a AF do modelo de *bowtie*

Imp: imputação

Fonte: próprio autor

Finalmente, a Figura 142 mostra um gráfico que ilustra a relação em porcentagem, entre os modelos estruturais (GAOs) discrepantes e a quantidade de dados faltantes.

Figura 142 – Modelos discrepantes (%) x Quantidade de dados faltantes (%)



Fonte: próprio autor

C.6 SCRIPT PARA IMPUTAÇÃO DOS DADOS

É mostrada abaixo uma parte do script em R usado para imputação de dados via algoritmo MICE utilizando o método PMM. Esta parte refere-se à imputação de dados com base em cada amostra de dados com 20% de dados faltantes. As amostras de dados faltantes são arquivos de dados do tipo texto (.txt), denominadas de: sample1_3686i, sample2_3686i, sample3_3686i, sample4_3686i e sample5_3686i)

```
# Imputação de dados de Amostras com 20% de dados faltantes pelo mecanismo MCAR e padrão de
# dados não monotônico.
# O método de imputação selecionado é o PMM (Predictive Mean Matching)

# Inicialmente, selecionar o diretório onde se encontram as amostras com 20% de dados faltantes
# setwd("D:/Teste/Amostras 20_Imp")

# Executar a função mice( ) para a amostra sample1_3686i.txt
imp1 <- mice(sample1_3686i, defaultMethod = c("pmm"))

# Após a função mice( ) ter sido executada, são geradas 5 amostras de dados imputados.
# Cada amostra de dados imputados é completada à respectiva amostra de dados faltantes:
data1 <- complete(imp1,1)
data2 <- complete(imp1,2)
data3 <- complete(imp1,3)
data4 <- complete(imp1,4)
```

```
data5 <- complete(imp1,5)

# Finalmente, as amostras com dados imputados são armazenadas no diretório "D:/Teste/Amostras
20_Imp"

write.csv(data1, file='sample1_3686Imp1.csv')
write.csv(data2, file='sample1_3686Imp2.csv')
write.csv(data3, file='sample1_3686Imp3.csv')
write.csv(data4, file='sample1_3686Imp4.csv')
write.csv(data5, file='sample1_3686Imp5.csv')

# Executar a função mice( ) para a amostra sample2_3686i.txt
Imp2 <- mice(sample2_3686i, defaultMethod = c("pmm"))

# Após a função mice( ) ter sido executada, são geradas 5 amostras de dados imputados.
# Cada amostra de dados imputados é completada à respectiva amostra de dados faltantes:
data1 <- complete(imp2,1)
data2 <- complete(imp2,2)
data3 <- complete(imp2,3)
data4 <- complete(imp2,4)
data5 <- complete(imp2,5)

# Finalmente, as amostras com dados imputados são armazenadas no diretório "D:/Teste/Amostras
20_Imp"

write.csv(data1, file='sample2_3686Imp1.csv')
write.csv(data2, file='sample2_3686Imp2.csv')
write.csv(data3, file='sample2_3686Imp3.csv')
write.csv(data4, file='sample2_3686Imp4.csv')
write.csv(data5, file='sample2_3686Imp5.csv')

# Executar a função mice( ) para a amostra sample3_3686i.txt
Imp3 <- mice(sample3_3686i, defaultMethod = c("pmm"))

# Após a função mice( ) ter sido executada, são geradas 5 amostras de dados imputados.
# Cada amostra de dados imputados é completada à respectiva amostra de dados faltantes:
data1 <- complete(imp3,1)
data2 <- complete(imp3,2)
data3 <- complete(imp3,3)
data4 <- complete(imp3,4)
data5 <- complete(imp3,5)

# Finalmente, as amostras com dados imputados são armazenadas no diretório "D:/Teste/Amostras
20_Imp"

write.csv(data1, file='sample3_3686Imp1.csv')
write.csv(data2, file='sample3_3686Imp2.csv')
write.csv(data3, file='sample3_3686Imp3.csv')
write.csv(data4, file='sample3_3686Imp4.csv')
write.csv(data5, file='sample3_3686Imp5.csv')

# Executar a função mice( ) para a amostra sample4_3686i.txt
Imp4 <- mice(sample4_3686i, defaultMethod = c("pmm"))

# Após a função mice( ) ter sido executada, são geradas 5 amostras de dados imputados.
# Cada amostra de dados imputados é completada à respectiva amostra de dados faltantes:
data1 <- complete(imp4,1)
data2 <- complete(imp4,2)
data3 <- complete(imp4,3)
data4 <- complete(imp4,4)
data5 <- complete(imp4,5)

# Finalmente, as amostras com dados imputados são armazenadas no diretório "D:/Teste/Amostras
20_Imp"
```

```
write.csv(data1, file='sample4_3686Imp1.csv')
write.csv(data2, file='sample4_3686Imp2.csv')
write.csv(data3, file='sample4_3686Imp3.csv')
write.csv(data4, file='sample4_3686Imp4.csv')
write.csv(data5, file='sample4_3686Imp5.csv')

# Executar a função mice( ) para a amostra sample5_3686i.txt
Imp5 <- mice(sample5_3686i, defaultMethod = c("pmm"))

# Após a função mice( ) ter sido executada, são geradas 5 amostras de dados imputados.
# Cada amostra de dados imputados é completada à respectiva amostra de dados faltantes:
data1 <- complete(imp5,1)
data2 <- complete(imp5,2)
data3 <- complete(imp5,3)
data4 <- complete(imp5,4)
data5 <- complete(imp5,5)

# Finalmente, as amostras com dados imputados são armazenadas no diretório "D:/Teste/Amostras
20_Imp"

write.csv(data1, file='sample5_3686Imp1.csv')
write.csv(data2, file='sample5_3686Imp2.csv')
write.csv(data3, file='sample5_3686Imp3.csv')
write.csv(data4, file='sample5_3686Imp4.csv')
write.csv(data5, file='sample5_3686Imp5.csv')
```

C.7 CONCLUSÕES

Com base no gráfico mostrado na Figura 142, observou-se que, para todas as amostras de dados com até vinte por cento (20%) de dados faltantes, quando foram aplicadas as técnicas de imputação de dados e posteriormente de aprendizagem bayesiana, nesta ordem, os modelos estruturais (GAOs) obtidos foram semelhantes ao modelo de referência adotado, ou seja, não apresentaram discrepâncias. Adicionalmente, para amostras contendo 24% de dados faltantes, a discrepância observada foi de 20% e para amostras contendo 30% de dados faltantes, a discrepância observada foi de 52%.

O gráfico da Figura 142 ilustra que, quanto maior a quantidade de dados faltantes, maior é a discrepância dos modelos aprendidos; caso não seja aplicada a técnica de imputação de dados antes de proceder à aprendizagem dos modelos.

APÊNDICE D – EXEMPLO DE APLICAÇÃO 2

Neste apêndice é apresentado o segundo exemplo de aplicação que é baseado num acidente que ocorreu num sistema de carregamento de hidrocarboneto na forma líquida em um caminhão tanque. As bases de dados para este exemplo são encontradas em (BADREDDINE e BEN AMOR, 2013).

Descreve-se a seguir a aplicação do *framework* para a síntese do SCSP

D.1 Fase 1 – Método para elaboração do HAZOP

As atividades pertinentes à esta fase, como por exemplo, a definição dos elementos, parâmetros, desvios e palavras guias da planta/processo, também não serão descritas para este exemplo. Neste exemplo, o estudo de HAZOP já existe de modo que nesta fase os dados disponíveis são devidamente organizados na tabela do HAZOP de acordo com a estrutura da Tabela 1.

D.2 Fase 2 – Método para elaboração dos modelos de acidentes

Vale ressaltar que como o foco deste trabalho é a modelagem do acidente a partir de um suposto histórico de falhas que possui dados ausentes/faltantes, devido a observabilidade parcial de alguns eventos críticos e/ou indesejados, a construção do modelo será realizada usando abordagem probabilística via algoritmo de aprendizagem bayesiana.

- **Etapa 1 – Definição inicial**

Nesta etapa as seguintes atividades devem ser realizadas.

- **Definição da planta/processo**

A planta/processo a ser considerado é a unidade de carregamento de hidrocarboneto em caminhões tanques, assim como seus dispositivos de realização de controle básico (SCBP). Este conjunto é o objeto de controle para o SCSP.

- **Definição do time de especialistas**

O time é constituído por engenheiros de processos, operadores de processos e engenheiros de segurança de processos. Este time possui conhecimento multidisciplinar sobre a planta/processo, e sobre as normas de segurança aplicáveis (IEC 61511, 2003) e (IEC 61508, 2010).

- **Definição da documentação do projeto**

Embora não tenham sido encontradas em Badreddine e Ben Amor (2013), documentações, como por exemplo, fluxograma do processo e da instrumentação do processo (P&ID), para este objeto de controle existem informações suficientes para as tomadas de decisões por parte do time de especialistas, de modo a caracterizar partes do sistema (planta/processo) e os elementos deste sistema que estão associados aos eventos críticos e/ou indesejados, assim como, às falhas críticas.

No trabalho de Badreddine e Bem Amor (2013) tem-se um diagrama de *bowtie*, obtido a partir de um método de modelagem baseado numa abordagem probabilística via aprendizagem de estruturas e parâmetros de redes bayesianas que semanticamente representam as AF e AE. Vale ressaltar que a abordagem a ser aplicada, considera bancos de dados completos ou incompletos / dados faltantes.

- **Registros históricos de falhas**

Em Badreddine e Ben Amor (2013), registros históricos de falhas são apresentados dois bancos de dados de treinamentos: (a) um denominado de TS_{FT}, do termo inglês *Training set for Fault Tree*, que considera as “causas” do evento topo, e (b) outro denominado de TS_{ET}, do termo inglês *Training set for Event Tree*, que considera as “consequências” decorrentes do evento topo; ambos baseados na suposição que os bancos de dados estão completos.

Por outro lado, como a abordagem deste trabalho endereça a modelagem de acidentes considerando bancos de dados incompletos ou com dados faltantes, os bancos de dados de treinamentos BDT_{AF} e BDT_{AE}, considerados neste exemplo, possuem dados faltantes ou incompletos, que foram gerados artificialmente via procedimento probabilístico descrito nos Apêndices A e B.

- **Etapa 2 - Aprendizagem da estrutura da árvore de falhas (AF)**

Subetapa 2.1 – Montagem do banco de dados de treinamento (BDTAF)

As amostras aleatórias constituídas de dados completos obtidas via Simulação Monte Carlo, foram obtidas a partir do procedimento descrito no Apêndice A. Adicionalmente, foram gerados de maneira artificial bancos de dados incompletos com 5%, 10%, 15%, 20%, 25% e 30% de dados faltantes, com base no algoritmo para remoção completamente aleatória de dados (MCAR) descrito no Apêndice B. Ainda com base no resultado do estudo de fiabilidade de modelos de acidentes aprendidos via imputação de dados e abordagem bayesiana, considerando bancos de dados faltantes, e que é apresentado no Apêndice C deste trabalho, considera-se neste exemplo de aplicação, que o BDT_{AF} possui 20% (vinte por cento) de dados

faltantes que corresponde ao valor máximo em porcentagem de dados faltantes em que a técnica de imputação pode ser aplicada com fiabilidade para a construção dos modelos de acidentes.

A Tabela 36 mostra parte do BDT_{AF} com dados incompletos ou faltantes para aprendizagem da AF. Nesta tabela a primeira coluna corresponde ao evento topo (ET) que representa o incêndio e explosão do caminhão tanque, e as colunas restantes correspondem aos eventos iniciadores (IEs) e eventos críticos (ECs) como "causas" observadas ou parcialmente observadas antes da ocorrência do ET, em qualquer combinação, como por exemplo, IE1 = DTA, EC2 = GO, IE3 = EF, IE4 = CTP, IE2 = TVF, EC1 = HGL, EC3 = SI e EC4 = PS.

A descrição dos IEs/CEs para o cenário considerado é mostrada na Figura 143.

Figura 143 – Descrição das "causas" do ET.

Evento	Descrição das "causas"
IE1 = DTA	perfuração do tanque
EC2 = GO	odor de gás hidrocarboneto
IE3 = EF	falha na exaustão
IE4 = CTP	planta/processo próxima do estacionamento dos caminhões
IE2 = TVF	falha da válvula do tanque
EC1 = HGL	vazamento de gás hidrocarboneto
EC3 = SI	fonte de ignição
EC4 = PS	presença de faíscas

Fonte: (BADREDDINE e BEN AMOR, 2013)

Tabela 36 – Parte do banco de dados de treinamento com vinte por cento (20%) de dados faltantes para aprendizagem da árvore de falhas (AF)

ET	DTA	GO	EF	CTP	TVF	HGL	SI	PS
1	1	1	1	NA	0	1	1	1
0	1	0	0	0	0	0	0	NA
NA	0	NA	NA	1	NA	0	1	1
NA	0	NA	NA	1	0	0	0	0
NA	1	NA	1	0	0	1	NA	0
1	NA	0	1	NA	1	NA	0	0
1	0	1	1	NA	1	1	1	NA
0	1	0	NA	0	0	0	0	NA
0	NA	1	1	0	1	NA	NA	1
0	0	1	NA	0	NA	0	1	1
0	0	1	NA	1	1	1	NA	1
0	0	NA	1	0	0	0	NA	0
NA	0	1	0	0	1	1	NA	1
1	NA	0	NA	0	0	0	0	0
NA	1	1	NA	0	1	1	0	0
1	0	0	0	0	NA	0	NA	1
0	1	1	0	0	NA	NA	0	1
0	NA	0	0	0	0	0	1	1
0	0	1	NA	0	NA	1	0	0
1	1	1	0	NA	0	1	0	NA
1	0	NA	0	0	1	1	0	0
0	0	0	0	NA	0	0	0	0
1	0	NA	NA	1	1	1	0	NA
0	1	0	1	0	0	0	0	0
1	0	1	NA	0	1	NA	1	1
1	0	0	1	0	0	0	1	NA
1	0	NA	1	NA	NA	1	1	1
NA	0	0	0	1	0	0	0	0
1	1	1	0	0	1	NA	0	0
1	NA	0	0	1	0	0	1	1
1	NA	1	0	0	NA	1	NA	0
1	1	1	1	0	0	1	NA	0
1	0	1	0	NA	1	NA	0	0
1	1	NA	1	1	0	1	1	1
0	0	1	0	0	1	NA	0	NA
0	NA	0	0	0	0	0	0	0
NA	NA	1	0	NA	1	1	NA	0
0	0	0	0	0	0	0	0	0
1	1	1	1	NA	1	1	NA	1
0	NA	0	0	0	0	0	0	0
1	1	NA	1	0	1	1	1	NA
1	1	0	0	1	0	0	1	1
1	0	1	0	0	NA	NA	NA	0

Fonte: próprio autor

Cada linha ou instância da matriz mostrada na Tabela 36, contém um valor binário (ex: 0 / Falso ou 1 / Verdadeiro) para o ET e para cada IE/EC que foi observado. Entretanto, para os IEs/ECs ou “causas” que não foram observadas em algumas instâncias, os valores contidos no BDT_{AF} para estes eventos, não contém valores binários disponíveis e são representados na Tabela 36 como “NA” (do termo em inglês “*Not Available”*).

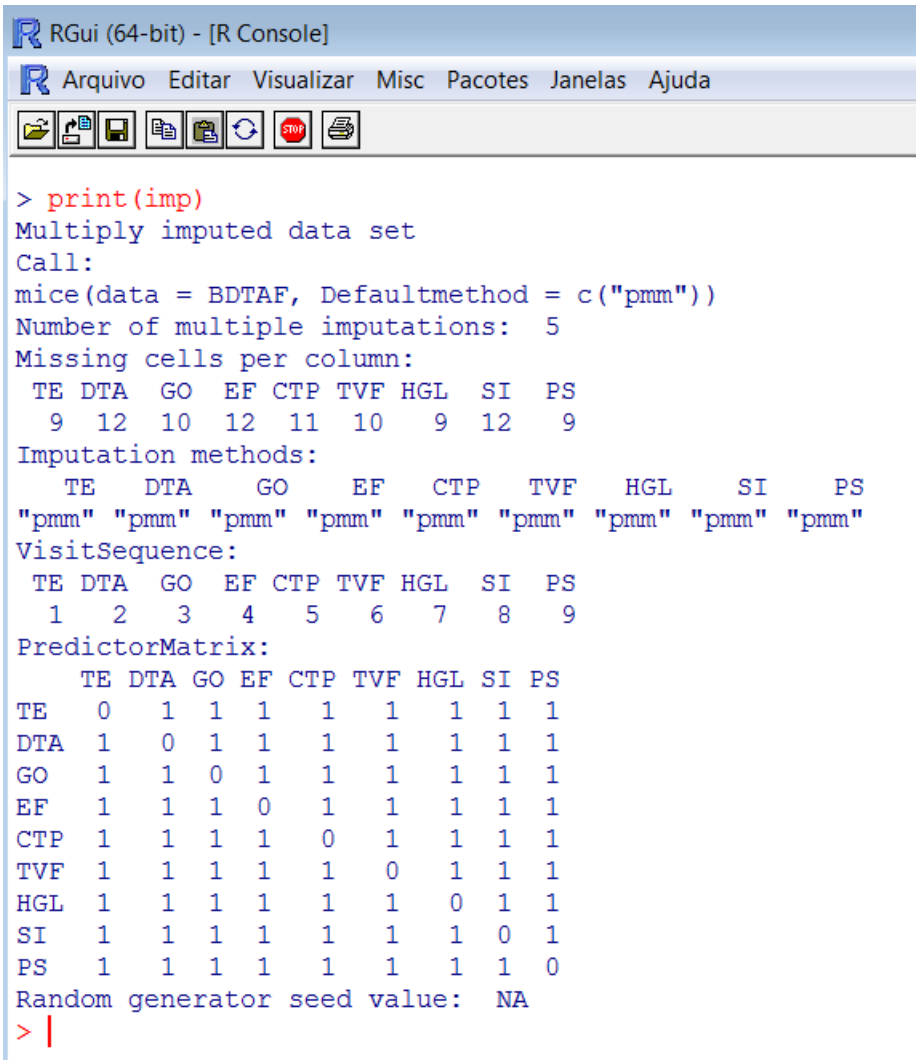
Subetapa 2.2 – Imputação de dados

A imputação dos dados faltantes do BDT_{AF} por valores “plausíveis” é feita via algoritmo de imputação multivariada baseada em equações encadeadas (MICE), que é disponibilizada em um pacote (*toolbox*) que é executado no software computacional estatístico R. A versão do R utilizada neste trabalho é a 3.2.4 e a versão do pacote MICE para R é a 3.25. O BDT_{AF} obtido com dados incompletos/faltantes, é convertido para um arquivo com formato (*.txt*) para ser importado para o ambiente R. O comando para a execução da imputação de dados tem o seguinte formato:

$$\text{imp} \leftarrow \text{mice}(BDT_{AF}, \text{defaultMethod=c}(\text{“pmm”}))$$

Um resumo de informações pertinentes à parametrização do processo de imputação, é mostrado na Figura 144.

