UNIVERSIDADE FEDERAL DE PERNAMBUCO
CENTRO DE TECNOLOGIA E GEOCIÊNCIAS
PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA QUÍMICA

Marilia Abílio Ramos

A METHODOLOGY FOR HUMAN RELIABILITY ANALYSIS OF OIL REFINERIES AND PETROCHEMICAL PLANTS OPERATIONS: THE HERO (HUMAN ERROR IN REFINERY OPERATIONS) HRA METHODOLOGY

Recife

2017

MARILIA ABÍLIO RAMOS

A METHODOLOGY FOR HUMAN RELIABILITY ANALYSIS OF OIL REFINERIES AND PETROCHEMICAL PLANTS OPERATIONS: THE HERO (HUMAN ERROR IN REFINERY OPERATIONS) HRA METHODOLOGY

Tese de Doutorado apresentada ao Programa de Pós-Graduação em Engenharia Química da Universidade Federal de Pernambuco, como requisito parcial à obtenção do título de Doutor em Engenharia Química.

Área de concentração: Tecnologia de Petróleo e Gás Natural
Orientador: Prof. Dr. Enrique López Droguett
Co-orientador: Prof. Dr, Márcio das Chagas Moura

Recife
2017

Catalogação na fonte
Bibliotecária Valdicèa Alves, CRB-4 / 1260

R175m Ramos, Marilia Abílio.
A methodology for human reliability analysis of oil refineries and petrochemical plants operations: the hero (human error in refinery operations) hra methodology / Marilia Abílio Ramos. - 2017.
201folhas, Il., tabs.; Abr., Mon. e Simb..

Orientador: Prof. Dr. Enrique López Droguett.
Coorientador: Prof. Dr. Márcio das Chagas Moura.

Tese (Doutorado) – Universidade Federal de Pernambuco. CTG. Programa de Pós-Graduação Engenharia Química, 2017.
Inclui Referências e Apêndices.
Nota: Trab. No Idioma Inglês.

1. Engenharia Química. 2. Human reliability analysis. 3. Oil refining. 4. Safety. 5 Human error. 6. Risk analysis. I. Droguett. Enrique López (Orientador). II. Moura. Márcio das Chagas(Coorientador). III. Título.

UFPE

660.2 CDD (22. ed.) BCTG/2017- 146

MARILIA ABILIO RAMOS

A METHODOLOGY FOR HUMAN RELIABILITY ANALYSIS OF OIL REFINERIES AND PETROCHEMICAL PLANTS OPERATIONS: THE HERO (HUMAN ERROR IN REFINERY OPERATIONS) HRA METHODOLOGY

Linha de Pesquisa: Tecnologia do Petróleo, Gás Natural e Biocombustíveis

Tese de Doutorado apresentada ao Programa de Pós-Graduação em Engenharia Química da Universidade Federal de Pernambuco, defendida e aprovada em 07 de abril de 2017 pela banca examinadora constituída pelos seguintes membros:

_____

Prof. Dr. Enrique López Droguett/DEP-UFPE
(Orientador)

_____

Prof. Dr. Márcio das Chagas Moura/DEP-UFPE
(Coorientador)

_____

Profª. Drª. Ísis Didier Lins/DEP-UFPE
(Examinadora Externa)

_____

Prof. Dr. José Geraldo de Andrade Pacheco Filho/DEQ-UFPE
(Examinador Interno)

_____

Prof. Dr. Mohand Benachour/DEQ-UFPE
(Examinador Interno)

_____

Prof. Dr. Romero Luiz Mendonça Sales Filho/DEE-UFRPE
(Examinador Externo)

_____

Dr. Rômulo Fernando Teixeira Vilela/GDO-CHESF
(Examinador Externo)

Aos meus pais e à minha irmã, por quem todo esforço sempre vale a pena.

AGRADECIMENTOS

Agradeço inicialmente ao professor Enrique López pela orientação, pelo acompanhamento e pela disponibilidade. Por ter sido um mentor desde a minha graduação até o fim do meu doutorado, e me apresentar a um novo mundo de temas de pesquisa. Por sempre me desafiar a sair da zona de conforto e trabalhar com novos tópicos.

O meu agradecimento por orientação se estende ao professor Márcio Moura, cujas contribuições para esta tese foram inestimáveis. Obrigada pelo tempo, pela paciência, pelas soluções propostas, e pela reciprocidade na amizade e carinho.

Agradeço ao professor Ali Mosleh, por me receber e me orientar na Universidade da California em Los Angeles (UCLA), e ser um terceiro mentor ao longo dessa tese. *Thank you for the constant guidance, for your critical feedback and for your time. Thank you for believing in me and in this thesis.*

Agradeço, no nome de Claudia Von, aos meus colegas do Centro de Estudos e Ensaios em Risco e Modelagem Ambiental (CEERMA) por fazer do cotidiano de trabalho um momento sempre agradável, e por fazer do CEERMA o espaço colaborativo que é. Foi no CEERMA que tive o primeiro contato com pesquisa, e me orgulho de nele me formar como pesquisadora.

Ao Programa de Pós-Graduação em Engenharia Química, pela minha formação profissional. No nome de Mohand Benachour, agradeço a todos os professores pelas portas abertas e pelo acompanhamento. Agradeço a Flavio Garrett e Priscila Macêdo, por solucionarem com carinho todos os problemas que surgiram durante o doutorado.

Agradeço ao Programa Ciência sem Fronteiras pelo financiamento dado para um ano de pesquisa na UCLA, através do CNPq. Sem esta oportunidade esta tese, fruto de um trabalho colaborativo com a UCLA, não teria sido possível. Agradeço também à Fundação Lemann pela bolsa complementar recebida durante o ano na UCLA.

À Agência Nacional do Petróleo, Gás Natural e Biocombustíveis – ANP, à Financiadora de Estudos e Projetos – FINEP e à PETROBRAS, por meio do Programa de Recursos Humanos da ANP para o Setor de Petróleo e Gás – PRH-ANP/MCT, em particular ao PRH 28, do Departamento de Engenharia Química, Centro de Tecnologia e Geociências da UFPE, pelo apoio financeiro. À professora Celmy Barbosa, ao pesquisador Jean Héliton, e a Vilckma Oliveira, por fazer do PRH28 o programa de sucesso que ele é.

Agradeço aos meus amigos pelos momentos de lazer, pelas cervejas, pela compreensão nos momentos de ausência e pelo abraço forte de quando nos encontramos. Agradeço nominalmente a Analice Souza, Bruno Ferreira, Jane Frazão, Marconi Madruga, Rafael Formiga, Rita Kramer, Roberta Mota, Yuri Brooman.

Agradeço a Eduardo Andrade, pelo simples fato de fazer parte da minha vida, e por tornar mais leve esse doutorado.

Acima de tudo, agradeço aos meus pais e à minha irmã, Francisco, Rinalda e Mariana. Aos meus pais, por serem os meus maiores exemplos de vida. Obrigada pelas conversas, pelos cafés, pelo apoio, pela presença. Por serem esses pilares fortes da minha vida, onde eu sempre posso me escorar quando as coisas ficam difíceis. À minha irmã, por acreditar em mim quando eu mesma não acreditava. Que um dia eu consiga colocar em palavras o quanto eu sou agradecida a você por tudo na minha vida. Essa tese não teria sido possível sem você ao meu lado.

One has to look out for engineers - they begin with sewing machines and end up with the atomic bomb (Marcel Pagnol)

ABSTRACT

The oil industry has grown in recent decades in terms of quantity of facilities and process complexity. However, human and material losses still occur due to major accidents at the facility. The analysis of these accidents reveals that many involve human failures that, if prevented, could avoid such accidents. These failures, in turn, can be identified, modeled and quantified through Human Reliability Analysis (HRA), which forms a basis for prioritization and development of safeguards for preventing or reducing the frequency of accidents. The most advanced and reliable HRA methods have been developed and applied in nuclear power plant operations, while the petroleum industry has usually applied Quantitative Risk Analysis (QRA) focusing on process safety in terms of technical aspects of the operation and equipment. This thesis demonstrates that the use of HRA in oil refining and petrochemical operations allows the identification and analysis of factors that can influence the behavior of operators as well as the potential human errors that can contribute to the occurrence of an accident. Existing HRA methodologies, however, were mainly developed for the nuclear industry. Thus, they may not reflect the specificities of refining and petrochemical plants regarding the interaction of the operators with the plant, the failure modes of the operators and the factors that influence their actions. Thus, this thesis presents an HRA methodology developed specifically for use in this industry, HERO - Human Error in Refinery Operations HRA Methodology. The Phoenix HRA methodology was used as a basis, which has three layers i) a crew response tree (CRT), which models the interaction between the crew and the plant; ii) a human response model, modeled through fault trees, that identifies the possible crew failures modes (CFMs); and (iii) "contextual factors" known as performance influencing factors (PIFs), modeled through Bayesian networks. In addition to building on such a structure, HERO's development relied on interviews with HRA specialists, visitations to a refinery and its control room, and analysis of past oil refineries accidents - four accidents were analyzed in detail. The methodology developed maintains the three-layer structure and has a guideline flowchart for the construction of the CRT, in order to model the team-plant interactions in oil refining and petrochemical operations; it also features CFMs and PIFs developed specifically for this industry, with definitions that make them easily relatable by an analyst. Finally, the methodology was applied to three potential accidental scenarios of refinery operations. In one of these scenarios, it was combined with a QRA to illustrate how an HRA can be applied to a traditional QRA and to demonstrate the influence of PIFs and of human error probability on the final risk. The use of this methodology for HRA of refineries and petrochemical plants operations can enhance this industry safety and allow for solid risk-based decisions.

Key words: Human reliability analysis. Oil refining. Safety. Human error. Risk analysis.

RESUMO

A indústria de petróleo teve grande crescimento nas últimas décadas em termos de quantidade de instalações e complexidade de processo. No entanto, perdas humanas e materiais ainda ocorrem devido a acidentes graves nas instalações. A análise desses acidentes revela que muitos envolvem falhas humanas que poderiam ser prevenidas de forma a evitar tais acidentes. Estas falhas, por sua vez, podem ser identificadas, modeladas e quantificadas através da Análise de Confiabilidade Humana (ACH), que forma uma base para priorização e desenvolvimento de salvaguardas na prevenção ou redução da frequência de acidentes. Os métodos de ACH mais avançados e confiáveis têm sido desenvolvidos e aplicados nas operações de controle de plantas nucleares; já a indústria de petróleo tem usualmente aplicado a Análise Quantitativa de Risco (AQR) com foco na segurança de processo em termos técnicos da operação e equipamentos. Esta tese demonstra que o uso da ACH em operações de refino e petroquímica possibilita a identificação e análise dos fatores que podem influenciar o comportamento do operador bem como as potenciais falhas humanas que podem contribuir para a ocorrência de um acidente. As metodologias de ACH existentes, no entanto, foram desenvolvidas para a indústria nuclear. Desta forma, elas não refletem as especificidades de refino e petroquímica no que se refere à interação dos operadores com a planta, aos modos de falha dos operadores e aos fatores que influenciam suas ações. Assim, esta tese apresenta uma metodologia de ACH desenvolvida especificamente para uso nessa indústria, a HERO - *Human Error in Refinery Operations HRA Methodology*. Como base, utilizou-se a Metodologia Phoenix, que possui três camadas i) uma árvore de resposta da equipe (*crew response tree* - CRT), que modela a interação da equipe com a planta; ii) um modelo de resposta humana, modelado através de árvores de falhas, que identifica os possíveis modos de falhas da equipe (*crew failures modes* - CFMs); e iii) os "fatores contextuais" conhecidos como fatores de desempenho ou *performance influencing factors* (PIFs), modelados através de redes Bayesianas. Além de basear-se em tal estrutura, o desenvolvimento da HERO apoiou-se em entrevistas com especialistas em ACH, visitas a uma refinaria e sua sala de controle e na análise de estudos de acidentes passados em refinarias – foram analisados em detalhe quatro acidentes. A metodologia desenvolvida mantém a estrutura de três camadas e possui um fluxograma-guia para construção da CRT, de forma a modelar as interações equipe-planta na operação de refino e petroquímicas; ela também apresenta CFMs e PIFs desenvolvidos especificamente para esta indústria, com definições que os tornam facilmente identificáveis por um analista. Por fim, a metodologia foi aplicada a três cenários acidentais de operações de refinaria. Em um destes cenários, ela foi conjugada a uma AQR de forma a ilustrar como uma ACH pode ser aplicada a uma tradicional AQR e para demonstrar a influência dos PIFs e da Probabilidade de Erro Humano no risco final. Espera-se que o uso da metodologia proposta nesta tese poderá aumentar a segurança em refinarias e petroquímicas e permitir sólidas decisões baseadas no risco.