Figura 144 – Resumo de informações do processo de imputação MICE



Fonte: próprio autor

No processo de imputação, são geradas 5 amostras de dados contendo os valores estimados para cada dado faltante, a fim de se considerar as incertezas associadas a este processo. Assim é necessário considerar as 5 amostras de dados para análise das mesmas. Desta forma, para se obter os 5 bancos de dados completos a partir das 5 amostras geradas, digita-se os comandos abaixo:

BDTAF1 ← complete(imp, 1)

BDTAF2 ← complete(imp, 2)

BDTAF3 ← complete(imp, 3)

BDTAF4 ← complete(imp, 4)

BDTAF5 ← complete(imp, 5)

A Tabela 37 mostra como exemplo, parte do BDT_{AF} com os dados imputados.

Tabela 37 – Parte do banco de dados de treinamento (BDT_{AF}) com dados imputados via MICE

ET	DTA	GO	EF	CTP	TVF	HGL	SI	PS
1	1	1	1	1	0	1	1	1
0	1	0	0	0	0	0	0	0
1	0	0	1	1	1	0	1	1
0	0	0	0	1	0	0	0	0
0	1	1	1	0	0	1	0	0
1	0	0	1	0	1	0	0	0
1	0	1	1	0	1	1	1	1
0	1	0	0	0	0	0	0	0
0	0	1	1	0	1	1	1	1
0	0	1	0	0	0	0	1	1
0	0	1	0	1	1	1	1	1
0	0	0	1	0	0	0	0	0
1	0	1	0	0	1	1	1	1
1	0	0	1	0	0	0	0	0
1	1	1	0	0	1	1	0	0
1	0	0	0	0	0	0	1	1
0	1	1	0	0	1	1	0	1
0	0	0	1	0	0	0	1	1
0	0	1	0	0	1	1	0	0
1	1	1	0	0	0	1	0	0
1	0	1	0	0	1	1	0	0
0	0	0	0	1	0	0	0	0
1	0	1	1	1	1	1	0	0
0	1	0	1	0	0	0	0	0
1	0	1	1	0	1	1	1	1
1	0	0	1	0	0	0	1	1
1	0	1	1	0	1	1	1	1
0	0	0	0	1	0	0	0	0
1	1	1	0	0	1	1	0	0
1	0	0	0	1	0	0	1	1
1	0	1	0	0	1	1	0	0
1	1	1	1	0	0	1	0	0
1	0	1	0	0	1	1	0	0
1	1	1	1	1	0	1	1	1
0	0	1	0	0	1	1	0	0
0	0	0	0	0	0	0	0	0
1	0	1	0	0	1	1	0	0
0	0	0	0	0	0	0	0	0
1	1	1	1	0	1	1	1	1
0	0	0	0	0	0	0	0	0
1	1	1	1	0	1	1	1	1
1	1	0	0	1	0	0	1	1
1	0	1	0	0	1	1	0	0

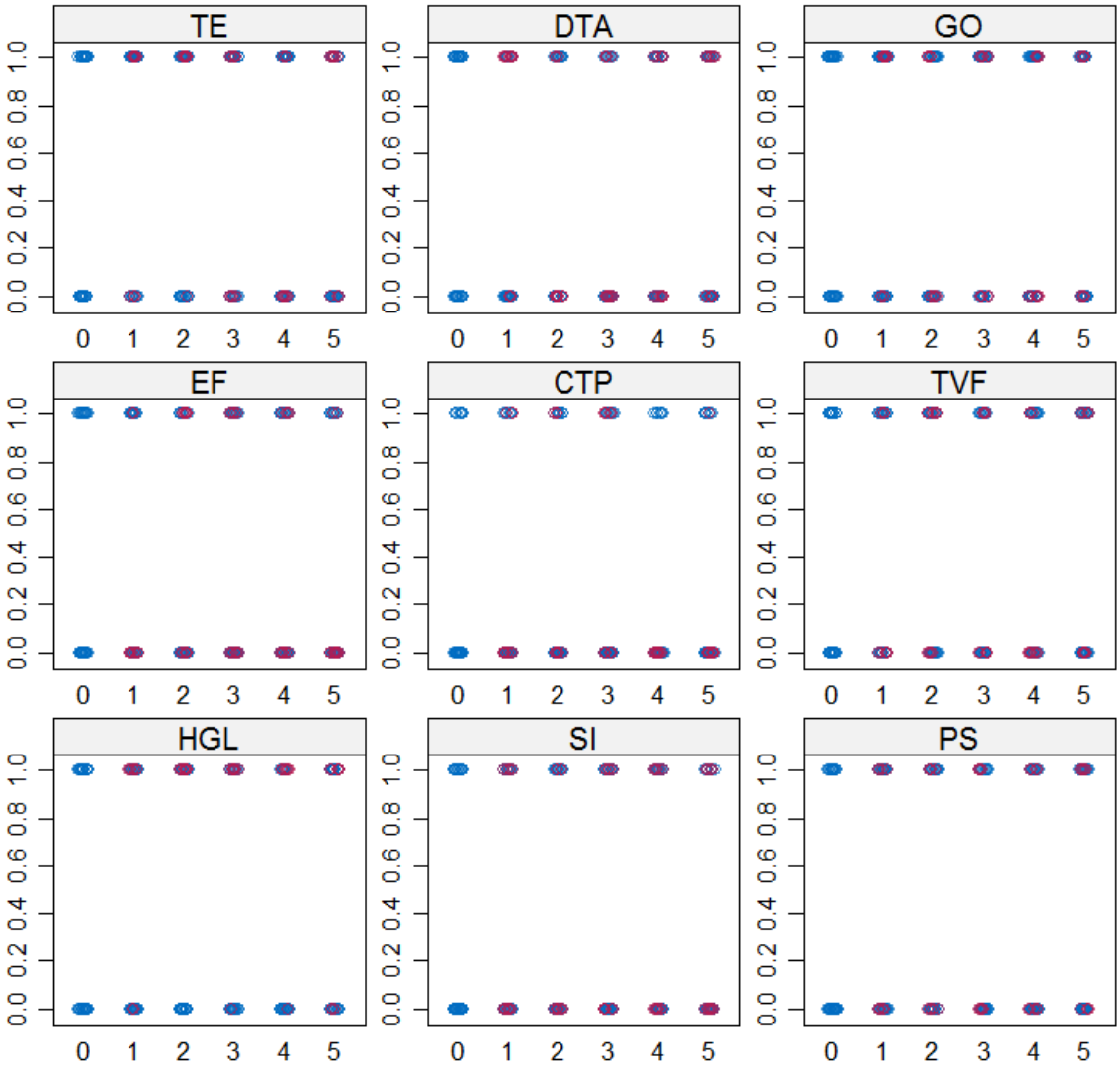
Fonte: próprio autor

De acordo com Buueren e Oudshoom (2011), deve-se inspecionar se não existem discrepâncias entre as distribuições dos dados originais (dados que foram observados) com os dados imputados via MICE no BDT_{AF}. O comando utilizado para esta atividade tem o seguinte formato:

```
stripplot(imp)
```

Gera-se assim gráficos com a distribuição de cada variável do banco de dados BDT_{AF}, conforme mostra a Figura 145. Neste gráficos os pontos azuis representam os dados observados e os vermelhos representam os dados imputados.

Figura 145 – Distribuições entre dados observados e imputados via MICE



Fonte: próprio autor

Como pode ser visto na Figura 145, as distribuições entre os dados originais (pontos azuis) e os dados imputados (pontos vermelhos) são semelhantes, não existindo discrepância entre eles. Este fato está diretamente relacionado com o

método de imputação selecionado. Dessa forma, o método “PMM” empregado para imputação é pertinente à aplicação envolvida.

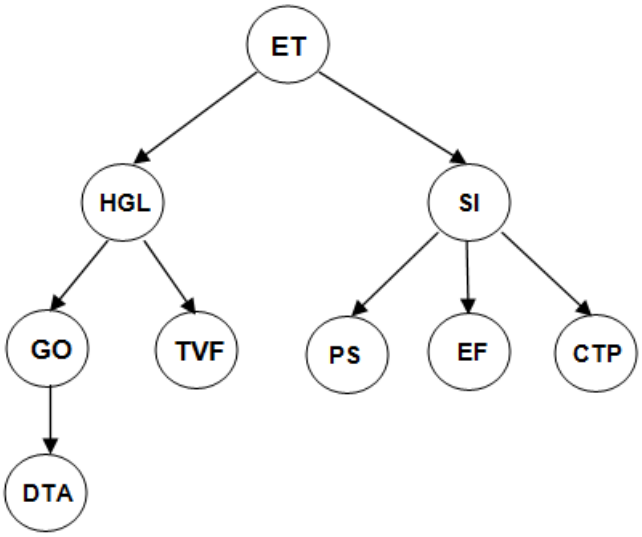
Subetapa 2.3 – Execução do algoritmo de aprendizagem Chow e Liu tree

Os 5 bancos de dados de treinamento: BDTAF1, BDTAF2, BDTAF3, BDTAF4 e BDTAF5, são utilizados como entradas de dados para a execução do algoritmo de aprendizagem.

O algoritmo de aprendizagem de *Chow* e *Liu* (CHOW e LIU, 1968), é aqui utilizado via ferramenta computacional *Hugin Educational*®. A estrutura ou GAO obtida nesta subetapa, é derivada a partir de cada banco de dado de treinamento, sendo obtidos 5 GAOs. Os 5 GAOs são comparados um a um e os que se mostram semelhantes são considerados como sendo a árvore de falha (AF) resultante. O(s) que se mostra(am) discrepante(s) é(são) desconsiderado(s).

A estrutura ou GAO da AF obtida nesta subetapa é mostrada na Figura 146.

Figura 146 – GAO da árvore de falhas (AF)



Fonte: próprio autor

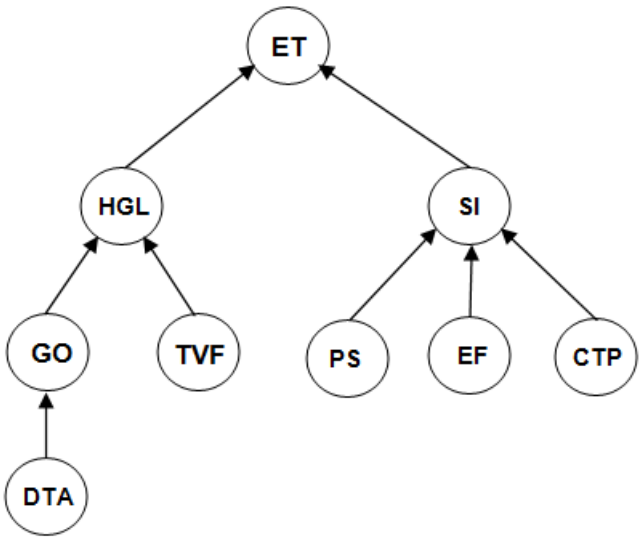
- **Etapa 3 – Construção do modelo da árvore de falhas (AF)**

A estrutura da AF é submetida à equipe de especialistas que verificam se as relações de dependência são pertinentes ou não e modificam a estrutura, adicionando e/ou removendo `arcos` e/ou EC_s até convergir a um modelo da AF que seja pertinente com a realidade do processo/planta.

Observa-se que a estrutura da rede bayesiana mostrada na Figura 146, representa uma distribuição de probabilidade conjunta na forma de árvore com os `arcos` que partem (saem) do ET, que no caso é o `nó` raiz, para as “causas”. Esta estrutura é então revista como um diagrama da árvore de falhas (AF), de modo que

os `arcos` tenham sua orientação invertida, ou seja, os mesmos devem ser dirigidos das “causas” para o ET. A Figura 147 mostra a AF resultante.

Figura 147 – Árvore de falhas (AF)



Fonte: próprio autor

- **Etapa 4 – Aprendizagem da estrutura da árvore de eventos (AE)**

Subetapa 4.1 – Montagem do banco de dados de treinamento (BDT_{AE})

Da mesma forma que o BDT_{AF}, o banco de dados de treinamento da árvore de eventos (BDT_{AE}) nesta subetapa, foi obtido a partir dos procedimentos mostrados nos Apêndices A e B, considerando que não foram encontrados registros históricos de falhas para este exemplo de aplicação.

Com base no estudo de fiabilidade de modelos de acidentes aprendidos via imputação de dados e abordagem bayesiana, considerando bancos de dados faltantes (Apêndice C), assume-se neste exemplo de aplicação, que o BDT_{AE} possui 20% (vinte por cento) de dados faltantes.

A Tabela 38 mostra parte do BDT_{AE} com dados incompletos ou faltantes para aprendizagem da AE. Nesta tabela a primeira coluna corresponde ao evento topo (ET) que identifica o incêndio e explosão após o derramamento de hidrocarboneto na forma líquida, e as demais colunas correspondem aos eventos indesejados (UE_s) e consequências indesejadas (OE_s) observadas ou parcialmente observadas, após a ocorrência do ET, em qualquer combinação. Os UE_s e OE_s são: OE5 = LD, OE4 = DE, OE3 = TODP, OE2 = DT, OE1 = TDP, UE4 = PPS, UE3 = TOE, UE1 = PF e UE2 = THE e são descritos na Figura 148.

Figura 148 – Descrição das “consequências” do ET.

Evento	Descrição das “consequências”
OE5 = LD	atraso na entrega de combustível
OE4 = DE	danos ambientais
OE3 = TODP	danos tóxicos às pessoas
OE2 = DT	danos a outros caminhões
OE1 = TDP	danos térmicos às pessoas
UE4 = PPS	planta/processo “parado”
UE3 = TOE	efeitos tóxicos
UE1 = PF	piscina de fogo
UE2 = THE	efeitos térmicos

Fonte: (BADREDDINE e BEN AMOR, 2013)

Tabela 38 – Parte do banco de dados de treinamento com vinte por cento (20%) de dados faltantes para aprendizagem da árvore de eventos (AE)

ET	LD	DE	TODP	DT	TDP	PPS	TOE	PF	THE
1	1	NA	1	1	1	1	1	NA	1
NA	1	1	1	0	1	1	1	1	1
NA	NA	0	1	0	0	1	0	0	0
0	1	1	0	NA	NA	0	0	0	NA
0	0	NA	1	0	1	1	NA	0	0
0	0	NA	NA	1	1	0	0	0	1
0	1	0	1	NA	0	1	0	0	0
NA	0	0	0	NA	NA	1	0	0	0
1	1	1	1	1	1	1	NA	1	1
NA	0	NA	0	0	1	0	0	0	1
0	NA	NA	NA	0	1	0	0	NA	1
0	NA	NA	1	0	1	1	0	0	NA
0	1	1	1	NA	0	0	NA	0	0
NA	1	0	0	1	NA	NA	0	NA	1
0	0	1	1	0	1	0	1	0	0
0	NA	1	0	1	0	NA	0	0	0
1	1	1	1	1	1	1	1	1	1
NA	0	1	NA	NA	NA	NA	1	NA	NA
NA	1	1	0	1	0	1	NA	1	NA
0	0	0	0	1	1	0	0	0	1
0	NA	1	1	0	0	0	1	0	0
0	0	1	0	NA	1	0	NA	NA	1
NA	0	NA	NA	1	NA	0	1	0	0
0	1	1	0	0	1	1	NA	0	0
0	0	0	1	1	0	NA	0	0	0
1	1	1	1	1	1	1	NA	1	1
0	0	NA	0	0	0	1	0	0	NA
0	1	NA	0	NA	1	1	0	0	0
0	NA	1	1	0	0	0	NA	0	0
0	0	0	0	NA	1	NA	0	0	NA
0	0	1	0	0	1	0	1	0	0
NA	1	0	1	NA	NA	1	0	NA	0
0	1	1	1	0	0	0	1	0	0
0	0	1	NA	0	1	0	1	0	0
1	1	1	1	0	1	1	1	NA	1
0	NA	0	0	0	1	1	0	0	0
0	NA	1	NA	0	0	1	0	0	0
0	0	0	1	0	NA	NA	0	NA	NA
0	1	0	NA	0	1	1	0	0	0
1	0	1	0	0	NA	NA	0	0	NA
NA	0	0	NA	1	1	0	0	0	1
0	1	1	0	0	NA	NA	0	0	0
0	0	NA	1	0	0	0	1	0	0

Cada linha ou instância da matriz mostrada na Tabela 38, contém um valor binário (ex: 0 / Falso ou 1 / Verdadeiro) para o ET e para cada UE/OE que foi observado. Para os UEs/OEs que não foram observadas em algumas instâncias, os valores contidos no BDT_{AE} para estes eventos, não contém valores binários disponíveis e são representados na Tabela 38 como “NA” (do termo em inglês “*Not Available*”).

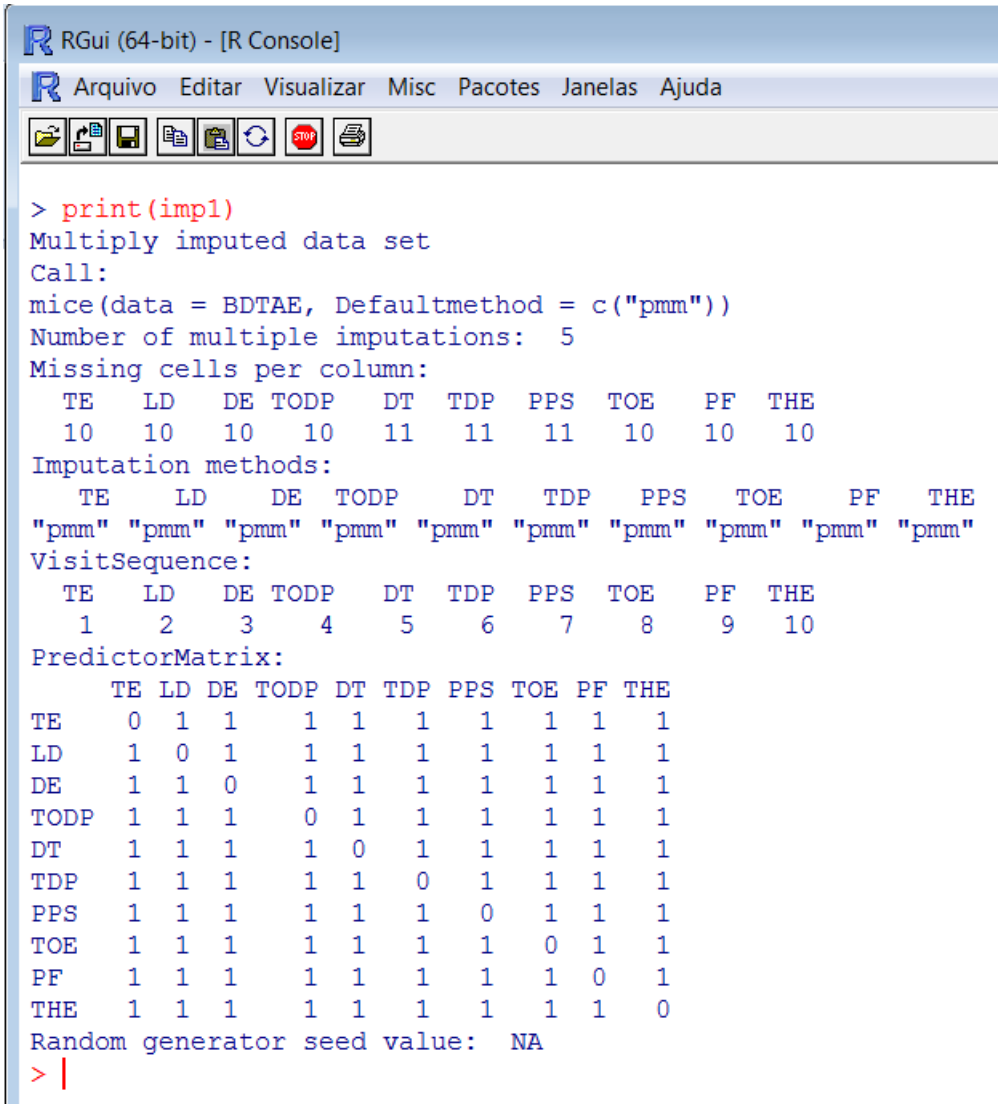
Subetapa 4.2 – Imputação de dados

A imputação dos dados faltantes do BDT_{AE} por valores “plausíveis é feita via algoritmo de imputação multivariada baseada em equações encadeadas (MICE). O BDT_{AE} com dados incompletos/faltantes é convertido para um arquivo com formato (*.txt*) para ser importado para o ambiente R. O comando para a execução da imputação de dados deste BDT_{AE} tem o seguinte formato:

imp1 ← mice(BDTAE, defaultMethod=c(“pmm”))

O resumo das informações pertinentes à parametrização do processo de imputação é mostrado na Figura 149.

Figura 149 – Resumo de informações do processo de imputação MICE



Fonte: próprio autor

Neste processo de imputação, tem-se 5 amostras de dados contendo os valores estimados para cada dado faltante. Desta forma, para se obter os 5 bancos de dados completos a partir das 5 amostras geradas, deve-se digitar os comandos abaixo:

BDTAE1 ← complete(imp1,1)

BDTAE2 ← complete(imp1,2)

BDTAE3 ← complete(imp1,3)

BDTAE4 ← complete(imp1,4)

BDTAE5 ← complete(imp1,5)

A Tabela 39 mostra como exemplo, parte do BDTAE4 com os dados imputados.

O comando “stripplot( )” é então executado para inspecionar se não existem discrepâncias entre as distribuições dos dados originais (dados que foram observados) com os dados imputados via MICE no BDT_{AE}.

Tabela 39 – Parte do banco de dados de treinamento (BDTAE4) com dados imputados via MICE

ET	LD	DE	TODP	DT	TDP	PPS	TOE	PF	THE
1	1	1	1	1	1	1	1	1	1
1	1	1	1	0	1	1	1	1	1
0	1	0	1	0	0	1	0	0	0
0	1	1	0	0	1	0	0	0	0
0	0	1	1	0	1	1	1	0	0
0	0	1	1	1	1	0	0	0	1
0	1	0	1	0	0	1	0	0	0
0	0	0	0	0	0	1	0	0	0
1	1	1	1	1	1	1	1	1	1
0	0	0	0	0	1	0	0	0	1
0	0	1	0	0	1	0	0	0	1
0	1	0	1	0	1	1	0	0	0
0	1	1	1	0	0	0	1	0	0
0	1	0	0	1	1	0	0	0	1
0	0	1	1	0	1	0	1	0	0
0	0	1	0	1	0	0	0	0	0
1	1	1	1	1	1	1	1	1	1
0	0	1	1	0	0	0	1	0	0
0	1	1	0	1	0	1	1	1	1
0	0	0	0	1	1	0	0	0	1
0	1	1	1	0	0	0	1	0	0
0	0	1	0	1	1	0	0	0	1
0	0	1	1	1	0	0	1	0	0
0	1	1	0	0	1	1	0	0	0
0	0	0	1	1	0	0	0	0	0
1	1	1	1	1	1	1	1	1	1
0	0	1	0	0	0	1	0	0	0
0	1	0	0	0	1	1	0	0	0
0	0	1	1	0	0	0	1	0	0
0	0	0	0	0	1	0	0	0	1
0	0	1	0	0	1	0	1	0	0
0	1	0	1	0	0	1	0	0	0
0	1	1	1	0	0	0	1	0	0
0	0	1	1	0	1	0	1	0	0
1	1	1	1	0	1	1	1	1	1
0	1	0	0	0	1	1	0	0	0

Figura 150 – Distribuições entre dados observados e imputados via MICE

Fonte: próprio autor

Os gráficos de distribuição de cada variável do banco de dados BDT_{AE}, é mostrada na Figura 150. Nestes gráficos os pontos azuis representam os dados observados e os vermelhos representam os dados imputados. A partir destes gráficos observa-se que os dados que foram imputados possuem uma distribuição semelhante à distribuição dos dados observados.

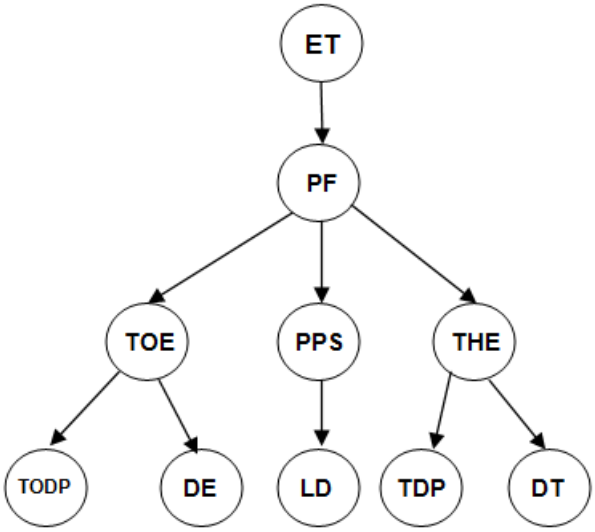
Subetapa 4.3 – Execução do algoritmo de aprendizagem *Chow* e *Liu tree*

Os 5 bancos de dados de treinamento: BDTAE1, BDTAE2, BDTAE3, BDTAE4 e BDTAE5, são utilizados como entradas de dados para a execução do algoritmo de aprendizagem.

O algoritmo de aprendizagem utilizado neste trabalho é o proposto por *Chow* e *Liu* (CHOW e LIU, 1968) junto com a ferramenta computacional *Hugin Educational*®. A estrutura ou GAO da AE é derivada a partir de cada banco de dados de treinamento, sendo obtidos portanto 5 GAOs. Os 5 GAOs são comparados um a um e os que mais se mostraram semelhantes são considerados como sendo a árvore de evento (AE) resultante. O(s) que se mostra(am) discrepante(s) é(são)

desconsiderado(s). A estrutura ou GAO obtido nesta subetapa é mostrada na Figura 151.

Figura 151 – GAO da árvore de eventos (AE)



Fonte: próprio autor

- **Etapa 5 – Construção do modelo de árvore de eventos (AE)**

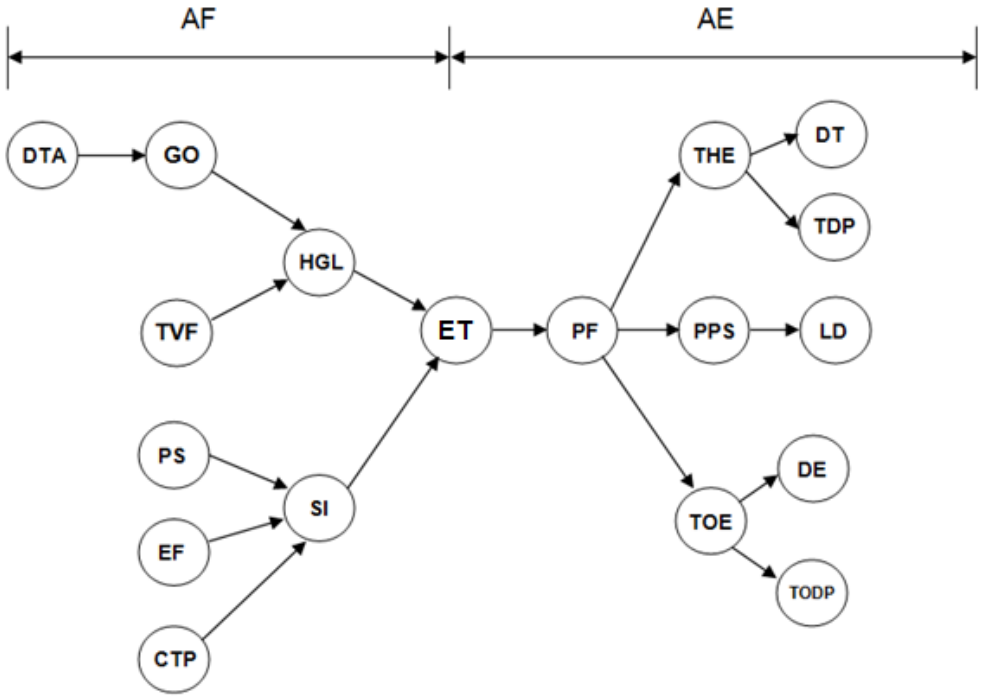
A estrutura ou AE mostrada na Figura 151, é submetida para os especialistas que verificam se as relações de dependência são pertinentes ou não e modificam a mesma, adicionando e/ou removendo `arcos` e/ou UE_s/OE_s até a estrutura convergir a um modelo da AE que seja pertinente com a realidade do processo/planta.

Adicionalmente, observa-se que a estrutura da rede bayesiana, mostrada na Figura 151, representa uma distribuição de probabilidade conjunta na forma de árvore com os `arcos` que parte (saem) do ET (`nó` raiz) para as “consequências”. Portanto a estrutura na forma como está é interpretada como um diagrama da árvore de eventos (AE).

- **Etapa 6 - Integração dos modelos AF e AE**

Nesta etapa, procede-se à integração dos modelos de AF e AE. A integração destes modelos é obtida, tendo como elemento comum o evento topo (ET). A Figura 152 mostra o resultado da integração dos modelos e representa um cenário completo de acidente, dado o ET, baseado no diagrama de *bowtie*. Na Figura 152, o lado esquerdo do ET representa a árvore de falhas (AF) e o lado direito do ET representa a árvore de eventos (AE).

Figura 152 – Modelo de acidente resultante da integração dos modelos de AF e de AE.



Fonte: próprio autor

D.3 Fase 3 - Integração dos modelos de acidentes com HAZOP.

As atividades pertinentes a esta fase são descritas abaixo e baseadas no método ilustrado na Figura 37.

- **Obter o modelo de acidente para cada evento topo (ET)**

Neste exemplo considera-se apenas 1 evento topo (ET) e o modelo de acidente considerado é ilustrado na Figura 152.

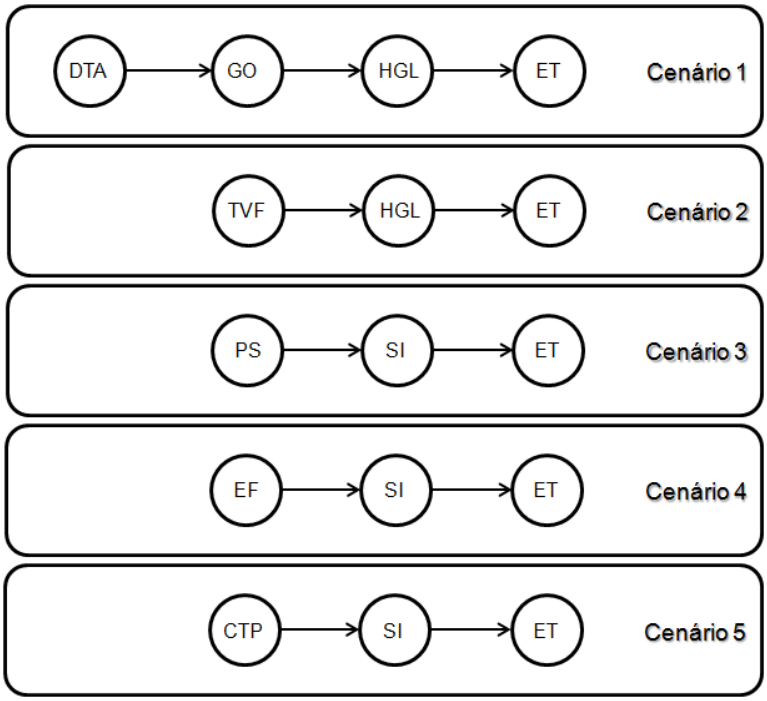
- **Identificar e separar a AF e AE de cada modelo**

A identificação da AF e da AE também é mostrada na Figura 152.

- **Identificar todos os cenários críticos da AF e AE**

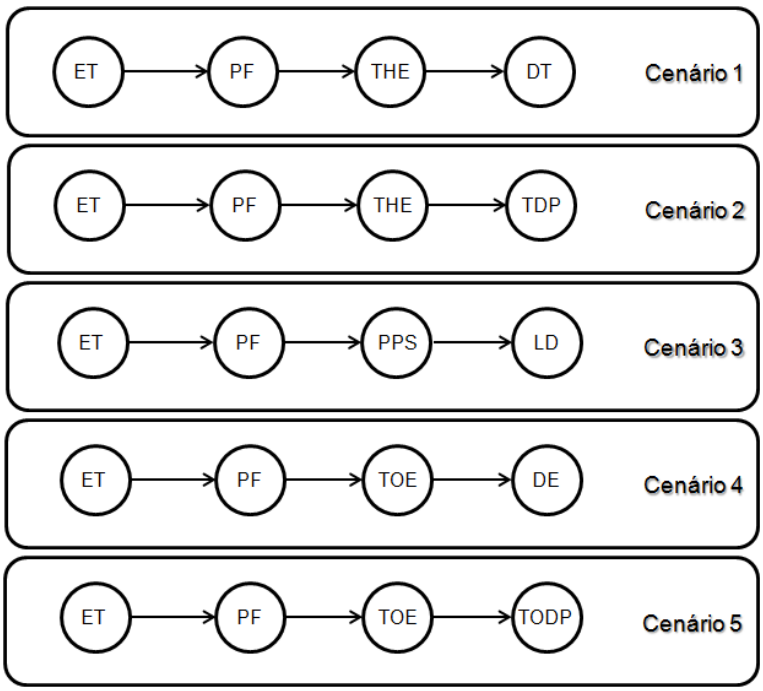
A Figura 153 mostra os cenários críticos pertinentes à árvore de falhas (AF). A Figura 154 mostra os cenários críticos pertinentes à árvore de eventos (AE).

Figura 153 – Cenários críticos pertinentes à AF.



Fonte: próprio autor

Figura 154 – Cenários críticos pertinentes à AE.

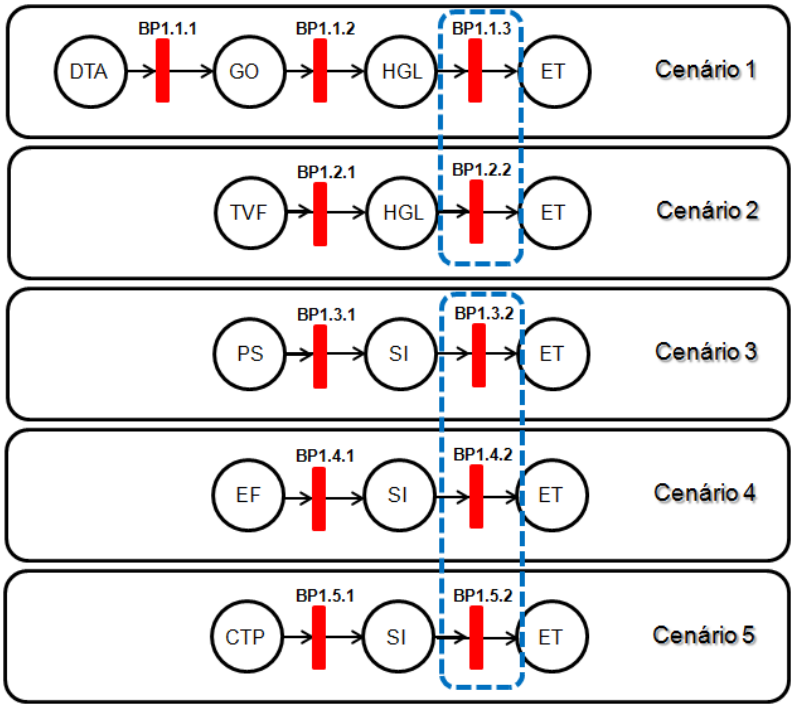


Fonte: próprio autor

- **Identificar as barreiras de prevenção e mitigação**

A Figura 155 mostra todas as barreiras de prevenção para cada cenário crítico da AF. Cada barreira é descrita por uma barra vermelha e representa uma função de segurança a ser executada pelo SCSP.