Palavras-chave: Análise de confiabilidade humana. Refino de petróleo. Segurança. Erro humano. Análise de risco.

LIST OF FIGURES AND ILLUSTRATIONS

LIST OF TABLES

LIST OF SYMBOLS, ABBREVIATIONS AND NOMENCLATURE

ALARP	As Low as Reasonably Possible
ARU	Aromatics Recovery Unit
ASEP	Accident Sequence Evaluation Program
ASP/SPAR	Accident Sequence Precursor Standardized Plant Analysis Risk Model
ATHEANA	A Technique for Human Event Analysis
BBN	Bayesian Belief Network
BP	Branch Point (flowchart)
CETESB	*Companhia Ambiental do Estado de São Paulo*
CFM	Crew Failure Mode
CREAM	Cognitive Reliability and Error Analysis Method
CRT	Crew Response Tree
CSB	Chemical Safety Board (United States)
CWS	Community Warning System
EiREDA	European Industry Reliability Data
EOC	Error of Commission
EOO	Error of Omission
EPA	Environmental Protection Agency (United States)
ESD	Event Sequence Diagram
ET	Event Tress
FAT/CAT	Fatality/catastrophe
FT	Fault Tree
HAZOP	Hazard and Operability Study
HCL	Hybrid Causal Logic
HEART	Human Error Assessment and Reduction Technique
HEP	Human Error Probability

HERO	Human Error in Refinery Operations
HFE	Human Failure Event
HGU	Hydrogen Generation Unit
HMI	Human Machine Interface
HRA	Human Reliability Analysis
HSE	Health and Safety Executive (United Kingdom)
HTA	High Temperature Alarm
HTHA	High Temperature Hydrogen Attack
IDAC	Information, Decision and Action in a Crew context
IRIS	Integrated Risk Information System (software)
ISOM	Isomerization unit
JCP	Joint Conditional Probability
MARS	European Major Accident Reporting System
NHT	Naphtha Hydrotreater unit
NPP	Nuclear Power Plant
NRC	Nuclear Regulatory Commission (United States)
OREDA	Offshore Reliability Data
OSHA	Occupational Safety and Health Administration (USA)
P&ID	Piping and Instrumentation Diagrams
PIF	Performance Influencing Factor
PRA	Probabilistic Risk Analysis
PSA	Probabilistic Safety Assessment
PSF	Performance Shaping Factor
QRA	Quantitative Risk Analysis
REDUC	Duque de Caixas Refinery
REGAP	Gabriel Passos Refinery
REVAP	Henrique Lage Refinery
RLAM	Landulpho Alves Refinery

SACADA	Scenario Authoring, Characterization, and Debriefing Application database project
SIP	shelter-in-place advisory
SPAR-H	Standardized Plant Analysis Risk Human Reliability Analysis
THERP	Technique for Human Error Rate Prediction
TMI	Three-Mile Island
TNO	the Netherlands Organisation for applied scientific research TNO

CONTENTS

CHAPTER 1 – INTRODUCTION

Petroleum refining installations and petrochemical plants pose safety concerns that are inherent to their characteristics - working with flammable and toxic fluids. The oil industry has made several advances in improving safety; however, accidents of all ranges still occur. Statistical analysis of the 489 major accidents from 1985 to 2001 in the European Union reported to the European Major Accident Reporting System (MARS) has showed that the second biggest number of accidents (17% of the total number) occurred in petrochemical installations[1]. Moreover, 70% of the major accidents took place when the plants were in normal operation status (NIVOLIANITOU; KONSTANDINIDOU; MICHALIS, 2006).

The case of the European Union abovementioned is not an isolated one. In the United States, the number of accidents in petroleum refineries is also significant. According to the Occupational Safety and Health Administration (OSHA), the United States had 36 fatality/catastrophe (FAT/CAT) accidents related to hydrocarbon release in the refining industry between 1992 and 2007. These accidents included 52 employee deaths and 250 employee injuries; 98 of these injuries required hospitalization. This number is extremely significant since it is more than the combined FAT/CAT of the next three industries over the same period[2] (OSHA, 2007).

Although the approximately 150 petroleum refineries operating in the U.S are roughly only one percent of all the facilities covered by the Environmental Protection Agency (EPA) Risk Management Program between 2000 and 2010, they experienced more recordable accidents than any other industry: 234 accidents. During 2012, the Chemical Safety Board (CSB) tracked 125 significant process safety accidents in U.S. petroleum refineries (CSB, 2014a). These are not isolated cases and examples of accidents involving petroleum refining installations go beyond the European Union and the U.S.

Brazil, in particular, has its own share of serious accidents in oil refineries. In 1972, a LPG explosion at Duque de Caixas Refinery (REDUC), Rio de Janeiro, killed 38 persons; in 1982, in the Henrique Lage Refinery, (REVAP), an acid gas leak killed 11 people, and in

[1] This number was only behind general chemicals, which were responsible for 32%,

[2] These industries are “Chemical Manufacturing, Not Elsewhere Classified” (12 FAT/CATs); “Industrial Organic Chemical Manufacturing” (12 FAT/CATs), and “Explosive Manufacturing”(11 FAT/CATs)

1998, at Gabriel Passos Refinery, (REGAP), a naphta leak resulted the death of 6 people (SOUZA; FREITAS, 2003). On January 18 2015 an explosion at the Hydrogen Generation Unit at Landulpho Alves Refinery (RLAM), Bahia, left 3 workers severely hurt (VEJA, 2015). More recently, on August 31 2016 a Sulphur vessel roof collapsed at REDUC paralyzing the plant, which was responsible for ten percent of the Brazilian refining capacity (FOLHA DE SÃO PAULO, 2016).

The examples mentioned in this introduction make it clear that safety is still a major issue when it comes to petrochemical plants and petroleum refining installation and processes. Interestingly, statistics show that majority of accidents (over 80%) in the chemical and petrochemical industries have human failure as a primary cause (KARIUKI; LOWE, 2007). Nonetheless, although it is accepted that human error is behind major accidents, few major hazard sites proactively seek out potential human performance issues (HSE, 2008).

In this sense, in this thesis, I make a deeper analysis of four major refinery accidents to investigate if they have involved human errors at some point and if they could, thus, have been avoided, as I seek to develop a methodology to analyze these errors. Among the events in recent years, these four accidents in US refineries can be considered as major as they resulted in significant human and financial losses:

- In 1997, an accident in the Tosco Avon Refinery in Martinez, California, resulted in the death of one operator and injured 46 persons. A piping ruptured on the Hydrocracker unit releasing hydrocarbon and hydrogen and causing an intense fire. The cause of the rupture was excessively high temperature, due to a temperature excursion not brought under control (EPA, 1998);
- In 2005, an accident occurred in BP's Texas City Refinery, and it was one of the worst industrial disaster in recent U.S. history. The overfilling of the raffinate splitter tower during the startup of an isomerization unit resulted in a flammable liquid geyser from a blowdown stack that was not equipped with flares, which lead to an explosion and fire. The accident killed 15 people and injured another 180, and resulted in financial losses exceeding $1,5 billion (CSB, 2007);
- In 2010, the largest fatal accident at a U.S. petroleum refinery since the BP Texas City occurred in Tesoro Anacortes Refinery, Washington. A catastrophic rupture of a heat exchanger in the Catalytic Reformer/Naphta hydrotreter Unit released highly flammable hydrogen and naphtha, which ignited and caused an

explosion and a fire that lasted for more than three hours. Seven employees were killed in the accident (CSB, 2014b);

- In 2012, a catastrophic pipe rupture in the Crude Unit at Chevron Richmond Refinery released flammable hydrocarbon process fluid, which partially vaporized into a large vapor cloud that engulfed 19 Chevron employees and ignited. All of the employees escaped, narrowly avoiding serious injury. The ignition of the flammable portion of the vapor cloud and subsequent continued burning of the hydrocarbon process fluid resulted in a large plume of particulates and vapor traveling across the Richmond. 15000 people had to look for medical treatment (CSB, 2015).

Human Reliability Analysis (HRA) has been making it possible for human contribution to risk to be assessed both qualitatively and quantitatively. HRA aims to identify, model and quantify human failure events (HFE) in the context of various accident scenarios. Such analyses have formed the basis for prioritizing and developing effective safeguards to prevent or reduce the likelihood of human caused accidents. To date, most credible and highly advanced HRA methods have largely been developed and applied in support of nuclear power plants (NPP) control room operations and in context of probabilistic risk analysis (PRA). A discussion on HRA methods and examples will be provided in Chapter 2.

In the petroleum industry, Quantitative Risk Analysis (QRA) is one of the main tools for risk management. According to Taylor (2014), HRA can be considered a relatively new concept within the petroleum industry, in which QRA has mostly focused on technical barriers. Laumann *et al*. (2014) point out that QRAs differ on the extent to which they incorporate human and organizational factors, and that a reason for this might be a lack of research on how to apply HRA in the petroleum industry. Another reason for it to be considered new in the oil and gas area, pointed by Boring (2015), is that there is no globally accepted requirement for QRA in the petroleum sector.

In fact, QRAs applied to the oil and gas industry have primarily identified hardware failure risks, neglecting those human failure events that contribute to the overall system risk. In Brazil, risk analysis studies for petrochemical plants normally follow the CETESB standard P.4.261 (CETESB, 2014), which determine rules for QRA. It starts by a qualitative risk analysis of the process, followed by the estimation of consequences and frequency and final Individual and Social Risks. It thus does not prescribe that a human factor analysis or HRA should be performed despite the benefits that would be brought up by doing so within a QRA.

These benefits include identification and analysis of factors that may influence the operators' behavior and of the potential human errors that may lead or contribute to major accidents.

Presently, dozens of HRA methods exist and new methods are still being developed. The so-called first-generation HRA methods were the first ones developed to help risk assessors predict and quantify the likelihood of human error. They include Technique for Human Error Rate Prediction – THERP (SWAIN; GUTTMAN, 1983) and Human Error Assessment and Reduction Technique – HEART (WILLIAMS, 1986). In the 1990s, efforts were made to improve the application of first-generation HRA methods, which led to the so-called second-generation methods, such as Cognitive Reliability and Error Analysis Method – CREAM (HOLLNAGEL, 1998), Standardized Plant Analysis Risk Human Reliability Analysis – SPAR-H (GERTAMN *et al*., 2005), and Information, Decision and Action in Crew context – IDAC (CHANG; MOSLEH, 2007a…e) (EKANEM *et al.*, 2016; BELL; HOLROYD, 2009). A deeper description and discussion of first- and second-generation methods will be provided in Chapter 2.