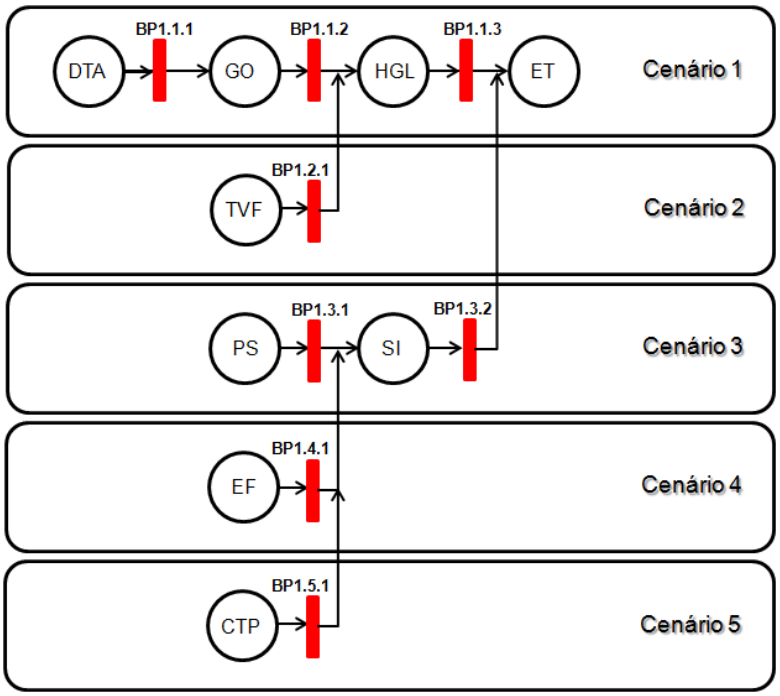
Figura 155 – Barreiras de prevenção



Fonte: próprio autor

Na Figura 155, as barreiras de prevenção BP1.1.3 e BP1.2.2 apresentam a mesma funcionalidade, e as barreiras de prevenção BP1.3.2, BP1.4.2 e BP1.5.2, também apresentam uma funcionalidade em comum. Neste contexto, considera-se apenas uma barreira para cada conjunto. A Figura 156 o diagrama resultante.

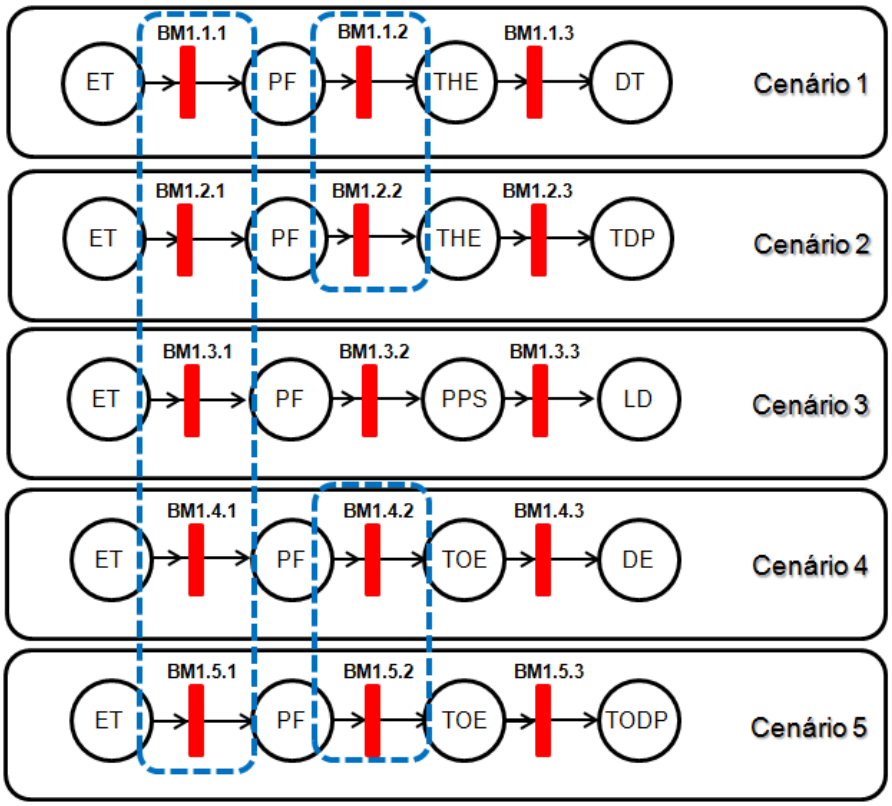
Figura 156 – Barreiras de prevenção



Fonte: próprio autor

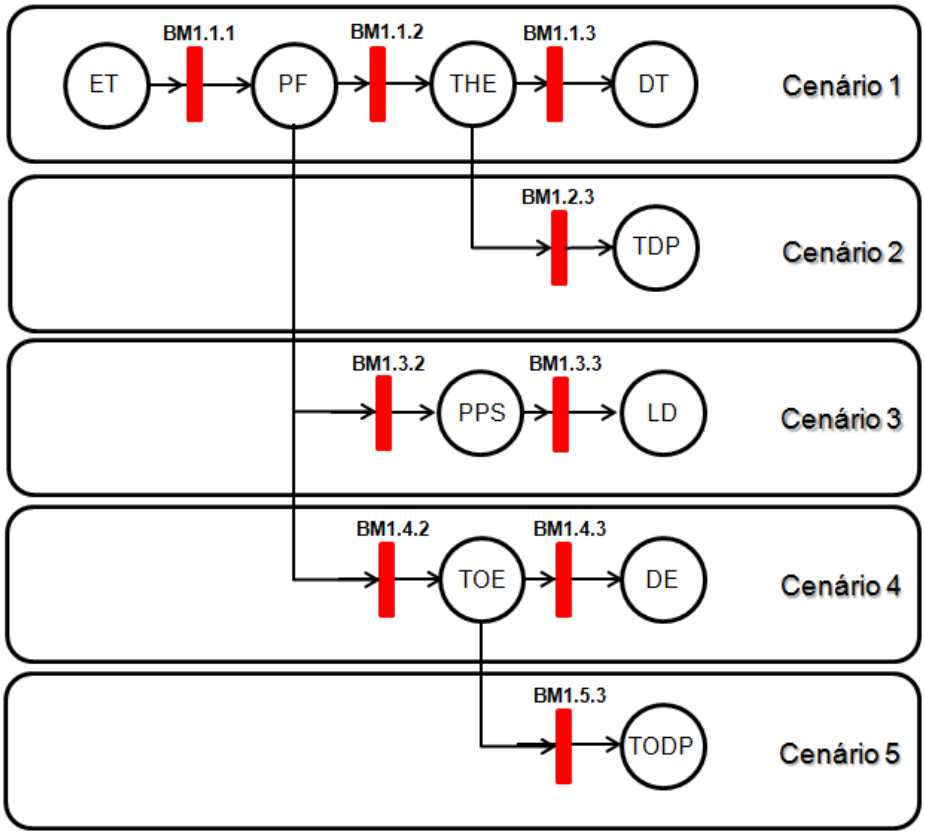
A Figura 157 mostra todas as barreiras de mitigação identificadas para cada cenário crítico da AE. Cada barreira é também descrita por uma barra vermelha e representa uma função de segurança a ser executada pelo SCSP. As barreiras de mitigação possuem o conjunto formado por BM1.1.1, BM1.2.1, BM1.3.1, BM1.4.1 e BM1.5.1, com uma mesma funcionalidade; e o conjunto de barreiras BM1.1.2 e BM1.2.2 uma segunda funcionalidade, e o conjunto de barreiras BM1.4.2 e BM1.5.2 uma terceira funcionalidade. A Figura 158 mostra o diagrama resultante da união de barreiras de mesma funcionalidade.

Figura 157 – Barreiras de mitigação



Fonte: próprio autor

Figura 158 – Barreiras de mitigação

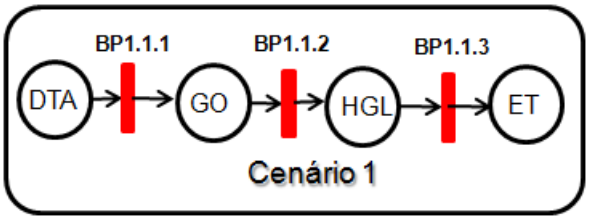


Fonte: próprio autor

- **Modelagem dos cenários críticos e barreiras em PFS**

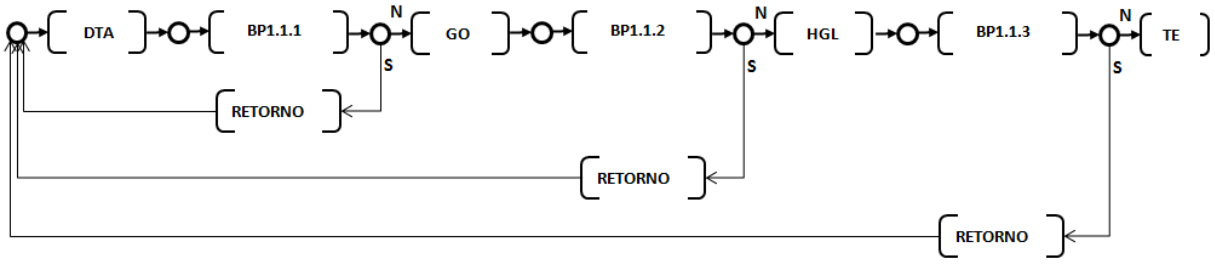
Com base na Figura 156, a Figura 159 ilustra o diagrama de barreiras do cenário crítico 1 e a Figura 160 ilustra o modelo em PFS correspondente.

Figura 159 – Diagrama de barreiras do cenário crítico 1



Fonte: próprio autor

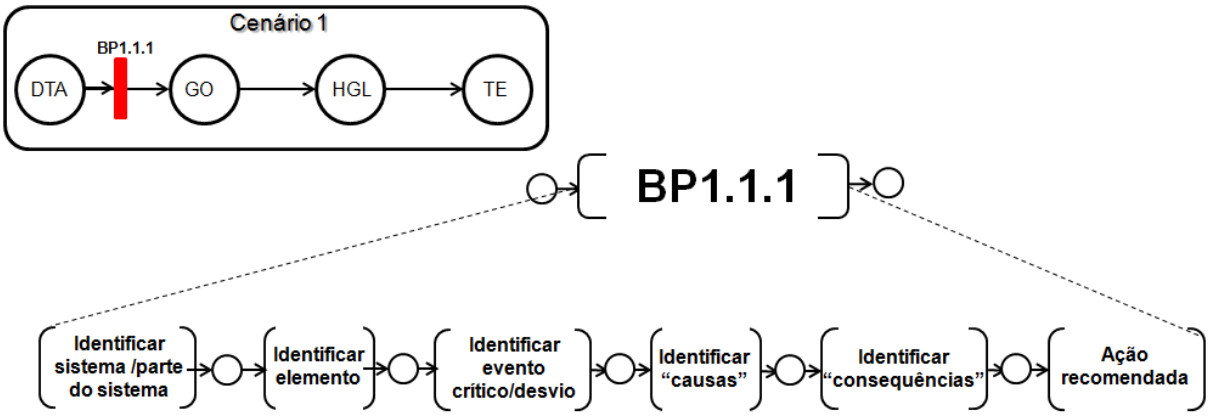
Figura 160 – Modelo de prevenção do cenário crítico 1 em PFS



Fonte: próprio autor

Cada `atividade` modelada em PFS associada a uma barreira de prevenção é refinada de forma a identificar as atividades pertinentes de cada barreira. As Figura 161 a Figura 163 mostram o refinamento das barreiras BP1.1.1 a BP1.1.3, respectivamente. As Tabela 40, Tabela 41 e Tabela 42, contém as informações de cada barreira respectivamente.

Figura 161 – Refinamento da BP1.1.1

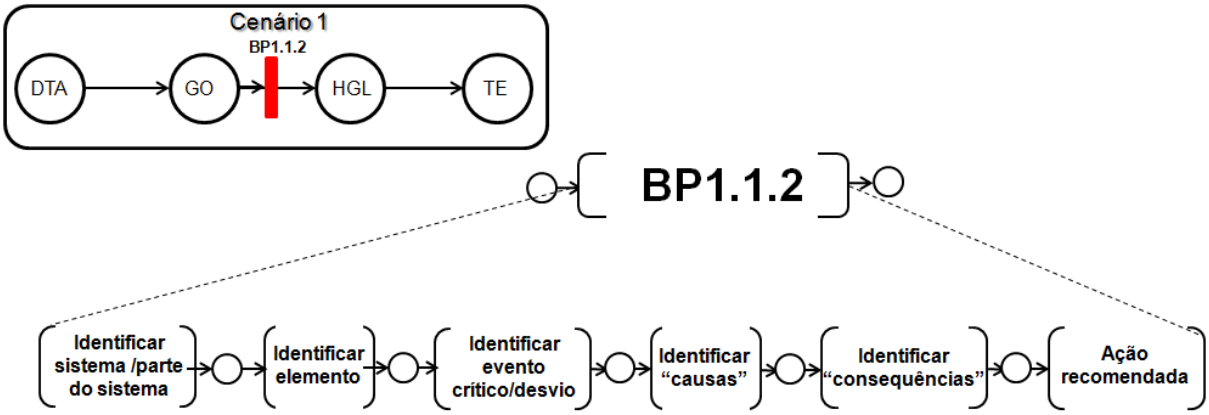


Fonte: próprio autor

Tabela 40 – Informações da BP1.1.1

Barreira	BP1.1.1
Sistema/parte do sistema	Pátio de carregamento dos caminhões tanque
Elemento	Tanque de combustível
Evento crítico/ desvio	Furo do tanque
Causa(s)	Falta de inspeção do tanque antes do procedimento de carregamento
Consequência(s)	Odor de gás provocado por vazamento do mesmo
Ações recomendadas	a) Elaborar plano de inspeção periódica dos tanques; b) Instalar sensores de gás no local onde o caminhão é estacionado para carregamento de hidrocarboneto c) Diagnosticar e sinalizar vazamento de gás
Equipamento(s)	a) SIS b) IHM
Sensor(es)	03 (três) sensores de gás
Atuador(es)	não se aplica

Figura 162 – Refinamento da BP1.1.2

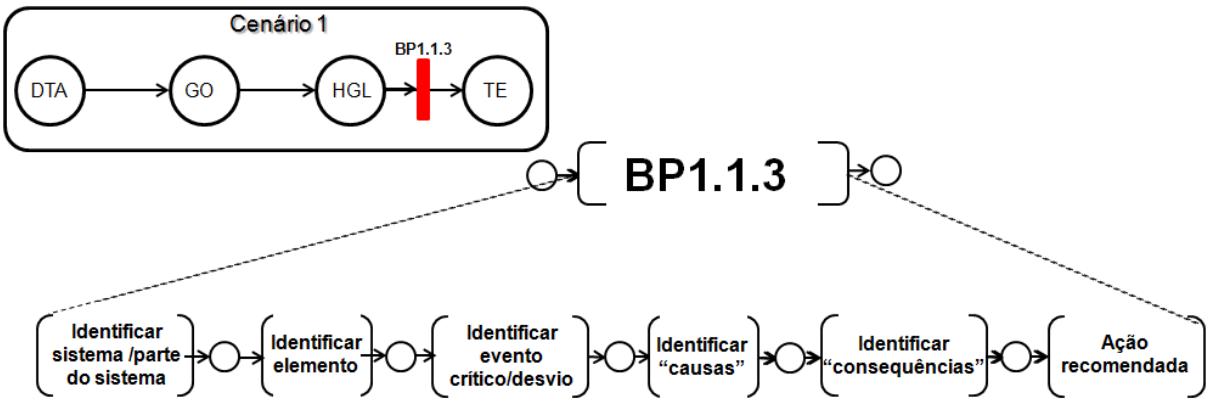


Fonte: próprio autor

Tabela 41 – Informações da BP1.1.2

Barreira	**BP1.1.2**
Sistema/parte do sistema	Pátio de carregamento dos caminhões tanque
Elemento	Tanque de combustível
Evento crítico/ desvio	Odor de gás
Causa(s)	Falha da barreira de prevenção BP1.1.1
Consequência(s)	Presença de gás no local de carregamento dos caminhões tanque
Ações recomendadas	a) Interromper o carregamento do tanque por meio do fechamento automático das válvulas de entrada de combustível no tanque.
Equipamento(s)	a) SIS b) IHM
Sensor(es)	03 (três) sensores de gás
Atuador(es)	Atuador de fechamento das válvulas de entrada de combustível no tanque

Figura 163 – Refinamento da BP1.1.3



Fonte: próprio autor

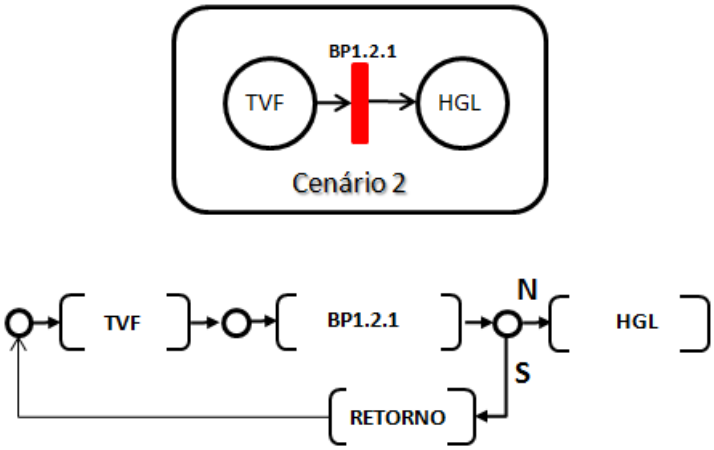
Tabela 42 – Informações da BP1.1.3

Barreira	BP1.1.3
Sistema/parte do sistema	Pátio de carregamento dos caminhões tanque

Elemento	Tanque de combustível
Evento crítico/ desvio	Vazamento de gás
Causa(s)	Falha da barreira de prevenção BP1.1.2
Consequência(s)	Incêndio
Ações recomendadas	a) Diagnosticar e sinalizar alarme de incêndio b) Alarmar sinal de evacuação da unidade de carregamento c) Alarmar sinal para acionamento da brigada de incêndio
Equipamento(s)	a) SIS b) IHM
Sensor(es)	Sensores de calor e fumaça
Atuador(es)	a) Buzina de evacuação da unidade de carregamento b) Buzina de acionamento da brigada de incêndio

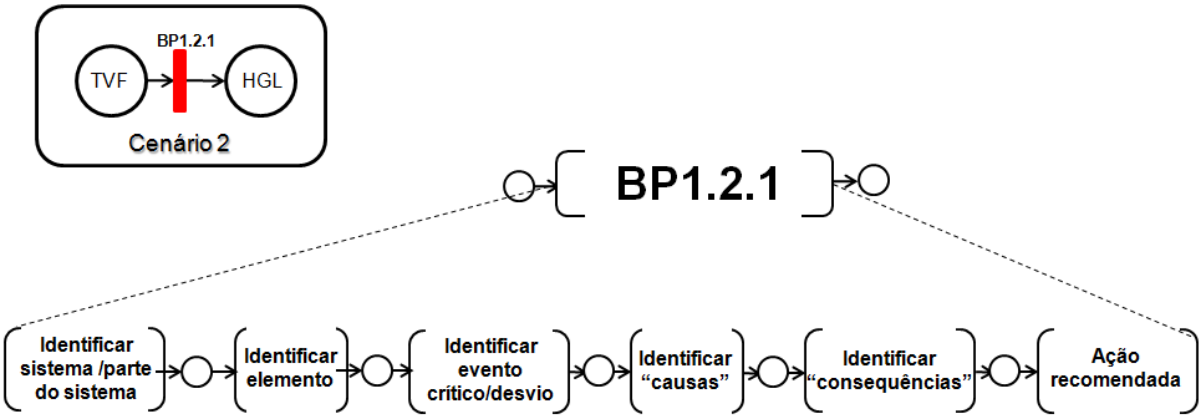
A Figura 164 mostra o modelo em PFS de prevenção do cenário crítico 2. A Figura 165 mostra o refinamento da BP1.2.1 e a Tabela 43, as informações desta barreira.