Despite their relevance, such methods, as Ekanem *et al*. (2016) point out, have issues that have led to inconsistencies, insufficient traceability and reproducibility in both the qualitative and quantitative phases. These issues have even greater relevance once we observe that they have allowed for (i) significant variability in the results seen in the application of different HRA methods, and (ii) significant variability in cases where different HRA analysts apply the same method. In order to address these issues, Mosleh *et al*. (2010, 2012), complemented by Ekanem (2013), have proposed a model-based hybrid HRA methodology under the name of Phoenix Methodology.

The Phoenix methodology is a model-based method that takes advantage of the best features of existing and emerging HRA methods. Phoenix introduces the Crew Response Tree (CRT), which provides a structure for capturing the context associated with human failure events (HFEs), including errors of omission and commission. It also makes use of a human response model that relates the observable Crew Failures Modes (CFMs) to "context factors" commonly known as Performance Influencing Factors (PIFs). However, actions taken in a nuclear power plant control room do not in all cases generalize to the types of actions performed elsewhere. As such, it can be challenging to extrapolate these scenarios to other domains like the petroleum industry (BORING; OIEN, 2014).

The development of an HRA methodology based on Phoenix, but designed specifically for the petroleum refinery and petrochemical plants context would thus allow to identify the peculiarities of this industry in regard to interactions between the crew and the plant, possible operators' errors and contextual factors. This would be possible given the combination of the benefits brought by Phoenix with the inherent characteristics of the petroleum sector concerning the type of work, the individuals and the organization that influence human performance, operators training and organization, operating procedures. In this sense, this thesis makes use of Phoenix methodology as a basis for a new methodology that will reflect the petroleum refinery context - the HERO (Human Error in Refinery Operations) HRA methodology.

Besides developing a new methodology for the specific cases of petroleum refineries and petrochemical plants, this thesis focuses in explaining its qualitative aspects. I thus take into consideration, while developing HERO, that it is of extreme relevance to have a strong and solid qualitative analysis when performing an HRA. This is supported by Taylor (2014), who points out that the International HRA Empirical Study (FORESTER *et al*., 2013) showed that HRA methods will not have an adequate basis to identify important performance drivers and to obtain a realistic human error probability (HEP) estimate unless the HRA includes a qualitative analysis covering a thorough set of scenario conditions and influencing factors.

1.1 OBJECTIVES

The main goal of this research is to develop an HRA methodology specifically for the petroleum refinery and petrochemical plants context in order to identify the peculiarities of this industry in regard to interaction between the crew and the plant, CFMs and PIFs . More specifically, I aim at building on Phoenix methodology to develop a robust oil refinery-oriented method which can improve the safety within petroleum industries and allow for stronger risk-informed decisions.

As a foundation, I make use of Phoenix methodology since it is a model-based method, which incorporates strong elements of current HRA good practices, leverages lessons learned from empirical studies, and the advantages of the best features of existing and emerging HRA methods. In order to create a new methodology that takes into consideration the context of petroleum refineries and petrochemical plants, I will follow these steps:

- I will analyze past oil refineries accidents through extensive research of accident reports and papers related. More specifically, I will analyze in deep four accidents: the Tosco Avon Refinery accident (1997), the BP Texas City refinery accident (2005), the Tesoro Anacortes Refinery accident (2010) and the Chevron Richmond Refinery accident (2012);
- I will construct a timeline of these four significant past oil refineries accidents in order to identify operators' decisions' points and operators' actions that contributed to the accident;
- I will identify the factors that could have any influence on the operators' actions during the accident, including cognitive, organizational and environmental factors;
- Through interviews with specialists, I will analyze how Phoenix's set of PIFs and CFMs can be modified to be applied in refinery and petrochemical control rooms: which ones will be maintained, which ones will be deleted and which CFMs and PIFs are relevant to oil refineries and petrochemical plant operations that are not covered by Phoenix's set;
- Through visitations to a Brazilian refinery control room and informal meetings with engineers and operators, I will analyze how the refinery crew interacts with the plant. These will be further detailed in Chapter 4;
- I will adapt the Phoenix methodology framework in order to reflect the oil refinery context with regard to interaction between the crew and the plant, CFMs and PIFs. This will be done in order to capture the various modes in which oil refinery operating crews could fail while conducting their day-to-day activities, and which factors could influence their actions. This is part of the development of the HRA methodology for oil refinery applications;
- I will apply the HRA methodology to be developed in this thesis to three oil refinery accident scenario. The first one consists of a leak in reactor tubes of a Hydrogen Generation Unit, the second one is a scenario based on the Chevron Richmond refinery accident, and the third one is a potential scenario in the Hydrotreating Unit.
- I will apply the HRA method within a Quantitative Risk Analysis in the third example abovementioned, and analyze the impact it has on the Individual Risk of the scenario.

1.2 THESIS STRUCTURE

This introductory chapter provided a general overview of this thesis, its motivation, objectives and the step-by-step to be followed in the next chapters. Chapter 2 will provide a literature review on HRA methods. I will thus explain how they were created, their relevance, strengths and limitations. The categorization concerning first- and second-generation methods will be explained and I will particularly address THERP as an example of a first-generation method, and SPAR-H as an example of a second-generation method. Following this, I will examine current HRA shortcomings and proceed to outlining the Phoenix methodology.

Chapter 3, in turn, will provide a review of past oil refineries accidents, namely the Tosco Avon Refinery accident (1997), the BP Texas City Refinery accident (2005), the Tesoro Anacortes Refinery accident (2010), and the Chevron Richmond refinery accident (2012). It will also introduce an analysis of the operators' actions during the course of the accident, and discuss the factors that affected such actions. The conclusions from the analysis of past accidents, summed with the analysis of interviews with the specialists and visitation to a refinery control room will form the basis to develop HERO HRA methodology that will be explained in Chapter 4.

Chapter 4 will strictly focus on presenting the elements that form HERO HRA Methodology, such as CRT, CFMs, FTs and PIFs. I will outline the guidelines and explain how to apply them. Chapter 5, finally, will show how the adapted methodology applies to potential risk scenarios in an oil refinery operation. I will make use of three case studies, namely: a Hydrogen Generation unit scenario, the Chevron Refinery accident in Richmond, and a Hydrotreating unit scenario. Finally, Chapter 6 will provide a summary of the findings, a discussion of the main contributions of this thesis, the main challenges I faced throughout all the phases to develop HERO HRA Methodology, and potential ideas for future work.

CHAPTER 2 - HRA: CREATION, METHODS, AND LIMITATIONS

Most, if not all, technological systems rely on human action to function properly. Although some – such as hydroelectric power plants – may function for extended periods of time without the need of human intervention, few of these systems are completely autonomous. In this sense, it is well acknowledged that human action is a major source of vulnerability to the integrity of interactive systems in any type of field; these include complex as well as simple ones (HOLLNAGEL, 1998). In Chapter 1, I introduced statistical data that highlights how human actions have contributed to accidents in oil refineries plants. In addition, according to Hollnagel (1993) somewhere in the range 60-90% of all system failures, regardless of the domain, could be attributed to erroneous human actions.

In this chapter, I will explore Human Reliability Analysis (HRA) as a form of assessing both quantitatively and qualitatively the human contribution to accidents. Swain & Guttmann (1983) define human reliability as the probability that a person (1) correctly performs an action required by the system in a required time and (2) that this person does not perform any extraneous activity that can degrade the system. HRA is thus, in short, a method by which human reliability is estimated (SWAIN, GUTTMAN; 1983, SWAIN, 1990).

This chapter will proceed as follows: I will first approach HRA's core concepts and then examine different methods that have been used throughout the years. I will distinguish between first- and second-generation methods and detail two examples: THERP and SPAR-H. Once these methods have been described, I will discuss the drawbacks that come along with first- and second-generation methods in general. Following this, I will introduce the Phoenix methodology and present its potential benefits when compared to the other methods.

This chapter serves as a background on the relevance of the Phoenix methodology. The understanding of the latter is crucial for the following chapters, as these will build on the Phoenix methodology to develop a methodology for petroleum refineries and petrochemical plants. In this sense, I will provide a comprehensive description of Phoenix's three layers and their elements. I will also explain what makes Phoenix the most suited HRA methodology to serve as a foundation for a new methodology. Finally, I will present a discussion on the current advances of HRA in oil refining and petrochemical operations area.

2.1 HUMAN RELIABILITY ANALYSIS: CONCEPTS AND HISTORY

As mentioned in the introduction, HRA allows human reliability to be estimated both quantitatively and qualitatively. Yet, although human error is the main object of study of HRA, it should not be viewed as the product of individual shortcomings (BORING, 2012). As argued by Hollnagel (1998), one of the undisputed assumptions in HRA approaches is that the quality of human performance depends on the conditions under which the tasks or activities are carried out. These conditions, in turn, have generally been referred to as Performance Shaping Conditions (PSFs) or Performance Influencing Factors (PIFs); they serve to either enhance or degrade human performance relative to a baseline. Human error can be generally categorized as errors of omission - when an operator fails in acting, i.e., he/she does not perform a specific task, and errors of commission - when an operator fails when acting, i.e., he/she performs a task in a wrong manner, or perform the wrong task.

The assessment of human reliability, according to Kirwan (1994), can be categorized into three functions: (a) Human Error Identification, which concerns the identification of what errors can occur; (b) Human Error, Quantification, which regards the decision of how likely the errors are to occur; and, if appropriate, (c) Human Error Reduction, which implies the improvement of human reliability by reducing error likelihood. As will be mentioned in the following section, HRA methods usually consider these three elements in the assessment of human reliability.

Human reliability studies are a relatively recent area of research. Its history can be traced back to 1952, when it was first addressed for a weapon system feasibility in Sandia National Laboratories, USA (SWAIN; 1990). In the 1960s, it started to be used for civil applications, with a focus on man machine system design. The first formal method for HRA was actually presented in November 1962 at the Sixth Annual Meeting of the Human Factors Society, followed by a monograph from Sandia Laboratories (SWAIN, 1963) outlining its quantification. This method, called Technique of Human Error Rate Prediction (THERP), is still used in HRA (PYY, 2000).

Interestingly, throughout the 1980s the number of HRA methods significantly increased. According to Hollnagel (2005), there is a strong correlation between the accident at Three-Mile Island (TMI)[3] on March 28, 1979 – which was the most serious accident in the

[3] The Three-Mile Island accident was the most serious accident in U.S. commercial nuclear power plant operating history. The TMI-2 reactor partially melted down. Although this is the most dangerous kind of nuclear

U.S. commercial nuclear plant operating history – and the growth in the number of HRA methods. Figure 1 presents the evolution of the number HRA methods through time.