Figura 164 – Modelo de prevenção do cenário crítico 2 em PFS



Fonte: próprio autor

Figura 165 – Refinamento da BP1.2.1



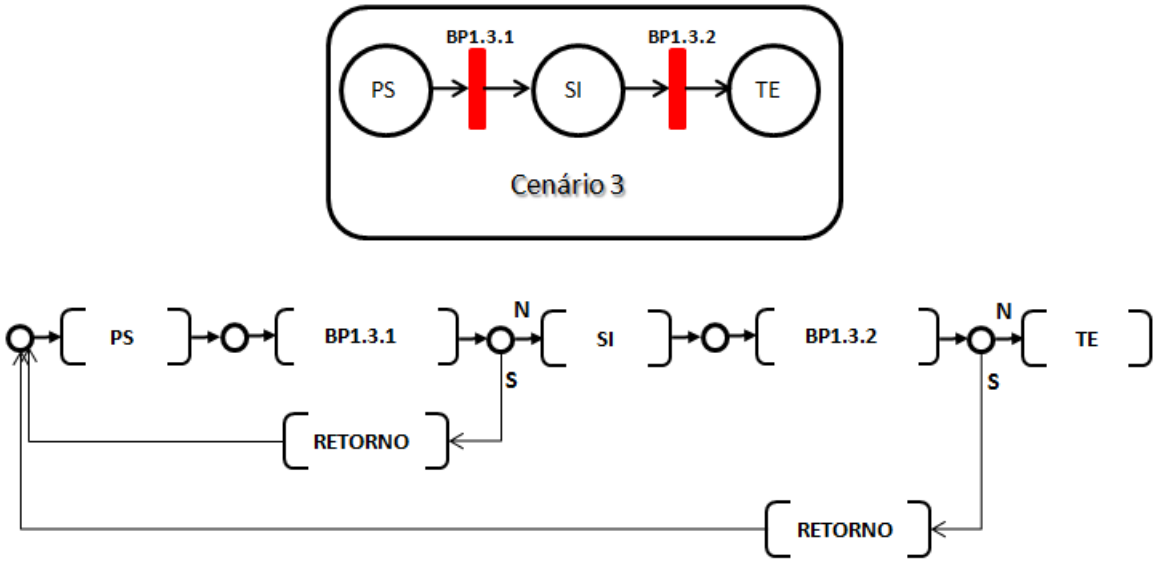
Fonte: próprio autor

Tabela 43 – Informações da BP1.2.1

Barreira	BP1.2.1
Sistema/parte do sistema	Pátio de carregamento dos caminhões tanque
Elemento	Válvula do tanque
Evento crítico/ desvio	Falha
Causa(s)	Desgaste mecânico
Consequência(s)	Presença de gás no local de carregamento dos caminhões tanque
Ações recomendadas	a) Diagnosticar e sinalizar falha da válvula do tanque b) Interromper o carregamento do tanque por meio do fechamento automático das válvulas de entrada de combustível no tanque
Equipamento(s)	a) SIS b) IHM
Sensor(es)	Sensor de falha da válvula
Atuador(es)	Atuador de fechamento das válvulas de entrada de combustível no tanque

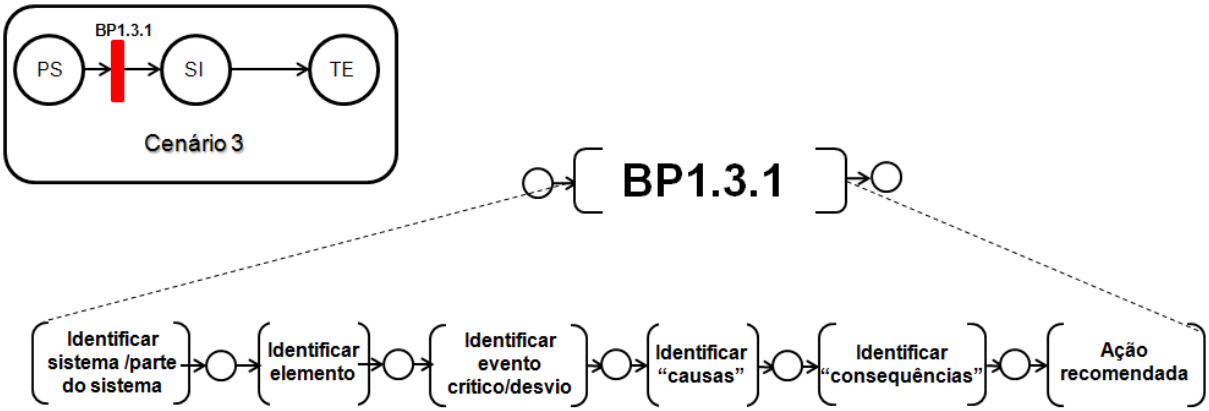
A Figura 166 mostra o modelo de prevenção do cenário crítico 3. As Figura 167 e Figura 168 mostram o refinamento das barreiras BP1.3.1 a BP1.3.2, respectivamente. As Tabela 44 e Tabela 45 apresentam as informações relacionadas a cada barreira do mesmo cenário.

Figura 166 – Modelo de prevenção do cenário crítico 3 em PFS



Fonte: próprio autor

Figura 167 – Refinamento da BP1.3.1

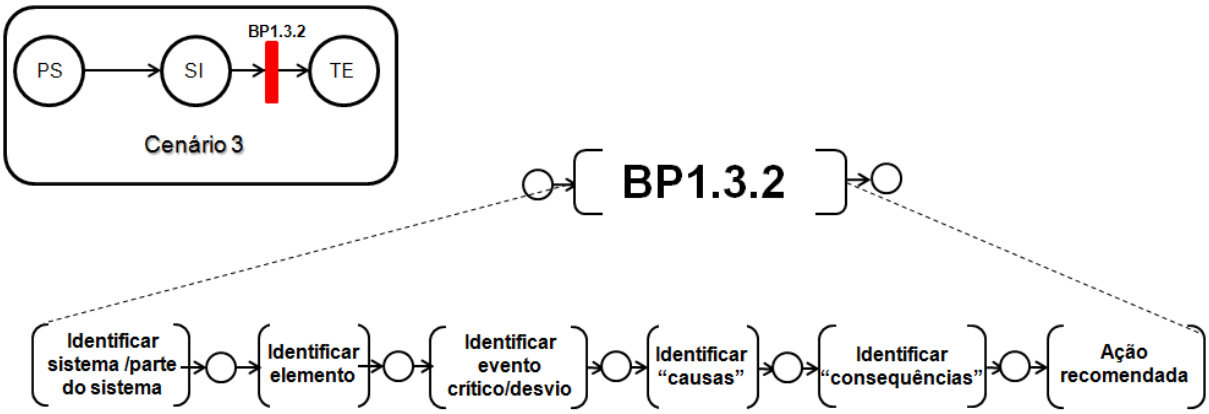


Fonte: próprio autor

Tabela 44 – Informações da BP1.3.1

Barreira	BP1.3.1
Sistema/parte do sistema	Pátio de carregamento dos caminhões tanque
Elemento	Tanque de combustível
Evento crítico/ desvio	faíscas
Causa(s)	a) motor do caminhão ligado b) equipamento elétrico energizado;
Consequência(s)	fonte de ignição com possibilidade de incêndio e explosão
Ações recomendadas	a) Sinalizar área proibida para fumantes e uso de celular; b) Diagnósticar e sinalizar presença de fumaça; c) Interromper o carregamento do tanque por meio do fechamento automático das válvulas de entrada de combustível no tanque
Equipamento(s)	a) SIS b) IHM
Sensor(es)	Sensores de fumaça
Atuador(es)	Atuador de fechamento das válvulas de entrada de combustível no tanque

Figura 168 – Refinamento da BP1.3.2



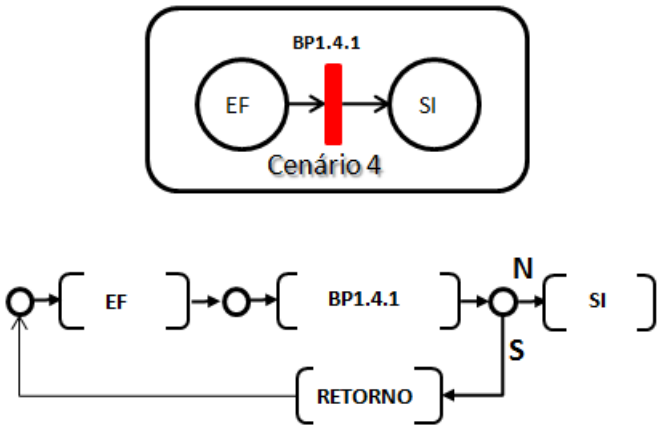
Fonte: próprio autor

Tabela 45 – Informações da BP1.3.2

Barreira	BP1.3.2
Sistema/parte do sistema	Pátio de carregamento dos caminhões tanque
Elemento	Tanque de combustível
Evento crítico/ desvio	Fonte de ignição
Causa(s)	Falha da barreira de prevenção BP1.3.1
Consequência(s)	Incêndio
Ações recomendadas	a) Diagnosticar e sinalizar alarme de incêndio b) Alarmar sinal de evacuação da unidade de carregamento c) Alarmar sinal para acionamento da brigada de incêndio
Equipamento(s)	a) SIS b) IHM
Sensor(es)	Sensores de calor e fumaça
Atuador(es)	c) Buzina de evacuação da unidade de carregamento d) Buzina de acionamento da brigada de incêndio

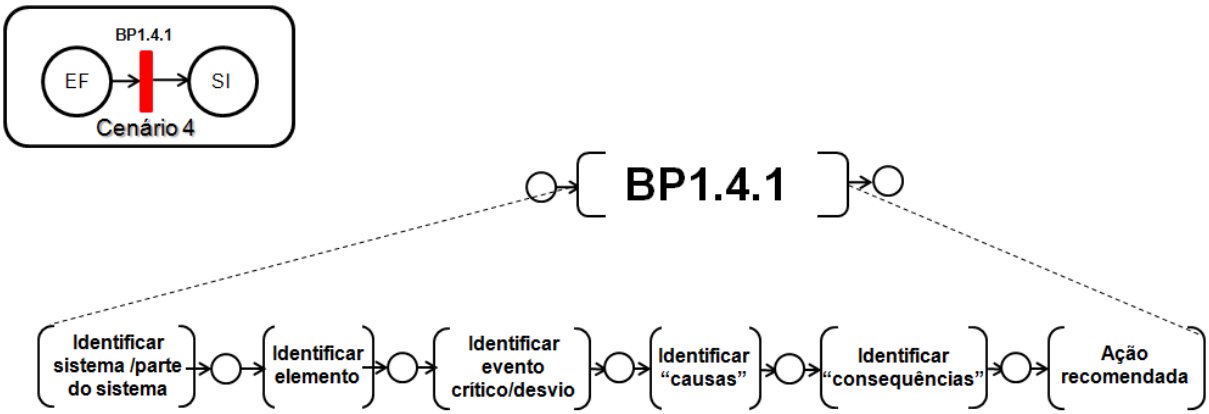
A Figura 169 mostra o modelo de prevenção do cenário crítico 4. A Figura 170 mostra o refinamento da barreira BP1.4.1 e a Tabela 46 as informações desta barreira.

Figura 169 – Modelo de prevenção do cenário crítico 4 em PFS



Fonte: próprio autor

Figura 170 – Refinamento da BP1.4.1



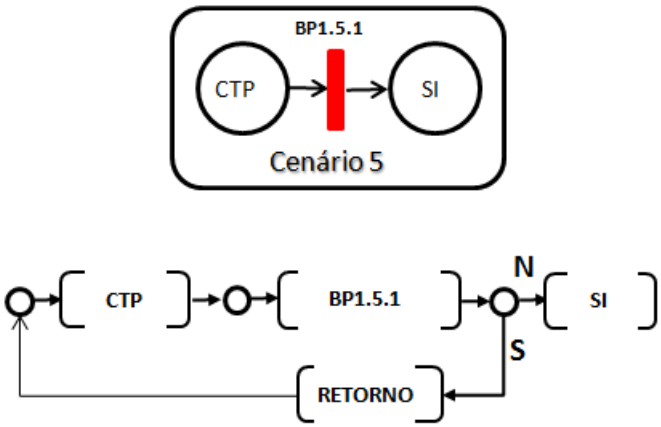
Fonte: próprio autor

Tabela 46 – Informações da BP1.4.1

Barreira	BP1.4.1
Sistema/parte do sistema	Pátio de carregamento dos caminhões tanque
Elemento	Exaustor
Evento crítico/ desvio	Falha do exaustor
Causa(s)	a) desgaste mecânico b) curto circuito na alimentação do exaustor
Consequência(s)	Fonte de ignição
Ações recomendadas	a) Elaborar plano de inspeção periódica do exaustor e circuito elétrico b) Diagnosticar e sinalizar falha do exaustor
Equipamento(s)	a) SIS b) IHM
Sensor(es)	Sensores do exaustor
Atuador(es)	não se aplica

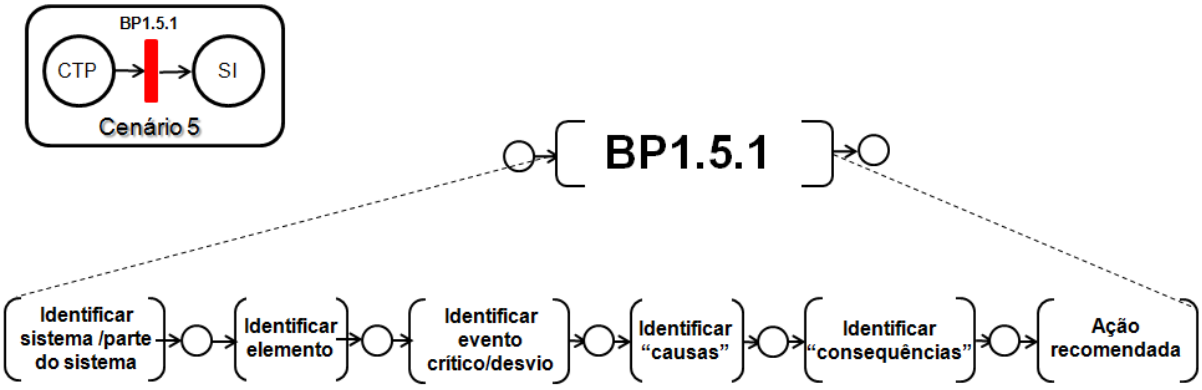
Finalmente, a Figura 171 mostra o modelo de prevenção do cenário crítico 5. A Figura 172 mostra o refinamento da barreira BP1.5.1 e a Tabela 47, as informações desta barreira.

Figura 171 – Modelo de prevenção do cenário crítico 5 em PFS



Fonte: próprio autor

Figura 172 – Refinamento da BP1.5.1



Fonte: próprio autor

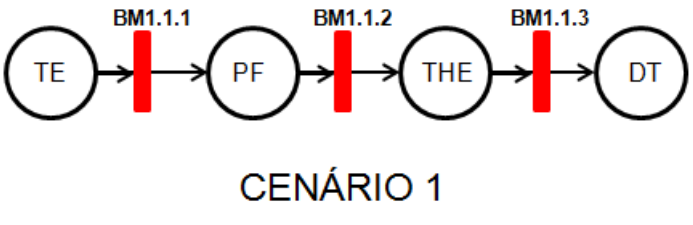
Tabela 47 – Informações da BP1.5.1

Barreira	BP1.5.1
Sistema/parte do sistema	Pátio de carregamento dos caminhões tanque
Elemento	Canteiro de obras
Evento crítico/ desvio	Equipamento elétrico energizado
Causa(s)	a) Canteiro de obras próximo ao pátio de carregamento de caminhões tanque (área classificada), b) Falta de orientação de uso de equipamentos durante procedimento de carregamento de combustível.
Consequência(s)	Fonte de ignição
Ações recomendadas	a) Elaborar plano para afastamento do canteiro de obras do pátio de carregamento de caminhões tanque, b) Sinalizar proibição de uso de equipamentos elétricos durante procedimento de carregamento de combustível c) Sinalizar alarme de equipamento elétrico energizado.
Equipamento(s)	a) SIS b) IHM
Sensor(es)	Sensores que detectam se o equipamento elétrico está ligado
Atuador(es)	não se aplica

Ainda na atividade de modelagem dos cenários críticos e barreiras em PFS, com base na Figura 158, são mostrados a seguir, os modelos de mitigação dos cenários 1 a 5; dado o mesmo evento topo (ET).

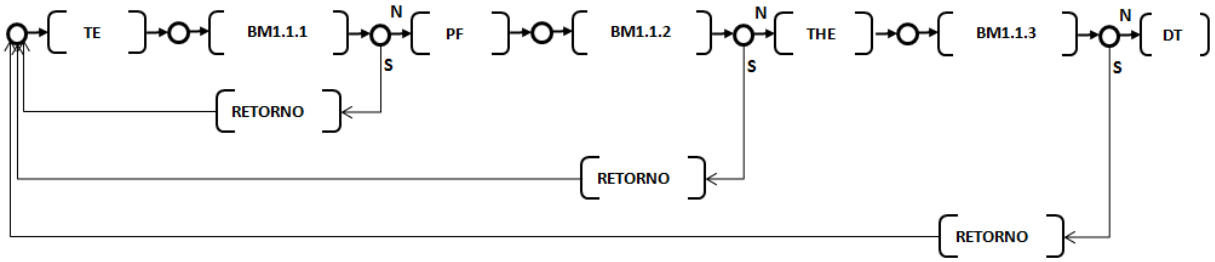
A Figura 173 mostra o diagrama de barreiras do cenário crítico 1 e a Figura 174 o modelo de mitigação do mesmo cenário em PFS. A seguir, as Figura 175 a Figura 177 mostram o refinamento das BM1.1.1, BM1.1.2 e BM1.1.3 respectivamente, e as informações relacionadas a cada barreira do mesmo cenário são apresentadas nas Tabela 48 a Tabela 50.

Figura 173 – Diagramas de barreiras do cenário crítico 1



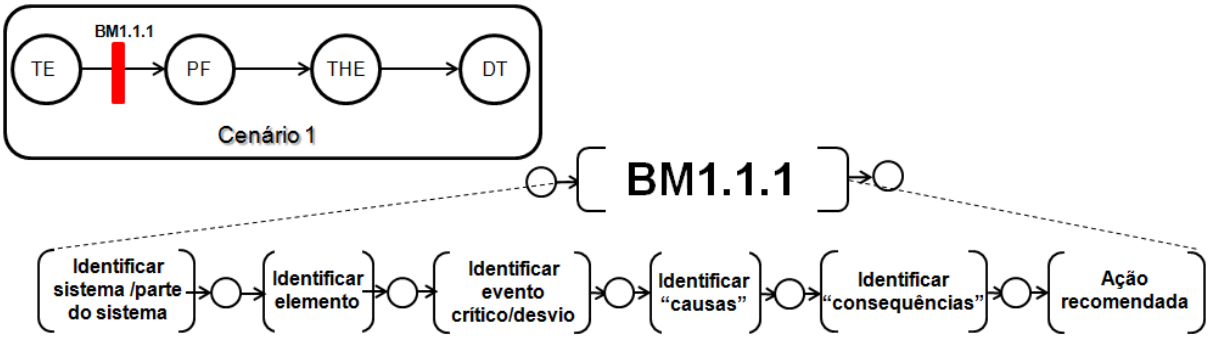
Fonte: próprio autor

Figura 174 – Modelo de mitigação do cenário crítico 1 em PFS



Fonte: próprio autor

Figura 175 – Refinamento da BM1.1.1

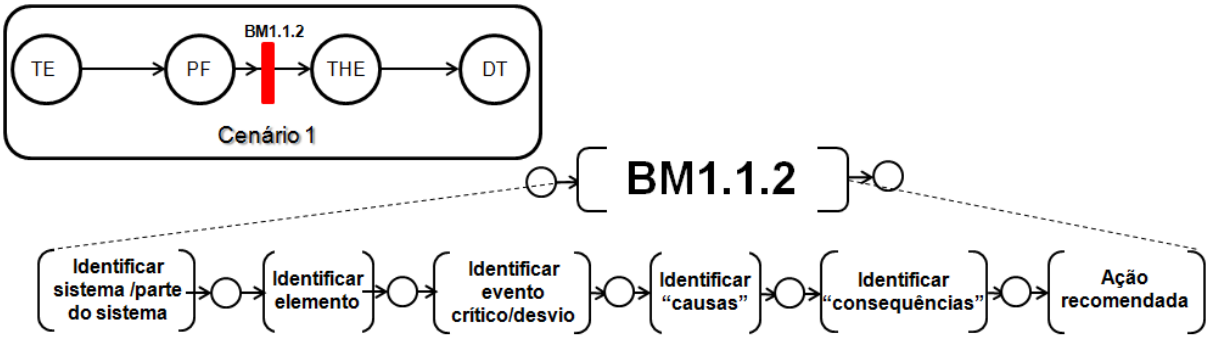


Fonte: próprio autor

Tabela 48 – Informações da BM1.1.1

Barreira	BM1.1.1
Sistema/parte do sistema	Pátio de carregamento dos caminhões tanque
Elemento	não se aplica
Evento crítico/ desvio	Incêndio e explosão
Causa(s)	Falhas das barreiras de prevenção BP1.1.3 e BP1.3.2
Consequência(s)	Piscina de fogo
Ações recomendadas	a) Diagnosticar e sinalizar incêndio b) Acionar brigada de incêndio c) Combater incêndio d) Alarmar evacuação da pátio de carregamento dos caminhões tanque
Equipamento(s)	a) SIS b) IHM
Sensor(es)	Sensores de fumaça e calor
Atuador(es)	a) Buzina para alarme sonoro de evacuação do pátio de carregamento; b) Buzina para alarme de brigada de incêndio

Figura 176 – Refinamento da BM1.1.2

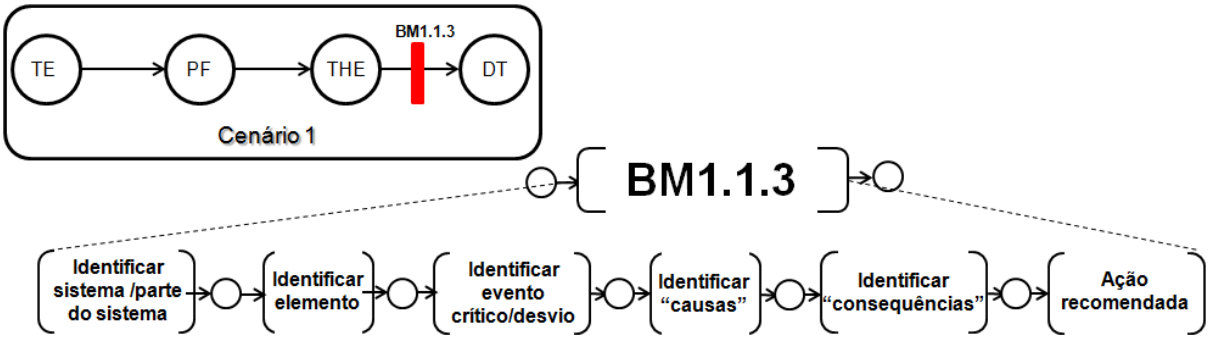


Fonte: próprio autor

Tabela 49 – Informações da BM1.1.2

Barreira	BM1.1.2
Sistema/parte do sistema	Pátio de carregamento dos caminhões tanque
Elemento	não se aplica
Evento crítico/ desvio	piscina de fogo
Causa(s)	Falha da barreira de mitigação BM1.1.1
Consequência(s)	Danos térmicos provocados por elevação de temperatura
Ações recomendadas	a) Diagnosticar e sinalizar incêndio b) Acionar brigada de incêndio c) Combater incêndio d) Alarmar evacuação da pátio de carregamento dos caminhões tanque
Equipamento(s)	a) SIS b) IHM
Sensor(es)	Sensores de fumaça e calor
Atuador(es)	a) Buzina para alarme sonoro de evacuação da unidade de ISOM; b) Buzina para alarme de brigada de incêndio

Figura 177 – Refinamento da BM1.1.3



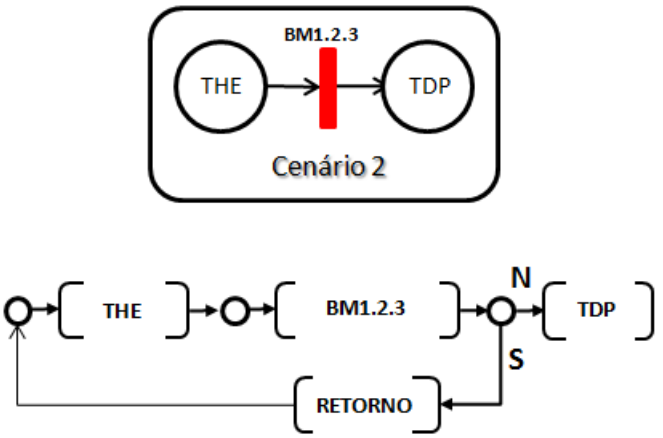
Fonte: próprio autor

Tabela 50 – Informações da BM1.1.3

Barreira	BM1.1.3
Sistema/parte do sistema	Pátio de carregamento dos caminhões tanque
Elemento	não se aplica
Evento crítico/ desvio	Efeitos térmicos
Causa(s)	Falha da barreira de mitigação BM1.1.2
Consequência(s)	Danos a outros caminhões
Ações recomendadas	a) Diagnosticar e sinalizar incêndio b) Acionar brigada de incêndio c) Combater incêndio d) Alarmar evacuação da pátio de carregamento dos caminhões tanque
Equipamento(s)	a) SIS b) IHM
Sensor(es)	Sensores de fumaça e calor
Atuador(es)	a) Buzina para alarme sonoro de evacuação da unidade de ISOM; b) Buzina para alarme de brigada de incêndio

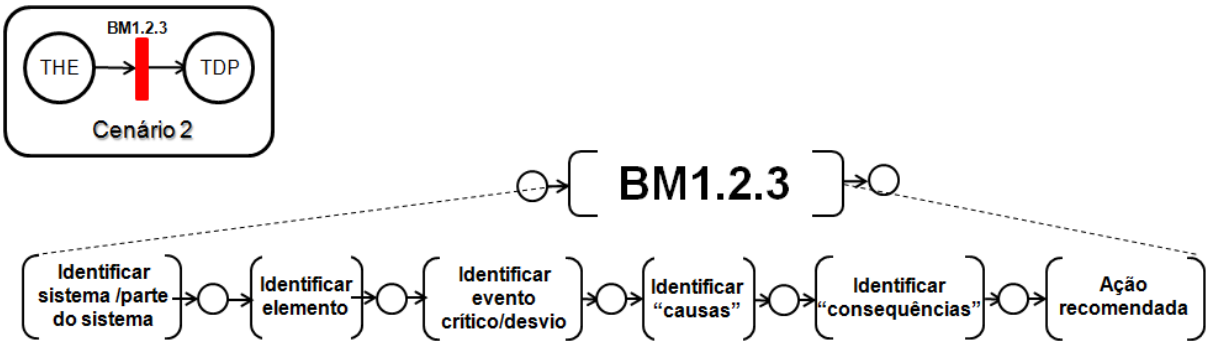
Com relação ao cenário crítico 2, a Figura 178 mostra o modelo de mitigação deste cenário em PFS. A seguir, a Figura 179 mostra o refinamento da barreira de mitigação denominada BM1.2.3, e a Tabela 51, as informações desta barreira.

Figura 178 – Modelo de mitigação do cenário crítico 2 em PFS



Fonte: próprio autor

Figura 179 – Refinamento da BM1.2.3



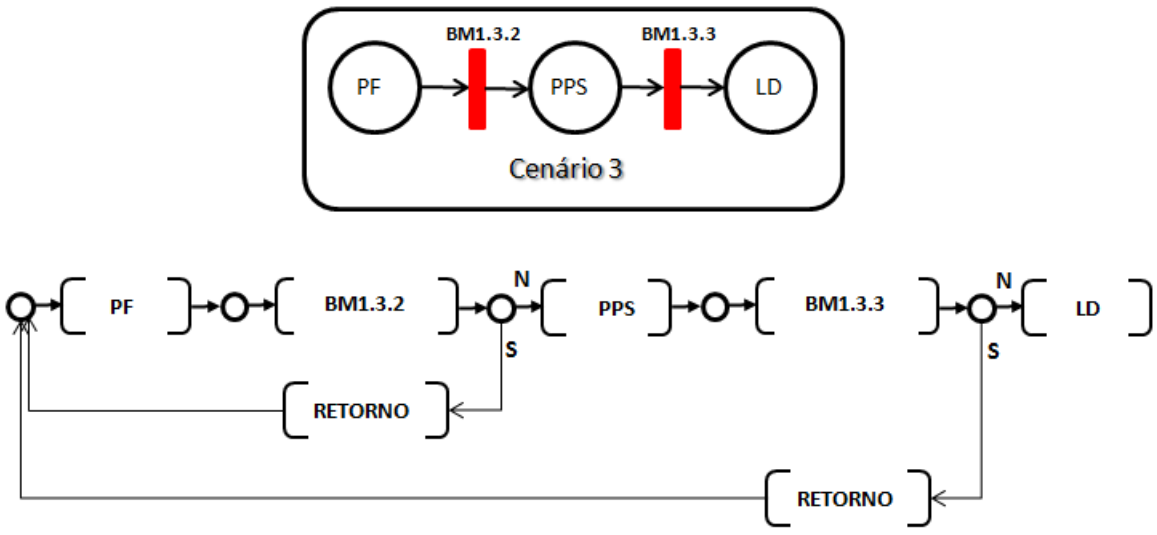
Fonte: próprio autor

Tabela 51 – Informações da BM1.2.3

Barreira	BM1.2.3
Sistema/parte do sistema	Pátio de carregamento dos caminhões tanque
Elemento	não se aplica
Evento crítico/ desvio	Efeito térmico provocado pela elevação de temperatura
Causa(s)	Falha da barreira de mitigação BM1.1.2
Consequência(s)	Danos térmicos às pessoas
Ações recomendadas	a) Diagnosticar e sinalizar incêndio b) Acionar brigada de incêndio c) Combater incêndio d) Alarmar evacuação da pátio de carregamento dos caminhões tanque
Equipamento(s)	a) SIS b) IHM
Sensor(es)	Sensores de fumaça e calor
Atuador(es)	a) Buzina para alarme sonoro de evacuação do pátio de carregamento; b) Buzina para alarme de brigada de incêndio

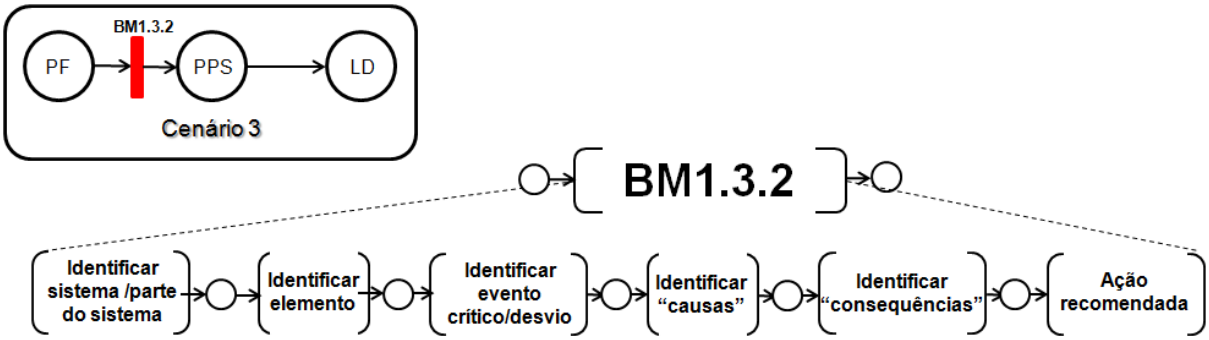
Com relação ao cenário crítico 3, a Figura 180 mostra o modelo de mitigação deste cenário em PFS. A seguir as Figura 181 e Figura 182 mostram o refinamento das barreiras de mitigação denominadas BM1.3.2 e BM1.3.3 respectivamente, e as Tabela 52 e Tabela 53, as informações obtidas para cada barreira de mitigação do mesmo cenário.

Figura 180 – Modelo de mitigação do cenário crítico 3 em PFS



Fonte: próprio autor

Figura 181 – Refinamento da BM1.3.2

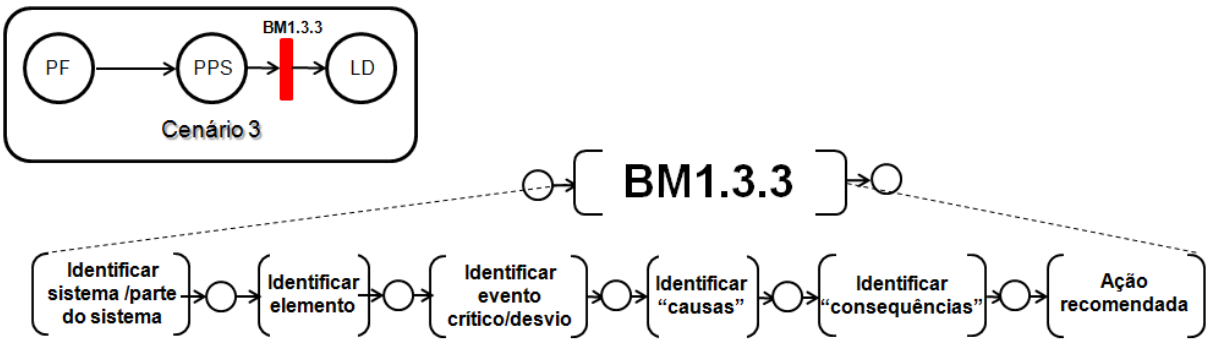


Fonte: próprio autor

Tabela 52 – Informações da BM1.3.2

Barreira	BM1.3.2
Sistema/parte do sistema	Pátio de carregamento dos caminhões tanque
Elemento	não se aplica
Evento crítico/ desvio	Piscina de fogo
Causa(s)	Falha da barreira de mitigação BM1.1.1
Consequência(s)	Degeneração do sistema produtivo
Ações recomendadas	a) Diagnosticar e sinalizar incêndio b) Acionar brigada de incêndio c) Combater incêndio d) Alarmar evacuação da pátio de carregamento dos caminhões tanque
Equipamento(s)	a) SIS b) IHM
Sensor(es)	Sensores de fumaça e calor
Atuador(es)	a) Buzina para alarme sonoro de evacuação do pátio de caminhões; b) Buzina para alarme de brigada de incêndio

Figura 182 – Refinamento da BM1.3.3.