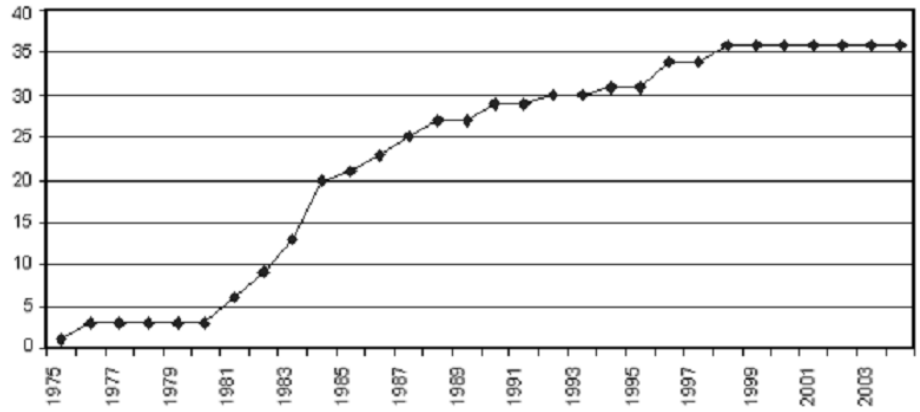


Figure 1: Cumulated number of HRA methods according to year of publication (HOLLNAGEL, 2005)

There are currently several reviews on HRA methods available. Hollnagel, in 1998, published the book that introduced CREAM (Cognitive Reliability and Error Analysis Method) HRA method. In doing so, he presented a review of 9 methods[4] by using a triad of method, classification scheme, and model - the MCM framework presented in the same book. In 2009, in turn, Bell and Holroyd drafted a review for the Health and Safety Executive (HSE) from the United Kingdom. They reported that 72 potential human reliability related tools were identified and reviewed 17 of them[5]. For each of these, Bell and Holroyd described what they claimed to offer in terms of human reliability and their procedures. The authors also analyzed the benefits and drawbacks of each of the 17 methods based on objective information available in the research literature, their potential application, and major hazard sectors for which they would be suitable (if appropriate). They also provided a comment on their validity and noted the resources required for their use.

power accident, its small radioactive releases had no detectable health effects on plant workers or the public (NRC, 2014).

[4] Namely: AIPA (FLEMING et al, 1975), CM (POTASH et al, 1981), OAT (WREATHALL, 1982), STAHR (PHILLIPS et al, 1983), THERP, Expert Estimation (COMER et al, 1984), SLIM/MAUD, HCR (HANNAMAN et al, 1984), MAPPS (SIEGEL et al, 1984)

[5] These are: THERP (SWAIN, GUTTMAN; 1983), ASEP (SWAIN, 1987), HEART (WILLIAMS, 1985), SPAR-H (GERTAMN et al, 2005), ATHEANA (FORESTER et al, 2000), CREAM (HOLLNAGEL, 1993), APJ (HUMPHREYS, 1995), PC (HUNNS, 1982), SLIM-MAUD (EMBREY et al, 1984), HRMS (KIRWAN, 1990), JHEDI (KIRWAN, 1990), INTENT (GERTMAN et al, 1990), CAHR (STRATER, 1997) CESA (STRATER et al, 1990), CODA (REER, 1997), MERMOS (LE BOT et al, 1997), NARA (KIRWAN et al, 2005)

In 2006, Forester *et al*., from the United States Nuclear Regulatory Commission (NRC), published a brief review of 10 methods, namely THERP, ASEP, HCR/ORE, CBDT, EPRI/HRA Calculator, SLIM/MAUD, FLIM, SPAR-H, ATHEANA, SHARP1. They also evaluated such methods against HRA good practices, outlined in "Good Practices for Implementing Human Reliability Analysis (HRA)" (Kolaczkowski *et al*, 2005), also a publication by NRC. More recently, Spurgini (2010) published a comprehensive book on Human Reliability Assessment Theory and Practice, in which he classified HRA methods as task-related, time-related and context-related methods. Using this classification, he reviewed 15 methods and discussed how they are implemented as well as their weaknesses and strengths. Figure 2 below illustrates the models reviewed by Spurgini (2010).

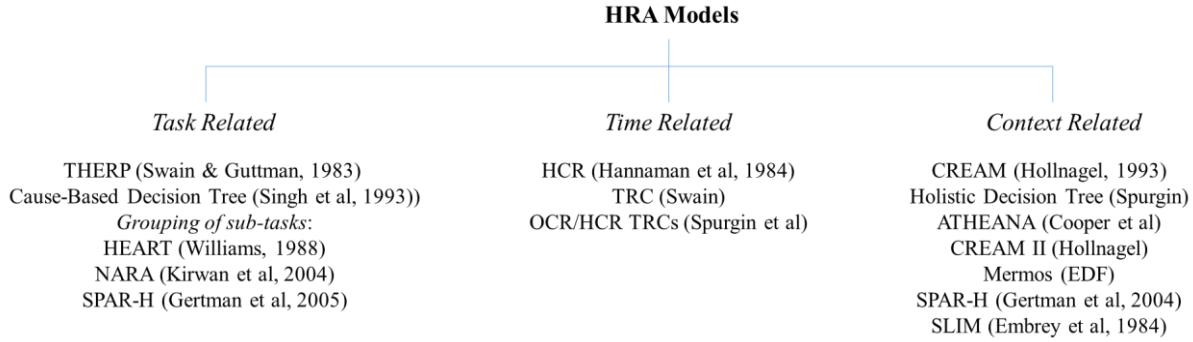


Figure 2 - HRA models reviewed by Spurgini (2010)

It is worth mentioning that although there can be several differences between HRA methods, HRA is often depicted as consisting of three distinct phases (Boring, 2009):

1. The modeling of the potential contributors to human error – the enlistment of some variety of task analysis to decompose an overall sequence of events into smaller units suitable for analysis. There is no universally agreed standard for the best level of decomposition.
2. The identification of the potential contributors to human error - the selection of relevant performance shaping factors. As with task decomposition, there is no standard list of performance shaping factors, and there is considerable variability between HRA methods.
3. The quantification of human errors – the calculation of a human error probability (HEP). Each HRA method features a different approach to quantification, including expert estimation, the use of PSF multipliers, Bayesian approaches, and

> simulations. The quantification determines the likelihood that the particular action modeled in the previous steps will fail. It is important to note that it is possible to have only qualitative HRA, which addresses insights particularly from the error identification phase but does not produce HEPs.

Most HRA specialists classify HRA methods as first and second generation. Boring (2012) points out that the guidance for classifying a particular method as first or second generation has not been entirely consistent. Indeed, there is no consensus in the literature when it comes to such classification. Hollnagel (1998), for instance, argues that so-called first generation HRA methods are the ones that do not consider cognition among their PSFs while second generation HRA methods explicitly consider and model cognitive PSFs. Atheana (US NRC, 2000), in turn, differentiates the generations according to the context and how it influences the error: first generation methods fail to consider the context in which humans made errors while second generation explicitly considers it.

Not all HRA specialists use the generation classification. Galizia *et al.* (2015), for example, distinguish between methods that are factorial (use performing shaping factors mostly related to the work environment and consider that PSFs have a direct impact on the task performance), contextual (model human activity primarily using the concept of Error Producing Conditions - context properties related to the history of the facility, the organization of the system, the characteristics of the interface, and they influence the nature and content of the performance of the task entrusted to the operator), and based on expert judgement (focus on determining error probabilities from estimates of expert judgment).

Nonetheless, as Boring (2012) points out, the HRA community has been generally more inclined to make use of the generational classification and has done so simply in terms of chronology. The oldest, first developed HRA methods are colloquially considered first generation methods, while subsequent methods—the descendants of the earlier methods—are considered second generation methods. A third generation methods would refer to simulation-based HRA, using virtual scenarios, virtual environments, and virtual humans to mimic the performance of humans in actual scenarios and environments (BORING, 2012). Hence, due to its popularity, this thesis makes use of the generational classification of HRA methods. The following section will thus approach first generation HRA methods and Section 2.2.2 will examine the so-called second generation methods.

2.2 HRA METHODOLOGIES REVIEW

2.2.1 First-generation HRA Methods

First-generation methods include between 35 and 40 methods. However, as Hollnagel (1998) remarks, it is safe to assume that some of them are variations of the same approach, and the number of significantly different HRA approaches is therefore smaller than it seems. Generally, they have in common the definition of PSFs, the use of the SRK cognitive method (skill-based, rule based, knowledge-based[6]), and the use of the error classification method according to the concept "omission-commission - *omission* identifies an action that is not done, is done late, or is done in advance; *commission* refers to the implementation of a performance by the operator that is not required by the process. First generation methods include THERP, HEART, SLIM-MAUD. The following subsection will briefly describe the THERP method. The relevance of THERP to HRA methods in general is obvious since it was the first HRA method to be formally presented.

2.2.1.1 THERP

As was previously mentioned in this chapter, THERP was the first formal HRA method to be presented. The aim of THERP is to calculate the probability of successful performance of activities needed for the execution of a task. THERP involves performing a task analysis to provide a description of performance characteristics of human tasks being analyzed. Results are represented graphically in an HRA event tree, which is a formal representation of required actions sequence needed (GALIZIA *et al.*, 2015).

An example of a THERP binary event tree is shown in Figure 3, diagramming the probability of misreading an analog meter.

[6] Skill-based behavior consists of the performance of more or less subconscious routines governed by stored patterns of behavior, e.g., use of a hand tool by one experienced with the tool. Rule-based behavior requires a more conscious effort in following stored (or written) rules, e.g., calibrating an instrument or using a checklist to restore locally operated valves to their normal operating status after maintenance. Knowledge-based behavior pertains to cases in which the task situation is, to some extent, unfamiliar--where considerably more cognition is involved in deciding what to do (SWAIN & GUTTMAN, 1983)

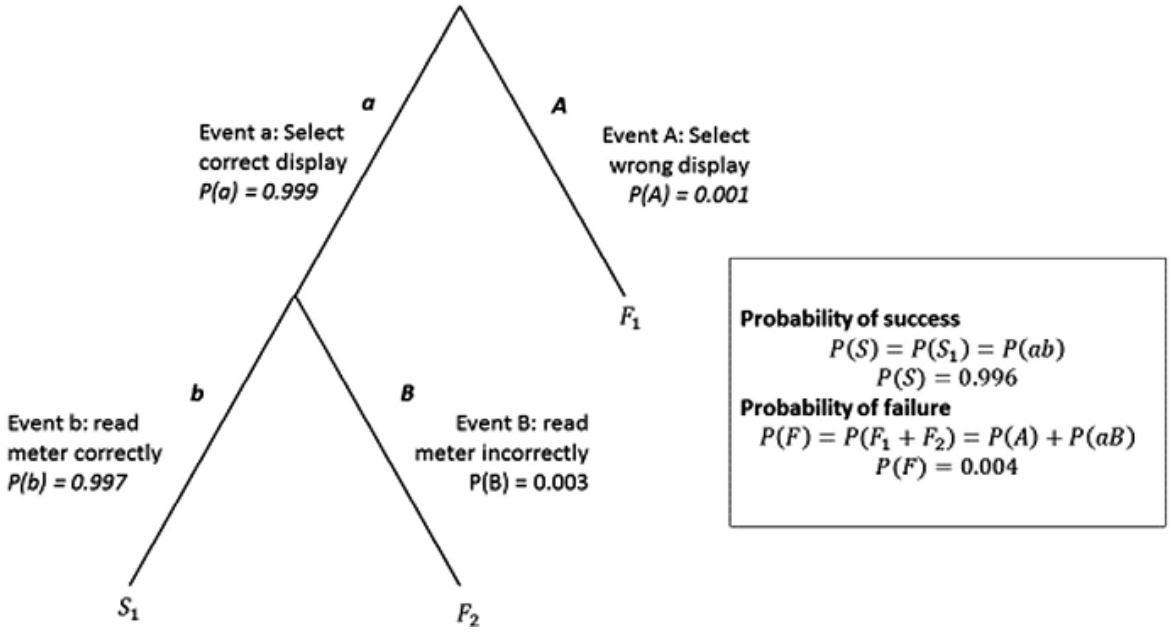


Figure 3: Example of THERP binary event tree (SHIRLEY *et al*, 2015)

THERP relies on a large human reliability database containing HEPs (Human Error Probabilities), which is based upon both plant data and expert judgments (GALIZIA *et al*., 2015). The nominal probability estimates from the analysis of the HRA event tree are modified for the effects of sequence-specific PSFs, which may include factors such as dependence between and within operators, stress levels, experience, quality of information provided, display types (HOLLNAGEL, 1998).

THERP consists of six steps (FELICE *et al*; 2012, HOLLNAGEL, 1998). Users must:

1. Define the system failures of interest. These failures include functions of the system in which human error has a greater likelihood to influence the probability of a fault, and those which are of interest to the analyst;
2. Identify, list and analyze related human operations performed and their relationship to system tasks and function of interest. This stage of process needs a comprehensive task and human error analysis. Task analysis lists and sequences the discrete elements and information required by task operators. For each step of task, possible occurring errors are considered by analyst and precisely defined. An event tree visually displays all events which occur within a system. The event tree thus shows a number of different paths each of which has an associated end state or consequence.
3. Estimate relevant human error probabilities;

4. Estimate the effects of human error on the system failure events. With the completion of the HRA, the human contribution to failure can then be assessed in comparison with the results of the overall reliability analysis;
5. Recommend changes to the system and recalculate the system failure probabilities. Once the human factor contribution is known, sensitivity analysis can be used to identify how certain risks may be improved in the reduction of HEPs. Error recovery paths may be incorporated into the event tree as this will aid the assessor when considering the possible approaches by which the identified errors can be reduced;
6. Review consequences of proposed changes with respect to availability, reliability and cost-benefit.

Swain and Guttman (1983) present a procedure with four phases for HRA to be applied through THERP:

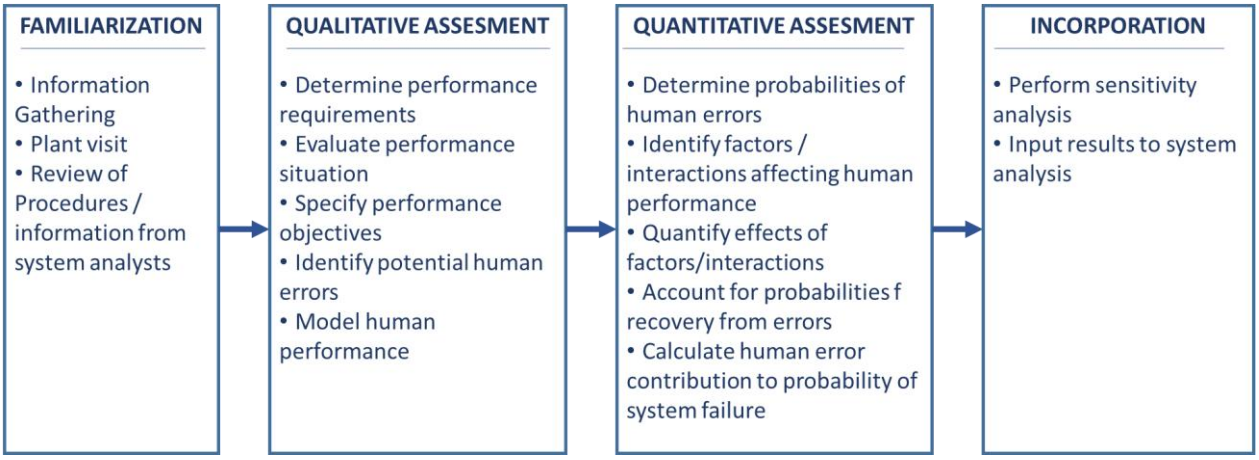


Figure 4: THERP application phases (SWAIN and GUTTMAN, 1983)

Swain and Guttmann (1983) state that the method is intended to assist trained risk analysts in quantifying human reliability. Hence, in order for THERP to be applied, a training is required. Indeed, when explaining the reasons for the abbreviated version of THERP, known as ASEP (Accident Sequence Evaluation Program), Swain (1987) states that, "… the THERP handbook is thorough, for its fullest application it requires considerable manpower and time on the part of a team of experts, including a human reliability specialist, systems analysts, plant personnel and others" (BELL, HOLROYD, 2009). Besides the required training, Kirwan (1994) summarizes THERP`s pros and cons as shown in Table 1.

Table 1:Pros and cons of THERP (Kirwan, 1994)

Pros	**Cons**
THERP is well used in practice	THERP can be resource intensive and time consuming.
It has a powerful methodology that can be audited	It does not offer enough guidance on modelling scenarios and the impact of PSFs on performance.
It is founded on a database of information that is included in the THERP handbook.	The level of detail that is included in THERP may be excessive for many assessments.

In addition to the elements mentioned in Table 1, Hollnagel (1998) states that THERP does not consider dependency between events and performance shaping factors since it uses binary event trees to model human actions. Finally, it is worth noting that although THERP has been applied to sectors such as offshore and medical, it was developed for probabilistic risk assessments of nuclear power plants, and has been extensively used in the nuclear industry, particularly in the USA. (BELL; HOLROYD, 2009). Interestingly, in the event of the 50 years of THERP's existence, Boring (2012) discussed its history and its significance to HRA by highlighting that all subsequent HRA methods are derived as a refinement of THERP or as an attempt to address perceived shortcomings with the original technique.

2.2.2 Second-generation HRA Methods

Second-generation methods, such as SPAR-H, CREAM, IDAC, try to overcome limitations of traditional methods. In particular, they provide guidance on possible and probable decision paths followed by the operator by using mental processes models provided by cognitive psychology. They also extend errors description beyond usual binary classification (omission-commission), recognizing importance of so-called "cognitive errors"; consider dynamic aspects of human-machine interaction (GALIZIA, 2015). The following subsection will explore in detail the SPAR-H method. The relevance of this method lies on the fact that is has been applied to oil operations and that it is currently being the object of modifications for use in this area, as will be further discussed throughout this chapter.

2.2.2.1 SPAR-H

SPAR-H - Standardized Plant Analysis Risk-Human Reliability Analysis method, was first developed in 1994 by the U.S. Nuclear Regulatory Commission (NRC) in conjunction with the Idaho National Laboratory (INL). It was initially called Accident Sequence Precursor

Standardized Plant Analysis Risk Model (ASP/SPAR). In 1999, based on the experience gained in field testing, this method was updated and renamed to its current denomination. The complete and current version was published in 2005 by the U.S.NRC (GERTMAN *et al*, 2005).

Chronologically, SPAR-H is a second generation method. However, if one considers context as a defining characteristic of second generation methods, SPAR-H falls short and might be considered a first generation method or even a hybrid (1.5th generation) method (BORING, 2012). The basic SPAR-H framework is the following (GERTMAN *et al*, 2005):

- It decomposes probability into contributions from diagnosis failures and action failures;
- It then accounts for the context associated with human failure events (HFEs) by using performance shaping factors (PSFs), and dependency assignment to adjust a base-case HEP;
- It uses pre-defined base-case HEPs and PSFs, together with guidance on how to assign the appropriate value of the PSF;
- It employs a beta distribution for uncertainty analysis, and
- Finally, it uses designated worksheets to ensure analyst consistency

Gertman *et al.* (2005) highlight that a number of HRA methods do not have an explicit human performance model. The SPAR-H method, however, is built on an explicit information-processing model of human performance. This human performance model is illustrated in Figure 5[7].

Eight PSFs were identified as being capable of influencing human performance and are accounted for in the SPAR-H quantification process (BELL and HOLROYD, 2009):

- Available time
- Stress and stressors
- Experience and training
- Complexity
- Ergonomics (& Human Machine Interface)
- Procedures

[7] For a detailed discussion on the components of the SPAR-H behavioral model the reader can refer to Gertman et al (2005).

- Fitness for duty
- Work processes

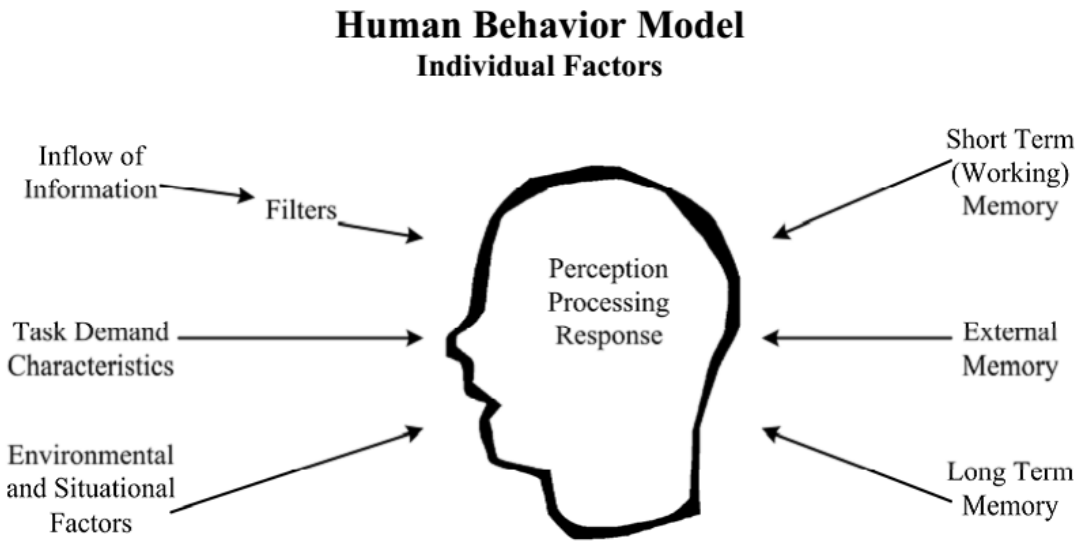


Figure 5: SPAR-H Human Performance model (GERTMAN *et al.*, 2005)

The potential beneficial influence as well as the detrimental influence of these factors is included in the method. SPAR-H addresses dependency trough ratings based on their combined effect on dependency among tasks, these correspond to zero, low, moderate, high or complete dependency among tasks. A major component of the SPAR-H method is the SPAR-H worksheet, which simplifies the estimation procedure. HEPs are determined by multiplicative calculation (i.e. Probability task failure x PSF1 X PSF2 x PSF3). Bell and Holroyd (2009) points out that Forester *et al.* (2006) consider that SPAR H is not a full scope HRA method in the sense that it does not provide guidance for identifying or modelling HFEs within the context of the PRA. Forester *et al*. (2006) list some pros and cons of SPAR-H, which can be seen in Table 2.

Finally, it is relevant to mention that SPAR-H was first developed for the nuclear sector and has been successfully applied to risk informed regulatory activities. Although Bell and Holroyd (2009) state that no evidence was found of the method being used in other sectors, some authors have applied SPAR-H to offshore industry scenarios, as will be noted in Section 2.5. Moreover, SPAR-H is being the object of adaptations by a research group for use in the Oil Industry, also discussed in Section 2.5.

Table 2: SPAR-H Pros and Cons (FORESTER *et al*., 2006)

Pros	**Cons**
A simple underlying model makes SPAR-H relatively easy to use and results are traceable.	The degree of resolution of the PSFs may be inadequate for detailed analysis.
The eight PSFs included cover many situations where more detailed analysis is not required.	No explicit guidance is provided for addressing a wider range of PSFs when needed, but analysts are encouraged to use more recent context developing methods if more detail is needed for their application, particularly as related to diagnosis errors.
The THERP-like dependence model can be used to address both subtask and event sequence dependence..	Although the authors checked the SPAH-H underlying data for consistency with other methods, the basis for selection of final values was not always clear.
	The method may not be appropriate where more realistic, detailed analysis of diagnosis errors is needed.

2.2.3 Current HRA Methods Shortcomings

The existing HRA methods present benefits and limitations. Although each method has its own specific weaknesses, as shown in the previous sections for THERP and SPAR-H, some general limitations for first and second generations methods can be listed. Hollnagel (1998) states that from the practitioner's standpoint, the first generation methods shortcomings refer mainly to (a) how the approaches are applied, and (b) the insufficient theoretical basis. Ahn *et al*. (2015) adds that a main drawback of these methods is its restricted power to describe situations of human performance - they would be therefore applicable only to tasks that are well defined as standard operation procedures. Tasks that require complex cognitive processes of judgment would be beyond the scope of first-generation HRA.