Fonte: próprio autor

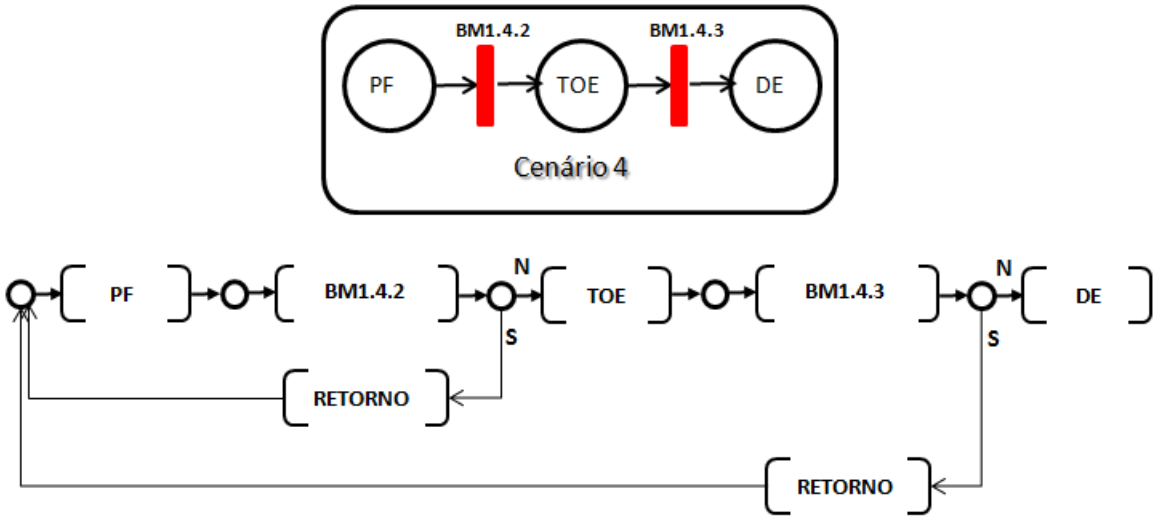
Tabela 53 – Informações da BM1.3.3

Barreira	BM1.3.3
Sistema/parte do sistema	Pátio de carregamento dos caminhões tanque
Elemento	Sistema produtivo
Evento crítico/	Degeneração do sistema produtivo

desvio	
Causa(s)	Falha da barreira de mitigação BM1.3.2
Consequência(s)	Atraso na cadeia de suprimento
Ações recomendadas	a) Diagnosticar e sinalizar incêndio b) Acionar brigada de incêndio c) Combater incêndio d) Alarmar evacuação da pátio de carregamento dos caminhões tanque
Equipamento(s)	a) SIS b) IHM
Sensor(es)	Sensores de fumaça e calor
Atuador(es)	a) Buzina para alarme sonoro de evacuação do pátio de caminhões; b) Buzina para alarme de brigada de incêndio

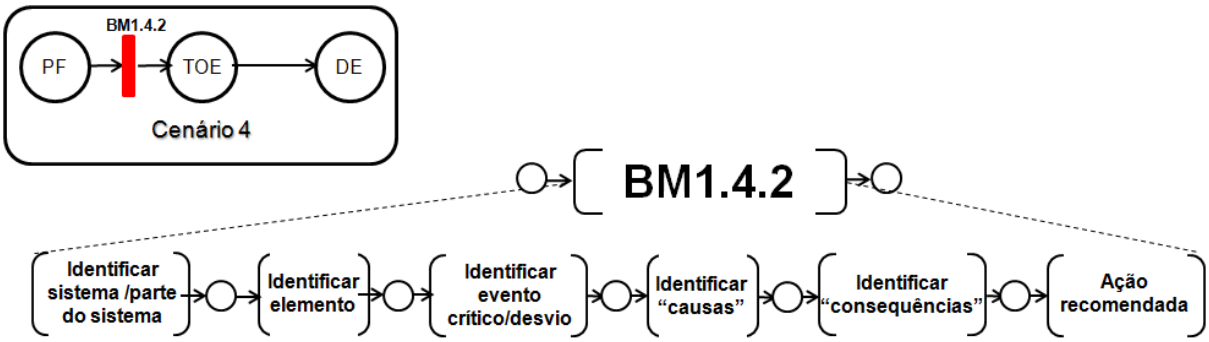
Com relação ao cenário crítico 4, a Figura 183 mostra o modelo de mitigação deste cenário em PFS. A seguir, as Figura 184 e Figura 185 mostram o refinamento das barreiras de mitigação denominadas BM1.4.2 e BM1.4.3 respectivamente, e as Tabela 54 e Tabela 55, as informações obtidas para cada barreira do mesmo cenário.

Figura 183 – Modelo de mitigação do cenário crítico 4 em PFS



Fonte: próprio autor

Figura 184 – Refinamento da BM1.4.2

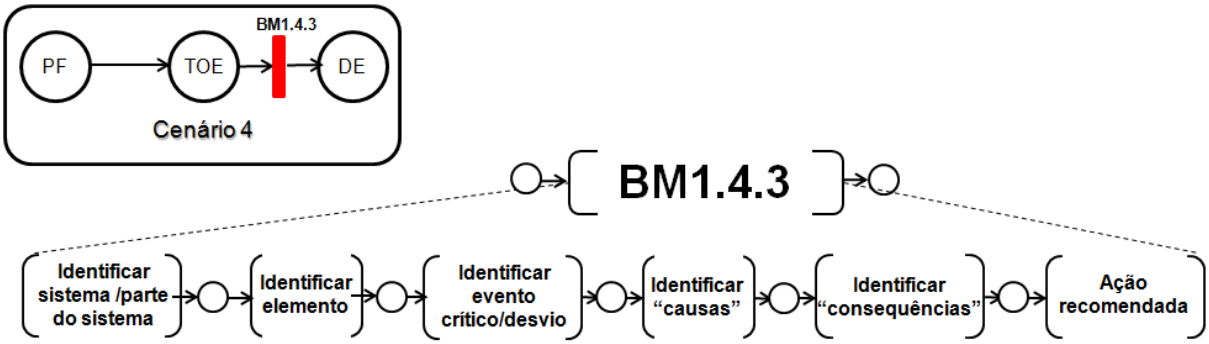


Fonte: próprio autor

Tabela 54 – Informações da BM1.4.2

Barreira	BM1.4.2
Sistema/parte do sistema	Pátio de carregamento dos caminhões tanque
Elemento	não se aplica
Evento crítico / desvio	Piscina de fogo
Causa(s)	Falha da barreira de mitigação BM1.1.1
Consequência(s)	Efeitos tóxicos provocados por fumaça tóxica
Ações recomendadas	a) Diagnosticar e sinalizar incêndio b) Acionar brigada de incêndio c) Combater incêndio d) Alarmar evacuação da pátio de carregamento dos caminhões tanque
Equipamento(s)	a) SIS b) IHM
Sensor(es)	Sensores de fumaça e calor
Atuador(es)	c) Buzina para alarme sonoro de evacuação do pátio de carregamento de caminhões; d) Buzina para alarme de brigada de incêndio

Figura 185 – Refinamento da BM1.4.3



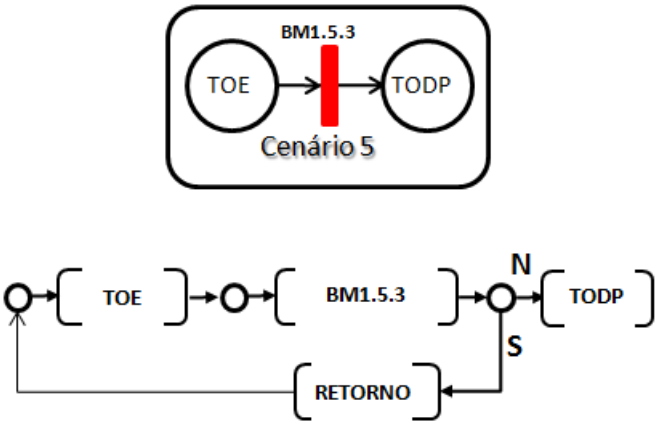
Fonte: próprio autor

Tabela 55 – Informações da BM1.4.3

Barreira	BM1.4.3
Sistema/parte do sistema	Pátio de carregamento dos caminhões tanque
Elemento	não se aplica
Evento crítico/ desvio	Efeitos tóxicos provocados por fumaça tóxica
Causa(s)	Falha da barreira de mitigação BM1.4.2
Consequência(s)	Danos ao meio ambiente
Ações recomendadas	a) Diagnosticar e sinalizar fumaça tóxica b) Planejar evacuação de pessoas das comunidades vizinhas
Equipamento(s)	a) SIS b) IHM
Sensor(es)	Sensores de fumaça
Atuador(es)	não se aplica

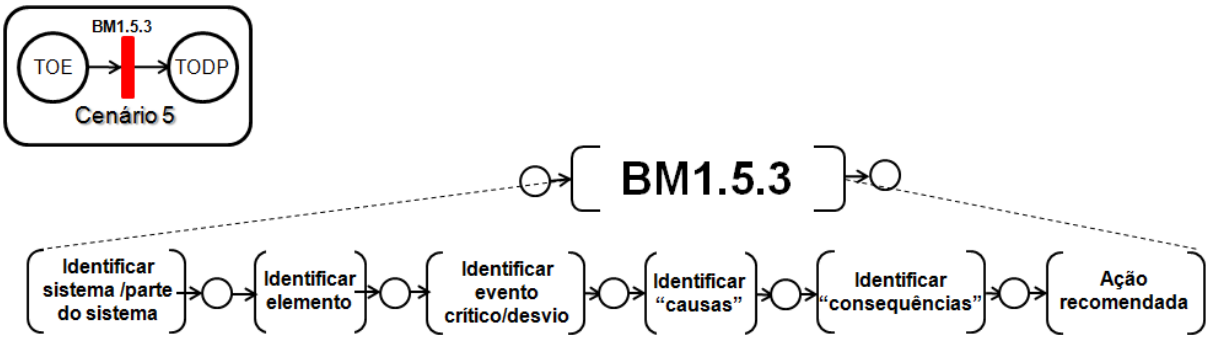
Finalmente, com relação ao cenário crítico 5, a Figura 186 mostra o modelo de mitigação deste cenário em PFS. A Figura 187 mostra o refinamento da barreira de mitigação BM1.5.3, e a Tabela 56, as informações desta barreira.

Figura 186 – Modelo de mitigação do cenário crítico 5 em PFS



Fonte: próprio autor

Figura 187 – Refinamento da BM1.5.3



Fonte: próprio autor

Tabela 56 – Informações da BM1.5.3

Barreira	BM1.5.3
Sistema/parte do sistema	Pátio de carregamento dos caminhões tanque
Elemento	não se aplica
Evento crítico/ desvio	Efeitos tóxicos provocados por fumaça tóxica
Causa(s)	Falha da barreira de mitigação BM1.4.2
Consequência(s)	Danos tóxicos às pessoas
Ações recomendadas	c) Diagnosticar e sinalizar fumaça tóxica d) Planejar evacuação de pessoas das comunidades vizinhas
Equipamento(s)	c) SIS d) IHM
Sensor(es)	Sensores de fumaça
Atuador(es)	não se aplica

- **Preenchimento da Tabela de HAZOP**

Nesta atividade, as informações das barreiras de prevenção e mitigação, obtidas para todos os cenários críticos modelados, são utilizadas para o preenchimento da Tabela de HAZOP. Os resultados desta etapa, ou seja, as Tabelas de HAZOP resultantes estão mostradas no Apêndice F deste trabalho.

D.4 Fase 4 – Geração dos algoritmos de defesa de prevenção e mitigação de falhas críticas.

O cenário completo (*bowtie*) deste acidente para o evento topo ET é representado via diagrama de barreiras na Figura 156 (diagrama de barreiras de prevenção) e na Figura 158 (diagrama de barreiras de mitigação).

A seguir com o procedimento proposto, tem-se a geração dos algoritmos de defesa de prevenção e mitigação de falhas críticas.

APÊNDICE E – TABELA DE HAZOP DO EXEMPLO DE APLICAÇÃO 1

Neste apêndice são apresentadas as Tabelas de HAZOP do primeiro exemplo de aplicação mostrado no capítulo 4.

A Tabela 57 mostra o HAZOP considerando as barreiras de prevenção de eventos críticos a partir do modelo de acidente da Figura 58. Adicionalmente, a Tabela 58 mostra o HAZOP considerando as barreiras de mitigação de eventos críticos do mesmo modelo de acidente.

Sistema / parte do sistema: Unidade de isomerização (ISOM) / Torre de isomerização

Tabela 57 – HAZOP: barreiras de prevenção

Barreira	Elemento	Evento Crítico / Desvio	Causa(s)	Consequência(s)	Ação	Equipamentos	Sensores	Atuadores
BP 1.1.1	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
BP 1.6.1	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
BP 1.6.2	Sensor de nível alto de refinado	Falha de alarme de nível	Falha da barreira de prevenção BP1.6.1	Falhas LICA	Fechar automaticamente a válvula de alimentação de refinado na torre de ISOM	a) SIS b) IHM	não se aplica	Atuador para fechamento da válvula de alimentação de refinado na torre de ISOM.
BP 1.6.3	Sensor de nível alto de refinado	Falhas LICA	Falha da barreira de prevenção BP1.6.2	Excesso de alimentação na torre de ISOM	Degenerar de forma controlada a torre de ISOM	a) SIS b) IHM	não se aplica	Comandos de “parada” de forma controlada da torre de isomerização.
BP 1.6.4	Refinado	Excesso de alimentação dentro da torre de ISOM	Falha da barreira de porevenção BP1.6.3.	Nível de refinado acima no nível máximo permitido	Degenerar de forma controlada a torre de ISOM	a) SIS b) IHM	não se aplica	Comandos de “parada” de forma controlada da torre de isomerização.

Sistema / parte do sistema: Unidade de isomerização (ISOM) / Torre de isomerização

Barreira	Elemento	Evento Crítico / Desvio	Causa(s)	Consequência(s)	Ação	Equipamentos	Sensores	Atuadores
BP 1.7.1	Sensor 2 de nível alto de refinado	Falha do sensor 2	a) Falha do sensor 2 b) Erro na calibração c) Falha na alimentação do sensor 2	Falha de alarme de nível	a) Diagnosticar e sinalizar falha do sensor 2 b) Diagnosticar e sinalizar erro de calibração do sensor 2 c) Diagnosticar e sinalizar falha na alimentação do sensor 2	a) SIS b) IHM	não se aplica	não se aplica
BP 1.8.1	Transmissor de nível (LT-1)	Falha na leitura do transmissor de nível (LT-1)	a) Erro na calibração do transmissor b) Falha no sistema de alimentação elétrica do transmissor	Falhas LICA	a) Diagnosticar e sinalizar erro na calibração do sensor b) Diagnosticar e sinalizar falha no sistema de alimentação elétrica do transmissor c) Fechar automaticamente a válvula de alimentação de refinado na entrada da torre de ISOM	a) SIS b) IHM	não se aplica	Atuador de fechamento da válvula de alimentação de refinado na entrada da torre de ISOM

Sistema / parte do sistema: Unidade de isomerização (ISOM) / Sala de Controle

Barreira	Elemento	Evento Crítico / Desvio	Causa(s)	Consequência(s)	Ação	Equipamentos	Sensores	Atuadores
BP 1.9.1	Sensor 1 de nível alto de refinado na torre de ISOM	Alarme de nível alto 1 ignorado pelo operador	a) Falha na gestão de riscos b) Falta de treinamento do(s) operadore(s)	Falha na operação da unidade de isomerização	a) Fechar automaticamente a válvula de alimentação da torre de ISOM b) Planejar e implementar um sistema de gestão de riscos c) Planejar e implementar treinamentos de operação e riscos da unidade de isomerização	a) SIS b) IHM	não se aplica	Atuador de fechamento da válvula de alimentação de refinado na entrada da torre de ISOM
BP 1.9.2	Refinado	Falha na operação da unidade de isomerização	Falha da barreira de prevenção BP1.9.1	Excesso de alimentação da torre de ISOM	a) Fechar automaticamente a válvula de alimentação da torre de ISOM	a) SIS b) IHM	não se aplica	Atuador de fechamento da válvula de alimentação de refinado na entrada da torre de ISOM
BP 1.10.1	Sensor de temperatura	Alarme de temperatura alta de refinado dentro da torre de ISOM ignorado pelo operador	a) Falha na gestão de riscos b) Falta de treinamento do(s) operadore(s)	Falha na operação da unidade de isomerização	a) Fechar automaticamente a válvula de alimentação da torre de ISOM b) Abrir válvula inferior da torre de ISOM para redução do nível e da temperatura c) Ligar bomba inferior d) Planejar e implementar um sistema de gestão de riscos e) Planejar e implementar treinamentos de operação e riscos da unidade de ISOM.	a) SIS b) IHM	não se aplica	a) Atuador de fechamento da válvula de alimentação de refinado na entrada da torre de ISOM b) Atuador de abertura da válvula inferior da torre de ISOM c) Contator de partida/parada da bomba inferior

Sistema / parte do sistema: Unidade de isomerização (ISOM) / Tanque de *blowdown*

Barreira	Elemento	Evento Crítico / Desvio	Causa(s)	Consequência(s)	Ação	Equipamentos	Sensores	Atuadores
BP 1.1.2	Tanque de blowdown	Excesso de alimentação de refinado	Falha da barreira de prevenção BP1.1.1.	Provável lançamento de vapores de hidrocarboneto (HC) na atmosfera	a) Instalar três sensores de nível alto no tanque de blowdown b) Diagnosticar e sinalizar alarme de nível alto no tanque de blowdonw, via algoritmo de votação 2oo3 c) Degenerar a unidade de isomerização de forma controlada	a) SIS b) IHM	Sensores de nível	Comandos de "parada" de forma controlada dos elementos da unidade de ISOM.
BP 1.2.1	Válvula V-6	Falha na abertura da válvula	a) Desgaste mecânico b) Falha do atuador	Elevação de nível de refinado no tanque	a) Instalar sensores de posição (aberta / fechada) na válvula V-6 b) Diagnosticar e sinalizar falha de fechamento da válvula V-6	a) SIS b) IHM	a) Chave fim de curso de válvula aberta b) Chave fim de curso de válvula fechada	não se aplica
BP 1.3.1	Sensor de nível	Falha de alarme de nível alto de refinado	a) Falha do sensor b) Erro na calibração do sensor c) Falha na alimentação do sensor	Elevação de nível de refinado no tanque	a) Instalar três sensores de nível alto de refinado b) Diagnosticar e sinalizar alarme de nível alto via algoritmo de votação 2oo3	a) SIS b) IHM	Sensores de nível	não se aplica
BP 1.4.2	Refinado	Excesso de alimentação de refinado no tanque	Falha da barreira de prevenção BP1.4.1	Nível de refinado acima do nível máximo permitido	a) Instalar três sensores de nível no tanque b) Diagnosticar e sinalizar alarme de nível alto via algoritmo de votação 2oo3.	a) SIS b) IHM	Sensores de nível denominados de LSH1, LSH2 e LSH3.	não se aplica