Ekanem *et al*. (2016) summarizes first generation methods major limitations as follows:

- Lack of procedures for identifying perhaps the most risk-significant category of human error, errors of commission (EOC), as compared with errors of omission (EOO);
- For the errors covered, the methods do not provide a convincing basis for error probabilities, and no theoretical foundations were offered for the quantification procedures;
- The limited experimental data used by some methodologies were insufficient to instill confidence in numbers on statistical grounds;

- Methods do not provide a causal picture of operator error – a need if one wishes to take steps towards reducing error probabilities;
- Methods were insufficiently structured to prevent significant analyst-to-analyst variability of the results generated.

As was mentioned in Section 2.2.2, second-generation methods were developed as an attempt to overcome some of these limitations. Ekanem *et al*. (2016) observe that these methods have a higher emphasis on context and operator cognition than first-generation methods. However, they indicate that second generation methods still have some limitations, which include:

- The lack of sufficient theoretical and experimental basis for the key ingredients and fundamental assumptions of many of these methods;
- The lack of a causal model of the underlying causal mechanisms to link operator response to measurable Performance Influencing Factors (PIFs)/PSFs or other characterization of the context;
- The majority of the proposed approaches still rely on very simple and in some cases implicit functions to relate PIFs to probabilities without the theoretical or empirical basis for such relations;
- In many instances, numbers are the result of expert elicitation, use of highly subjective scales, and unsubstantiated "reference probabilities".

As can be observed, both first- and second-generation methods offer several drawbacks even though HRA methods have shown significant advances in the last decades. In the light of overcoming the shortcomings listed above, and based on expectations from various authors on HRA methods, Mosleh and Chang (2004) have listed high-level requirements in the development of new HRA methods. They specify that an HRA method should enable analysts to:

- identify human response (errors are the main focus) in PSA context;
- estimate response probabilities; and,
- identify causes of errors to support development of preventive or mitigating measures.

Moreover, the method should:

- include a systematic procedure for generating reproducible qualitative and quantitative results,

- have a causal model of human response with roots in cognitive and behavioral sciences, and with
    - elements (e.g. PSFs) that are directly or indirectly observable, and
    - a structure that provides unambiguous and traceable links between its input and output
- be detailed enough to support data collection, experimental validation, and various applications of PSA. Data and model are two tightly coupled entities.

In addition, they add that that the model should be data-informed, and conversely the data collocation and analysis must be model-informed. Given the expectations listed above, Mosleh and Chang (2004) claim a model-based approach that provides explicit cognitive causal links between operator behaviors and directly or indirectly measurable causal factors should be at the core of the advanced methods.

Finally, Mosleh and Chang (2004) note that

- Only a causal model can provide both the explanatory and predictive capabilities. Without a causal model it is difficult for instance to explain why in some cases seemingly similar contexts result in different outcomes;
- Only a model-based approach provides the proper framework for tapping into and integrating models and data from the diverse scientific disciplines that address different aspects of human behavior;
- A causal model that explicitly capture the generic and more fundamental aspects of human response can be tested and enhanced using data and observations from diverse context. This is particularly important as the situations of interest in HRA are highly context-dependent and rare, meaning that adequate statistical data are unlikely to be available for a direct estimation of operator response probabilities;
- A generic causal model will have a much boarder domain of applicability, reducing the need for developing application-specific methods. For instance the same underlying model can be used for errors during routine maintenance work, as well as operator response to accidents;
- Only a model-based method can ensure reproducibility of the results, and robustness of the predictions;

A model-based Human Reliability Analysis framework was introduced in Mosleh *et al*. (2010) and Hendrickson *et al*. (2010), with an example application in Shen *et al*. (2010).

This model-based HRA was further developed at Mosleh *et al.* (2012) and Oxstrand *et al.* (2012). Ekanem (2013) improved several aspects of this method, developing a model-based methodology called Phoenix. Such methodology will be discussed in detail in the following section.

2.3 PHOENIX METHODOLOGY

As mentioned in Section 1, the Phoenix methodology was developed to overcome the limitations from existing first- and second-generation HRA methods as well as to provide a solution able to meet expectations listed in the previous section of this chapter. Hence, Phoenix is a model-based methodology that incorporates strong elements of current HRA good practices, leverages lessons learned from empirical studies, and takes advantage of the best features of existing and emerging HRA methods.

This section introduces the Phoenix methodology structure and elements since the methodology to be presented in Chapter 4 will build on them. In order not to repeat the works cited previously, which presents all elements of Phoenix in detail - in particular Ekanem (2013), this section provides an overview of Phoenix and avoids overemphasizing details. Since the methodology developed in this thesis was based on Phoenix, the understanding of its elements is necessary, but in-depth details on the CFMs and PIFs are not required. Thus, for details on the methodology, readers may refer to Ekanem (2013) and for an overview of the qualitative framework, Ekanem and Mosleh (2014,a) and Ekanem *et al*. (2016). The quantitative framework is also presented in Ekanem and Mosleh (2014,b).

Phoenix analysis framework has three main layers: the “crew response tree” (CRT) (top layer), the human performance model (mid layer) – which uses fault trees, and the PIFs (bottom layer), as can be seen in Figure 6. The next sub-sections details each of these layers.

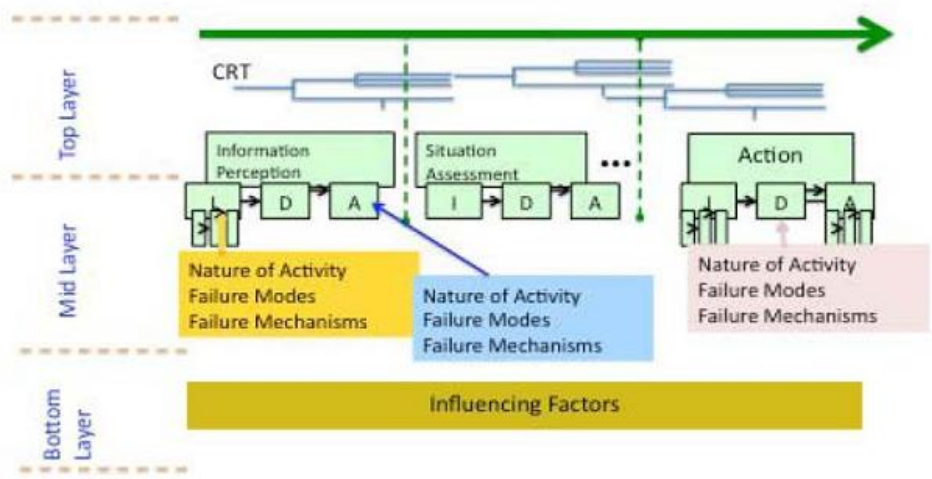


Figure 6: Phoenix's layers (MOSLEH *et al*, 2010)

2.3.1 Top Layer - Crew Response Tree

According to Mosleh *et al*. (2010) the crew response tree (CRT) is the first modeling tool for the qualitative analysis process. It is a forward branching tree of crew cognitive activities and actions, and acts as a crew-centric visual representation of the crew-plant scenarios. It provides the roadmap and blueprint that supports the performance and documentation of the qualitative analysis. Its role is to ensure a systematic coverage of the interactions between the crew and the plant that is consistent with the scope of the analysis being conducted, thereby providing traceability for the analysis. The CRTs can be constructed for crew response situations that are Procedure Driven (PD), Knowledge Driven (KD), or a Hybrid of both (HD)[8] (EKANEM *et al*, 2013).

In the CRT, each sequence of events indicates a graphical representation of one of the possible crew response across the entire accident sequence. This helps increasing consistency and reducing variability in the HRA task analysis. Moreover, the CRT can be used not only to find the paths to predefined HFEs and possible recoveries, but also as an aid to identify new HFEs (EKANEM, 2013). The CRTs are developed to model HFEs corresponding to a given safety function. Safety function, in turn, may refer to the intended function of a specific plant system, a desired state of the plant or system in response to plant upset, or a combination of

[8] The procedure driven response considers the operators are strictly following procedure as strategy. The knowledge driven response considers the operators are strictly following their knowledge as strategy, instead of written procedures.

both. Sometimes, there is more than one safety function along the path to the HFE (EKANEM *et al*, 2016).

Phoenix provides a flowchart in order to aid the analyst to construct the CRTs, with questions to guide the addition of branches to the CRT. It can be seen in Ekanem *et al.* (2016).

2.3.2 Mid Layer - Human Response Model

The mid layer comprehends the human response model – the human failure mechanisms and their causes. It captures the remaining aspects of the context through a set of supporting models of crew behavior in the form of causal trees that are linked to the CRT branches. Phoenix uses the crew centered version of the Information, Decision and Action (IDA) cognitive model as the basis for this linkage (SMIDTS *et al*, 1997). IDA is a three stage model and these stages serve as the basis for linking failure mechanisms to the possible human failures. The IDA stages are as follows (EKANEM, 2013; CHANG; MOSLEH, 2007a):

- I - Information pre-processing: This phase refers to the highly automatic process of processing incoming information. It includes information filtering, comprehension and retrieval;
- D - Diagnosis/ Decision making: In this phase the crew uses the perceived information and the cues from the previous stage, along with stored memories, knowledge and experience to understand and develop a mental model of the situation. In addition, the crew engages in decision making strategies to plan the appropriate course of action.
- A - Action: In this final phase the crew executes the decision made through the D process

Next sub-section details IDA stages and structure.

The crew errors are defined through the IDA stages. This means that the crew can:

- fail while information gathering (I stage);
- have the correct and complete information in hand, but fail in situation assessment, problem solving and decision making (D stage);
- have the correct and complete information and make a correct decision, but fail to execute the correct action (A stage).

Thus, Crew Failures Modes (CFMs) are used to further specify the possible forms of failure in each of the Information, Decision and Action phases (i.e. they represent the manner in which failures occur in each IDA phase). They are the generic functional modes of failure of the crew in its interactions with the plant and represent the manifestation of the crew failure mechanisms and proximate causes[9] of failure (EKANEM, 2013). Potentially, all CFMs are relevant to each CRT branch point and therefore each HFE.

Nonetheless, when an analysis is conducted in the context of a particular scenario, depending on the I-D-A phase, only a subset of the CFMs will apply. Therefore, Phoenix provides an initial set of fault trees to aid analysts in selecting the relevant CFMs for each branch point within each scenario. These fault trees were developed in order to bridge the gap between the fields of HRA and psychology/human factors and they are based on salient information from cognitive psychology literature. Phoenix´s set of fault trees can be seen in Ekanem (2013).

The next sub-section provides an overview of IDAC.

2.3.2.1 Overview of IDAC

IDAC (Information, Decision and Action in Crew Context) is an operator behavior model developed based on many relevant findings from cognitive psychology, behavioral sciences, neuroscience, human factors, field observations, and various first and second-generation HRA methodologies. It models individual operator's behavior in a crew context and in response to plant abnormal conditions (EKANEM, 2013). IDAC is well described in a series of five papers by Chang and Mosleh. The first of them (2007a) provides an overview of the model; the second one (2007b) details the performance influencing factors model; the third one (2007c) focus on the operator response model; the forth paper (2007d) details the causal model of operator problem-solving response; and, finally, the fifth one (2007e) provides a dynamic simulation of the model.

At a high level of abstraction, IDAC is composed of models of information processing (I), problem solving and decision-making (D), action execution (A), of a crew (C). Given incoming information, the crew model generates a probabilistic response, linking the context

[9] Proximate causes are categories of clusters of psychological failure mechanisms that can lead to failure in cognitive functions such as detection, understanding, decision making. Therefore, proximate causes are the consequence of psychological failure mechanisms and serves as the obvious indication of the more basic cause of failure to perform a function (EKANEM, 2013).

to the action through explicit causal chains (EKANEM, 2013). Hence, it combines the effects of rational and emotional dimensions when modeling cognition; which occurs through a small number of generic rules-of-behavior that govern the dynamic responses of the operator. Figure 7 presents IDAC operator cognitive model. The modeling blocks are (CHANG; MOSLEH, 2007a):

1. I Block - Information pre-processing: refers to the individual's highly automatic process of handling the coming information. This includes information filtering, comprehension and retrieval, relating and grouping, and prioritization, but stops before further inference and collusions.
2. D Block - Diagnosis and decision-making activities: this block covers the operator response phases of situation assessment, diagnosis and response planning. The cognitive response to an information obtained in the previous phase is translated into a problem statement or a goal, thus requiring resolution. The process of problem-solving or goal-resolution involves the selection of a problem-solving method or strategy. This involves a series of decisions to be made or solutions to be selected based on available alternatives.
3. A Block - Action execution process: executes the decision made through the D process. The actions are typically skill-based, requiring little mental effort.
4. MS Block - Mental state: influences the dynamic activities within the I-D-A blocks. The mental state combined with memory represents the operator's cognitive and psychological states. It explains why and how a response process initiates, why and how a cognitive activity starts and continues, and why and how a goal or strategy is selected or abandoned. The interaction between a mental state and the I-D-A activities is a dynamic process of mutual influence: the mental state influences the activities within each of the IDA blocks, and as a result of these activities the mental state is updated (dashed lines in Figure 7)

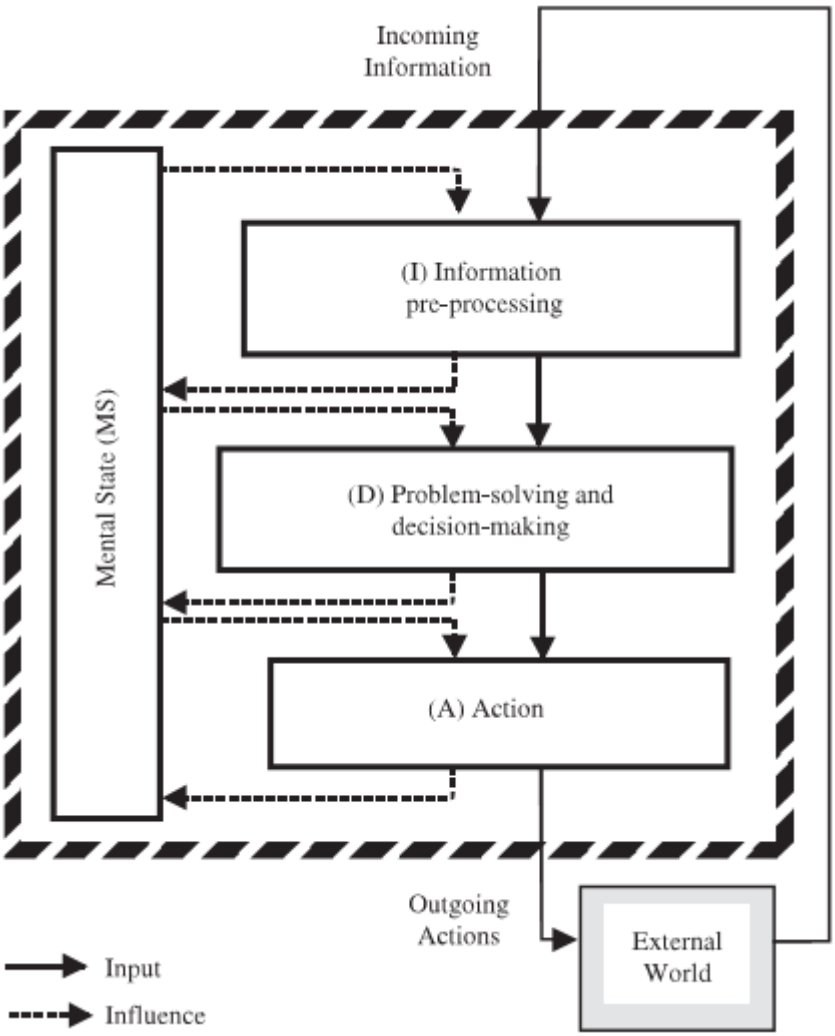


Figure 7: IDAC operator cognitive flow model (CHANG and MOSLEH, 2007a)

It is important to note that IDAC model includes a nested I-D-A structure, as can be seen in Figure 8. This means that the I block, for instance, involves its own I-D-A sub-processes - recognition of the incoming information (I in I); deciding how to process the information (keeping, discarding, merging) (D in I), and preforming the actions according to the decision (A in I).

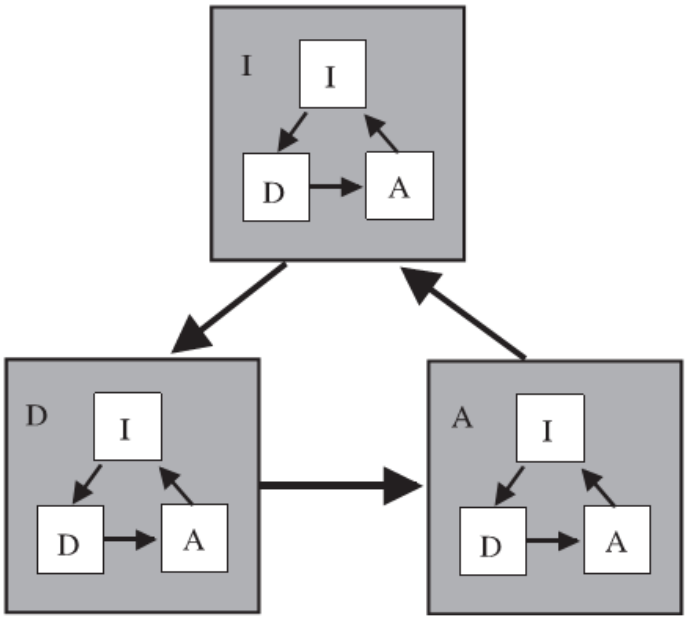


Figure 8: The nested I-D-A structure concept (CHANG and MOSLEH, 2007a)

2.3.3 Third Layer - Performance Influencing Factors

PIFs form the third layer of the qualitative analysis framework. PIFs, also referred to as performance shaping factors (PSFs), are context factors (including plant factors) that affect human performance and can either reduce or increase the likelihood of error. In this sense, PIFs are, in short, contextual factors that are not captured in the first two layers of the qualitative analysis (EKANEM, 2013). According to Ekanem (2013), presently, no standard set of PIFs have been adopted to be used by HRA methods.

Indeed, each HRA method uses a different set of PIF for its HEP quantification, many of which have overlapping definitions. While most of these PIF sets have some roots in human performance literature, they are not suitable for use in developing a causal model. This is due to the fact that they were only designed to be assessed by experts and not for model quantification. When the assessments of PIFs are done by experts, they can mentally compensate for the overlapping definitions, whereas using the same PIFs in a model requires the analyst to remove the overlap or explicitly capture the mental adjustment. Also, some of the available PIF sets do not contain adequate information to cover the different aspects of human-system interaction while other sets lack a differentiation between factors that influence performance and behavior that are used to indicate the state of these performance factors (EKANEM, 2013).

Phoenix's set of PIFs was initially based on the ones proposed by Groth (2009) and Groth and Mosleh (2012). Groth's set was created by aggregating information used in a number of HRA methods including IDAC, SPAR-H, CREAM, HEART, THERP. It also incorporates the PIFs from US NRC's Good Practice for HRA.

The CFMs and the PIFs are connected through Bayesian Belief Networks (BBNs). The BBN show paths of influence of the PIFs on each other and also on the various CFMs (EKANEM, 2013). BBNs are becoming a popular part of the risk and reliability analysis discipline because of their ability to incorporate both qualitative and quantitative information from different sources for analysis (EKANEM, 2013). The following sub-section presents a brief overview on BBNs.

2.3.3.1 BBN Overview

Borb and Nicholson (2003) define a Bayesian network as a graphical structure that allows to represent and reason about an uncertain domain. The nodes in a Bayesian network represent a set of random variables, $\mathbf{X} = X_1,..X_i,...X_n$, from the domain. A set of directed arcs (or links) connects a pairs of nodes, $X_i \rightarrow X_j$, thus representing the direct dependencies between variables. Assuming discrete variables, the strength of the relationship between variables is quantified by conditional probability distributions associated with each node.

BBNs are based on Bayes' theorem, which describes the probability of an event, based on prior knowledge of conditions that might be related to the event. It stated mathematically as:

$$P(A|B) = \frac{P(B|A)P(A)}{P(B)}$$

In which:

- P(A) and P(B) are the probabilities of observing A and B without regard to each other.
- P(A | B), a conditional probability, is the probability of observing event A given that B is true.
- P(B | A) is the probability of observing event B given that A is true.

An example of a BBN diagram is represented in Figure 9. In this diagram, node B and C are the parents of node A, which means that node A is their child. Node B, in turn, is the

child of nodes D and E. Nodes D and E have one child, but have no parents. Node A, finally, is an end node, i.e. it has no arc pointing out of it.

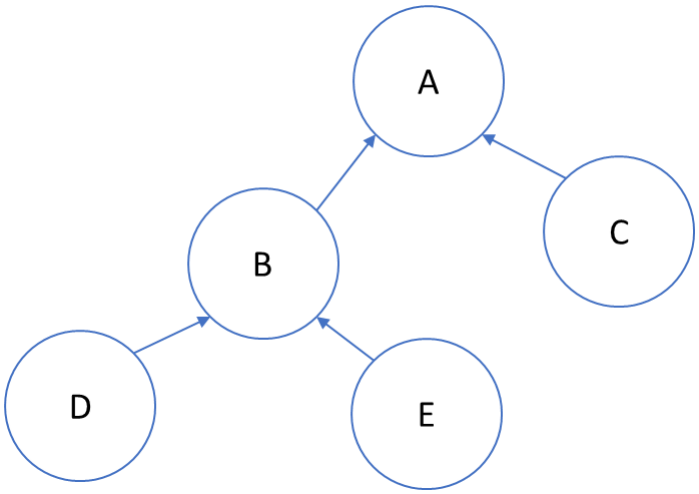


Figure 9: Sample BBN

Podoffilini *et al*. (2014) note that the use of BBNs is increasingly raising interest within the HRA domain. They point out that a reason is their natural ability to represent the joint effect of numerous factors that are possibly correlated and interacting. Another reason for the growing interests in using BBNs in HRA is that they can be built by aggregating heterogeneous sources of information: data and expert judgment of different forms[10]. Ekanem (2013) reinforces this last argument by highlighting BBNs' capacity to incorporate both qualitative and quantitative information from different sources for analysis.

In addition, Ekanem (2013) adds that BBNs provide the flexibility of updating the model (present state of knowledge) to incorporate new evidence as they become available. Also, they provide a causal structure used for modeling interdependences among elements of the system.

According to Podoffilini *et al*. (2014), applications of BBNs for HRA have addressed different issues. A number of studies have explored their multi-level modeling to integrate the quantitative treatment of management and organizational factors in HRA, as in Mohaghegh *et al*. (2009), Vinnem *et al*. (2012) and Trucco *et al*. (2008). BBN versions of existing HRA models were also proposed, as in Groth and Swiler (2013), which presents a Bayesian

[10] For reference, Ramos and Droguett (2013) can be read for use of two-step Bayesian analysis in cases where data are non-homogeneous

network version of the SPAR-H, and Kim *et al*. (2006), which used BBNs in the CREAM method. BBNs have also been applied in HRA on areas other than NPP operations, as in Martins and Maturana (2013), which applied it for HRA of an oil tanker operation. Mkrtchyan *et al*. (2015), finally, present a complete review of applications and gaps using BBNs for HRA.