Sistema / parte do sistema: Unidade de isomerização (ISOM) / Tanque de *blowdown*

Barreira	Elemento	Evento Crítico / Desvio	Causa(s)	Consequência(s)	Ação	Equipamentos	Sensores	Atuadores
BP 1.4.3	Refinado	Nível de refinado acima do nível máximo permitido	Falha da barreira de prevenção BP1.4.2	Provável lançamento de vapores de hidrocarboneto na atmosfera	a) Diagnosticar e sinalizar alarme de nível muito alto b) Degenerar a unidade de isomerização de forma controlada	a) SIS b) IHM	Sensores de nível denominados de LSHH1, LSHH2 e LSHH3.	Comandos de “parada” de forma controlada dos elementos da unidade de ISOM

Sistema / parte do sistema: Unidade de isomerização (ISOM) / Tanque de refluxo

Barreira	Elemento	Evento Crítico / Desvio	Causa(s)	Consequência(s)	Ação	Equipamentos	Sensores	Atuadores
BP 1.4.1	Válvula de alívio RV-4	Falha no fechamento	a) Desgaste mecânico b) Falha no atuador	Excesso de alimentação de refinado no tanque de refluxo	a) Instalar sensores de posição (aberta / fechada) na válvula RV-4 b) Diagnosticar e sinalizar falha de fechamento da válvula RV-4	a) SIS b) IHM	a) Chave fim de curso de válvula aberta b) Chave fim de curso de válvula fechada	não se aplica
BP 1.5.1	Bomba de refluxo	Falha da bomba	a) Desgaste mecânico b) Falha no sistema de alimentação elétrica do conjunto motor-bomba	Excesso de alimentação no tanque de refluxo	a) Instalar sensores na bomba b) Diagnosticar e sinalizar falha da bomba de refluxo	a) SIS b) IHM	Sensor de falha da bomba	não se aplica

Sistema / parte do sistema: Unidade de Isomerização (ISOM) / Tanque de *blowdown*

Tabela 58 – HAZOP: barreiras de mitigação

Barreira	Elemento	Evento Crítico / Desvio	Causa(s)	Consequência(s)	Ação	Equipamentos	Sensores	Atuadores
BM1.1.1	Tanque de *blowdown*	Lançamento de hidrocarboneto altamente inflamável na atmosfera	Falha da barreira de prevenção BP1.4.3	Formação de nuvem de vapor de hidrocarboneto altamente inflamável	a) Instalação de um sistema de queima (*flare system*) dos gases na chaminé do tanque de blowdown b) Instalar sensores de detecção de gás hidrocarboneto c) Diagnosticar e sinalizar alarme de presença de gás na chaminé do tanque via algoritmo de votação 2oo3	a) SIS b) IHM	03 (três) sensores de gás	não se aplica
BM 1.1.2	Tanque de *blowdown*	Formação de nuvem de hidrocarboneto altamente inflamável	Falha da barreira de mitigação BM1.1.1	Movimentação da nuvem de vapor	a) Alarmar sinal de evacuação da unidade de isomerização b) Alarmar sinal para acionamento da brigada de incêndio	a) SIS b) IHM	não se aplica	a) Buzina para alarme sonoro de evacuação da unidade de ISOM b) Buzina para alarme sonoro da brigada de incêndio

Sistema / parte do sistema: Unidade de Isomerização (ISOM) /

Barreira	Elemento	Evento Crítico / Desvio	Causa(s)	Consequência(s)	Ação	Equipamentos	Sensores	Atuadores
BM 1.1.3	Unidade de ISOM	Movimentação de nuvem de vapor	Falha da barreira de mitigação BM1.1.2	Movimentação da nuvem de hidrocarboneto para local com provável fonte de ignição	Degenerar de forma controlada os equipamentos das unidades vizinhas à unidade de ISOM	a) SIS b) IHM c) Rede Industrial	não se aplica	Comandos de "parada" para outros PES responsáveis pela degeneração controlada dos equipamentos das unidades vizinhas à unidade de ISOM.
BM 1.1.4	Unidade de ISOM	Ignição	Falha da barreira de mitigação BM1.1.3	Nuvem de vapor e explosão (VCE) provocado por fonte de ignição	a) Impedir a entrada e/ou circulação de veículos na unidade de ISOM b) Monitoração da presença de pessoas e/ou veículos na unidade	a) IHM	Câmeras	não se aplica
BM 1.1.5	Unidade de ISOM	Nuvem de vapor e explosão (VCE) provocada por fonte de ignição	Falha da barreira de mitigação BM1.1.4	Nuvem de vapor e explosão (VCE)	a) Combater incêndio b) Evacuar pessoas para local seguro	Equipamentos de combate a incêndio	não se aplica	não se aplica
BM 1.2.5	Unidade de ISOM	Nuvem de vapor e explosão (VCE)	Falha da barreira de mitigação BM1.1.4	Incêndio	a) Combater incêndio b) Evacuar pessoas para local seguro	Equipamentos de combate a incêndio	não se aplica	não se aplica
BM 1.3.4	Unidade de ISOM	Ignição	Falha da barreira de mitigação BM1.1.3	Nuvem de vapor de hidrocarboneto	a) Instalar câmeras b) Impedir a entrada e/ou circulação de veículos na unidade de ISOM c) Degenerar de forma controlada os equipamentos das unidades vizinhas à unidade de ISOM	a) SIS b) IHM c) Rede Industrial	Câmeras	Comandos de "parada" para outros PES responsáveis pela degeneração controlada dos equipamentos das unidades vizinhas à unidade de ISOM.

Sistema / parte do sistema: Unidade de Isomerização (ISOM) /

Barreira	Elemento	Evento Crítico / Desvio	Causa(s)	Consequência(s)	Ação	Equipamentos	Sensores	Atuadores
BM 1.4.3	Unidade de ISOM	Movimentação de nuvem de vapor	Falha da barreira de mitigação BM1.1.2	Nuvem de vapor de hidrocarboneto altamente inflamável sobre a unidade de ISOM	Degeneração de forma controlada dos equipamentos da unidade de ISOM	a) SIS b) IHM	Câmeras	Comandos de “parada” de forma controlada dos elementos da unidade de ISOM
BM 1.5.2	Unidade de ISOM	Formação de nuvem de vapor de hidrocarboneto altamente inflamável	Falha da barreira de mitigação BM1,1,1	Incêndio e explosão	a) Alarmar sinal de evacuação da unidade de isomerização b) Alarmar sinal para acionamento da brigada de incêndio	a) SIS b) IHM	não se aplica	a) Buzina para alarme sonoro de evacuação da unidade de ISOM b) Buzina para alarme de acionamento da brigada de incêndio
BM 1.5.3	Unidade de ISOM	Incêndio e explosão	Falha da barreira de mitigação BM1.5.2	Piscina de fogo	a) Alarmar sinal de evacuação da unidade de isomerização b) Alarmar sinal para acionamento da brigada de incêndio c) Combater incêndio	a) SIS b) IHM	não se aplica	a) Buzina para alarme sonoro de evacuação da unidade de ISOM b) Buzina para alarme de acionamento da brigada de incêndio
BM 1.6.3	Unidade de ISOM	Incêndio e explosão	Falha da barreira de mitigação BM1.5.2	Piscina de hidrocarboneto (HC)	a) Alarmar sinal de evacuação da unidade de isomerização b) Alarmar sinal para acionamento da brigada de incêndio c) Combater incêndio	a) SIS b) IHM	não se aplica	a) Buzina para alarme sonoro de evacuação da unidade de ISOM b) Buzina para alarme de acionamento da brigada de incêndio

APÊNDICE F – TABELA DE HAZOP DO EXEMPLO DE APLICAÇÃO 2

Neste apêndice são apresentadas as Tabelas de HAZOP do segundo exemplo de aplicação que foi mostrado no Apêndice D.

A Tabela 59 mostra o HAZOP considerando as barreiras de prevenção de eventos críticos a partir do modelo de acidente da Figura 152. Adicionalmente, a Tabela 60 mostra o HAZOP considerando as barreiras de mitigação de eventos críticos do mesmo modelo de acidente.

Sistema / parte do sistema: Pátio de carregamento de hidrocarboneto na forma líquida em caminhões tanques

Tabela 59 – HAZOP: barreiras de prevenção

Barreira	Elemento	Evento Crítico / Desvio	Causas	Consequências	Ação	Equipamentos	Sensores	Atuadores
BP 1.1.1	Tanque de combustível	Furo no tanque	Falta de inspeção do tanque	Odor de gás provocado por vazamento do mesmo	a) Elaborar plano de inspeção periódica dos tanques b) Instalar sensores de gás no pátio de carregamento de hidrocarboneto c) Diagnosticar e sinalizar vazamento de gás	a) SIS b) IHM (Interface Homem Máquina)	Sensores de gás (lógica de votação 2oo3)	não se aplica
BP 1.1.2	Tanque de combustível	Odor de gás	Falha da barreira de prevenção BP1.1.1	Vazamento de gás no pátio de carregamento de hidrocarbonetos	a) Interromper o carregamento do tanque por meio do fechamento automático das válvulas de entrada de combustível no tanque	c) SIS d) IHM (Interface Homem Máquina)	sensores de gás (lógica de votação 2oo3)	a) Atuador para fechamento das válvulas de entrada de combustível no tanque
BP 1.1.3	Tanque de combustível	Vazamento de gás	Falha da barreira de prevenção BP1.1.2	Incêndio	a) Diagnosticar e sinalizar alarme de incêndio; b) Alarmar sinal de evacuação do pátio de carregamento c) Alarmar sinal para acionamento da brigada de incêndio	a) SIS b) IHM (Interface Homem Máquina)	Sensores de calor e fumaça	a) Buzina de evacuação da unidade de carregamento b) Buzina de acionamento da brigada de incêndio
BP 1.2.1	Válvula do tanque	Falha da válvula	a) Desgaste mecânico b) Falha na vedação	Vazamento de gás	a) Diagnosticar e sinalizar falha de válvula do tanque b) Interromper o carregamento do tanque por meio do fechamento automático das válvulas de entrada de combustível no tanque	c) SIS d) IHM (Interface Homem Máquina)	Sensor de falha da válvula	Atuador de fechamento das válvulas de entrada de combustível no tanque.

Sistema / parte do sistema: Pátio de carregamento de hidrocarboneto na forma líquida em caminhões tanques

Barreira	Elemento	Evento Crítico / Desvio	Causas	Consequências	Ação	Equipamentos	Sensores	Atuadores
BP 1.3.1	Tanque de combustível	Faíscas	a) Motor do caminhão ligado; b) Equipamento elétrico energizado	Fonte de ignição	a) Sinalizar área proibida para fumantes e uso de celular b) Diagnosticar e sinalizar presença de fumaça c) Interromper processo de carregamento de combustível no tanque por meio de fechamento automático das válvulas de entrada de combustível	a) SIS b) IHM	Sensores de fumaça	a) Atuador para fechamento das válvulas de entrada de combustível no tanque
BP 1.3.2	Tanque de combustível	Fonte de ignição	Falha na barreira de prevenção BP1.3.1	Incêndio	a) Diagnosticar e sinalizar alarme de incêndio; b) Alarmar sinal de evacuação do pátio de carregamento c) Alarmar sinal para acionamento da brigada de incêndio	a) SIS b) IHM	Sensores de calor e fumaça	a) Buzina de evacuação da unidade de carregamento b) Buzina de acionamento da brigada de incêndio.

Sistema / parte do sistema: Pátio de carregamento de hidrocarboneto na forma líquida em caminhões tanques

Barreira	Elemento	Evento Crítico / Desvio	Causas	Consequências	Ação	Equipamentos	Sensores	Atuadores
BP 1.4.1	Exaustor	Falha do exaustor	a) Desgaste mecânico b) Curto circuito na malha de alimentação do exaustor	Fonte de ignição	a) Elaborar plano de inspeção periódica do exaustor e do circuito elétrico de alimentação b) Diagnosticar e sinalizar alarme de falha do exaustor	a) SIS b) IHM (Interface Homem Máquina)	Sensores de falha do exaustor	não se aplica
BP 1.5.1	Canteiro de obras	Equipamento elétrico energizado durante processo de carregamento	a) Canteiro de obras próximo de pátio de carregamento b) Falha de orientação de uso de equipamentos elétricos durante processo de carregamento	Fonte de ignição	a) Elaborar plano de afastamento do canteiro de obras do pátio de carregamento de caminhões. b) Sinalizar proibição de uso de equipamentos elétricos durante processo de carregamento c) Sinalizar alarme de equipamento elétrico ligado	a) SIS b) IHM	Sensores de detecção de equipamentos energizados	a) Alarme de equipamento elétrico energizado.

Sistema / parte do sistema: Pátio de carregamento de hidrocarboneto na forma líquida em caminhões tanques

Tabela 60 – HAZOP: barreiras de mitigação

Barreira	Elemento	Evento Crítico / Desvio	Causas	Consequências	Ação	Equipamentos	Sensores	Atuadores
BM 1.1.1	não se aplica	Incêndio e explosão	Falhas das barreiras de prevenção BP1.1.3 e BP1.3.2	piscina de fogo	a) Diagnosticar e sinalizar alarme de incêndio b) Acionar brigada de incêndio c) Combater incêndio d) Alarmar evacuação de pessoas do pátio de carregamento de caminhões	a) SIS b) IHM	Sensores de fumaça e calor	a) Buzina para alarme sonoro de evacuação do pátio de carregamento. b) Buzina para alarme de chamada da brigada de incêndio.
BM 1.1.2	não se aplica	piscina de fogo	Falha da barreira de mitigação BM1.1.1	Efeitos térmicos provocados pela elevação de temperatura	a) Diagnosticar e sinalizar alarme de incêndio b) Acionar brigada de incêndio c) Combater incêndio d) Alarmar evacuação de pessoas do pátio de carregamento de caminhões	a) SIS b) IHM	Sensores de fumaça e calor	a) Buzina para alarme sonoro de evacuação do pátio de carregamento. b) Buzina para alarme de chamada da brigada de incêndio.
BM 1.1.3	não se aplica	Efeito térmico provocado pela elevação da temperatura	Falha da barreira de mitigação BM1.1.2	Danos a outros caminhões (explosão)	a) Diagnosticar e sinalizar alarme de incêndio b) Acionar brigada de incêndio c) Combater incêndio d) Alarmar evacuação de pessoas do pátio de carregamento de caminhões	a) SIS b) IHM	Sensores de fumaça e calor	a) Buzina para alarme sonoro de evacuação do pátio de carregamento. b) Buzina para alarme de chamada da brigada de incêndio.

Sistema / parte do sistema: Pátio de carregamento de hidrocarboneto na forma líquida em caminhões tanques

Barreira	Elemento	Evento Crítico / Desvio	Causas	Consequências	Ação	Equipamentos	Sensores	Atuadores
BM 1.2.3	não se aplica	Efeito térmico provocado pela elevação da temperatura	Falha da barreira de mitigação BM1.1.2	Danos térmicos (queimaduras) às pessoas.	a) Diagnosticar e sinalizar incêndio b) Acionar brigada de incêndio c) Combater incêndio d) Alarmar evacuação do pátio de carregamento dos caminhões	a) SIS b) IHM	Sensores de fumaça e calor	a) Buzina para alarme sonoro de evacuação do pátio de caminhões b) Buzina para acionamento da brigada de incêndio.
BM 1.3.2	não se aplica	Piscina de fogo	Falha da barreira de mitigação BM1.1.1	Degeneração não programada do sistema produtivo	a) Diagnosticar e sinalizar alarme de incêndio b) Acionar brigada de incêndio c) Combater incêndio d) Alarmar evacuação do pátio de carregamento dos caminhões	a) SIS b) IHM	Sensores de fumaça e calor	a) Buzina para alarme sonoro de evacuação de pessoas do pátio de caminhões b) Buzina para acionamento da brigada de incêndio
BM 1.3.3	Sistema produtivo	Degeneração não programada do sistema produtivo	Falha da barreira de mitigação BM1.3.2	Atraso na cadeia de suprimentos	a) Diagnosticar e sinalizar alarme de incêndio b) Acionar brigada de incêndio c) Combater incêndio d) Alarmar evacuação do pátio de carregamento dos caminhões	a) SIS b) IHM	Sensores de fumaça e calor	a) Buzina para alarme sonoro de evacuação de pessoas do sistema produtivo b) Buzina para acionamento da brigada de incêndio

Sistema / parte do sistema: Pátio de carregamento de hidrocarboneto na forma líquida em caminhões tanques

Barreira	Elemento	Evento Crítico / Desvio	Causas	Consequências	Ação	Equipamentos	Sensores	Atuadores
BM 1.4.2	não se aplica	Piscina de fogo	Falha da barreira de mitigação BM1.1.1	Efeitos tóxicos provocados por fumaça tóxica	a) Diagnosticar e sinalizar alarme de incêndio b) Acionar brigada de incêndio c) Combater incêndio d) Alarmar evacuação de pessoas do pátio de carregamento	a) SIS b) IHM	Sensores de fumaça e calor	a) Buzina para alarme sonoro de evacuação do pátio de carregamento b) Buzina para alarme de acionamento da brigada de incêndio
BM 1.4.3	não se aplica	Efeitos tóxicos provocados por fumaça tóxica	Falha da barreira de mitigação BM1.4.2	Danos ao meio ambiente	a) Diagnosticar e sinalizar fumaça tóxica b) Planejar evacuação de pessoas das comunidades vizinhas	a) SIS b) IHM	Sensores de fumaça	não se aplica
BM 1.5.3	não se aplica	Efeitos tóxicos provocados por fumaça tóxica	Falha da barreira de mitigação BM1.4.2	Danos tóxicos às pessoas	a) Diagnosticar e sinalizar fumaça tóxica; b) Planejar evacuação de pessoas das comunidades vizinhas	a) SIS b) IHM	Sensores de fumaça	não se aplica