In Phoenix, the end nodes are the CFMs, and its parents are the PIFs, i.e. it models the influence the PIFs have on the CFMs. Moreover, it can model the dependency, if there is one, between the PIFs and between the CFMs.

2.3.4 Phoenix Quantitative Framework

The final goal of quantification in HRA is to estimate the human error probability (HEP) for a particular human failure event (HFE). In Phoenix, an HFE is the result of one or several sequences of events (overall context) for a given plant PRA scenario (S) according to the CRT and corresponding linked causal models. The HEP can be estimated as follows: (MOSLEH *et al*, 2012 ; EKANEM and MOSLEH, 2012):

$$P(HFE|S) = \sum_{i=1}^{I} P(HFE|CFM_i) \left[\sum_{j}^{J} P\left(CFM_i \middle| F_{j1}, F_{j2}, \dots, F_{jn}; S\right) \times P\left(F_{j1}, F_{j2}, \dots, F_{jn} \middle| S\right) \right] \quad (1)$$

- The summation in the brackets is the probability of i-th CFM considering all possible CRT scenarios (j= 1,2,…, J) that lead to the HFE of concern. Each scenario is characterized by a set of n factors (or different instances of a fixed super set of factors). The set $\{F_{j1}, F_{j2}, \dots, S\}$ includes the usual PIFs and everything else in the scenario context (e.g. elapse time in a scenario, specific crew actions) that affect the probability of HFE.
- The term $P\left(CFM_i \middle| F_{j1}, F_{j2}, \dots, F_{jn}; S\right)$ is the probability of the i-th CFM given the context for a given CRT scenario S, and $P(F_{j1}, F_{j2}, \dots, F_{jn}|S)$ is the probability of the context given the particular PRA scenario S.

In theory, all PIFs need to be considered in estimating $P(CFM_i|F_{j1}, F_{j2}, \ldots, F_{jn}; S)$ and $P(F_{j1}, F_{j2}, \ldots, F_{jn}|S)$ for each CRT scenario j and CFM_i. However, the crew response modeling methodology provides a basis for down-selecting those PIFs that are most relevant to each CFM. The crew response modeling methodology also provides the minimal combination of CFMs that could lead to the HFE of interest - the CFM cut-sets. These CFM cut-sets together with the PIFs identified as relevant to the CRT scenarios are the main inputs to the quantitative analysis process. The CFMs are then quantified in order to obtain the estimated HEP for the HFE of interest using the BBN model.

The quantitative analysis process comprehends the steps illustrated in Figure 10.

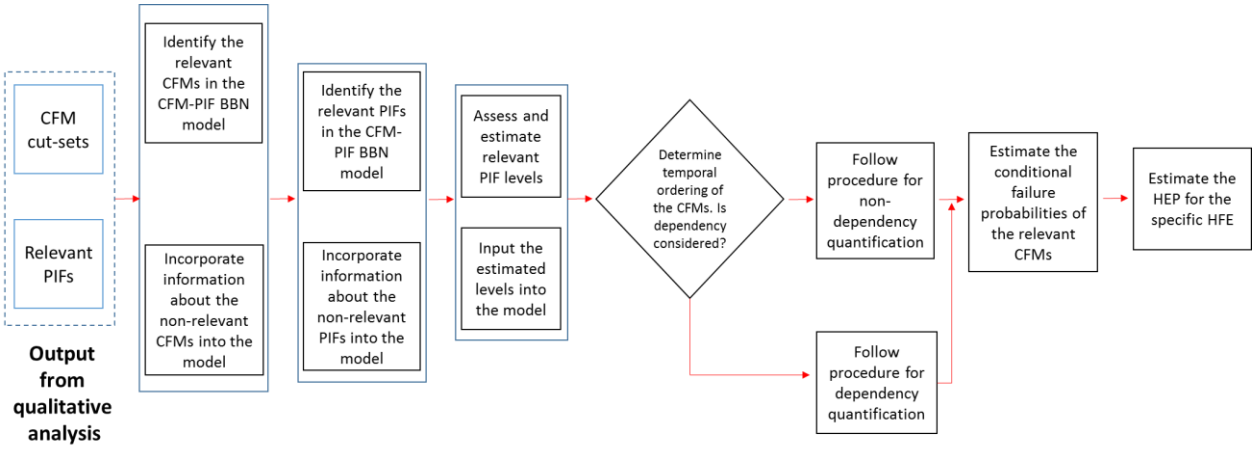


Figure 10: Overview of Phoenix Quantitative Analysis process (EKANEM, 2013)

The steps displayed in Figure 10 are well detailed in Mosleh *et al*. (2012), Ekanem (2013) and Ekanem and Mosleh (2014b). A summary of the mains steps is described below:

1. Identification of the relevant CFMs in the CFM – PIF BBN model: not all CFMs are relevant for a particular HFE. As explained previously, the relevant CFMs are identified as part of the qualitative analysis process and they form the CFM cut-sets. The other CFMs are considered "non relevant" to the HFE, which means that they have not occurred in the specific HFE. To incorporate it into the model, the analyst must:
    a. Open the conditional probability tables for each of the non-relevant CFMs;
    b. Change all the conditional probabilities for the failure state of each CFM to 0 (zero)

   c. Change all the conditional probabilities for the success state of each CFM to 1 (one)

2. Identification of the relevant PIFs in the CFM – PIF BBN model: Similarly to what occurs with the CFMs, not all PIFs are relevant to the particular HFE. The non-relevant PIFs are considered to not have an impact on the crew performance in the scenario. To incorporate it into the model the analyst must:
   a. Open the marginal probability tables for each of the non-relevant PIFs;
   b. Change all the levels for the nominal state of the PIF (marginal probability) to 1 (one);
   c. Change all the levels for the degraded state of the PIF (marginal probability) to 0 (zero).
3. Assessment of the relevant PIF levels: The levels of each of the relevant PIFs are assessed by the HRA analyst and then inputted into the model for each PIF node. Phoenix provides tables to be used for each PIF for the assessment of its level. After determining the levels of the PIFs, these estimates need to be inputted into the model. This is done through the following steps:
   a. Open the marginal probability tables for each of the PIFs.
   b. Change all the levels for the nominal state of the PIF (marginal probability) to reflect the estimated probability.
   c. Change all the levels for the degraded state of the PIF (marginal probability) to reflect the estimated probability.

Note that the analysts may change their assessment of the PIF levels as they go through the scenario. This information is incorporated into the BBN model in the form of evidence for that particular PIF node by either changing the levels of its states or by instantiating the PIF node to the appropriate state.

4. Determination of the temporal ordering of the relevant CFMs and estimation of the conditional probabilities of the relevant CFMs: The order in which the CFMs occur is an important factor in the quantification process. The HRA analyst has to determine if the CFMs will be quantified in terms of dependency or not in order to choose the right procedure for quantification.

   It should be noted that the issue of dependency is an ongoing issue that has been recognized and acknowledged in the HRA community, but has not been fully addressed. Although some methods do consider dependency, such as THERP and

SPAR-H, Ekanem and Mosleh (2013) points out that none of these has adequately addressed it. When considering dependency the analyst considers that early crew successes or failures will influence later crew judgments and subsequent actions.

a. Non-dependency quantification: considering an HFE consisting of two CFMs (CFM_1 and CFM_2), then $HEP = P(CFM_1 = 1) \times P(CFM_2 = 1)$ i.e., the human error probability is the probability of the occurrence of CFM_1 multiplied by probability of the occurrence of CFM_2. The estimate to the probabilities of a CFM given *n* PIFs is done through (2).

$$P(CFM \cap PIF_1, PIF_2, \dots, PIF_n) = P(CFM|PIF_1, PIF_2, \dots, PIF_n) \times P(PIF_1) \times P(PIF_2) \times \dots P(PIF_n) \quad (2)$$

Ekanem and Mosleh (2014b) provides a sample of the results of the joint conditional probabilities (JCP) of the CFMs given various PIF levels. The JCPs were generated based on an elaborate methodology used to aggregate data from different sources to form a representative estimate of the required BBN model parameters. However, the authors highlight that the results have not yet been subjected to the full spectrum of all data sources and expert review and hence should not be used for analysis at this point.

b. Dependency quantification: consider an HFE consisting of two CFMs (CFM1 and CFM2). If dependency is considered, then $HEP = P(CFM_1 = 1) \times P(CFM_2 = 1|CFM_1 = 1)$ i.e. the human error probability if the probability of the occurrence of CFM_1 multiplied by the probability of the occurrence of CFM_2 given that CFM_1 has already occurred. Ekanem and Mosleh (2013) provide a method to calculate the HEP using dynamic Bayesian analysis.

5. Estimation of the HEP for the HFE of interest: The final step in the analysis process involves the incorporation of the conditional probabilities of the relevant CFMs into the logic equation of the CFM cut-sets in order to obtain the estimated HEP for the HFE of interest.

Ekanem and Mosleh (2014b) remarks that one of the major issues in the field of HRA is the availability of the required type of data for analysis. To estimate the BBN model parameters (the data required for building the conditional probability tables for each of the 19 CFMs), they used data from different sources and aggregate them together using Bayesian methods in order to provide representative estimates. The sources of data currently used for parameter estimation include data from other HRA methods, expert estimates, and operating experience. They highlight, though, that the results have not yet been subjected to the full spectrum of all data sources and expert review and should not be used for analysis at this point.

Ekanem and Mosleh (2014b) point out that the Integrated Risk Information System (IRIS) software tool[11] can be used to support the quantification process. It was built by the Center for Risk and Reliability at the University of Maryland, College Park, USA. It uses a three-layer hybrid causal logic (HCL) modeling approach, which allows the application of different PRA modeling techniques to various aspects of the system. Deterministic causal paths are modeled using event sequence diagrams (ESD) which are similar to ETs and FTs while the non-deterministic cause-effect relationships are modeled using BBNs. Using this software Phoenix 1st layer (the CRT) can be modeled though the ESD, the 2nd layer (fault trees) is modeled trough the FT module, which links the CFMs to CRT branches, and the 3rd layer can make use of the BBNs module to build the CFM-PIF BBN and quantify it. Therefore, the integrated model (CRT, FT & BBN) is solved using the hybrid causal logic approach provided by IRIS software.

2.4 WHY PHOENIX?

The choice for Phoenix methodology as a basis to develop an HRA methodology specific to oil refineries and petrochemical plants operations in this work relies on the fact that it is a model-based methodology. Besides, it is a recent methodology which was developed considering the attributes that could make a robust HRA methodology for experts in HRA and related domains, listed in Mosleh *et al*. (2010). Ekanem (2013) presents a summary of how Phoenix attempts to achieve these attributes; the mains element are reproduced in Table 3.

[11] More information on IRIS can be seen at http://crr.umd.edu/software

Table 3: Phoenix HRA and Attributes of a Robust HRA Method (EKANEM, 2013)

No	Attributes of a Robust HRA Methodology	Phoenix HRA Methodology
1	Content Validity (coverage of plant, crew, cognition, action, errors of commission , errors of omission, etc)	CRT is used to model crew-plant interaction scenarios
		IDA (cognitive) model used to represent human cognition in terms of information processing, decision making, and action execution
		Errors of omission and commission modeled in the CRT and demonstrated using the example applications[12]
2	Explanatory power, "causal model" for error mechanisms and relation to context, theoretical foundations	CFM-PIF framework which links CFMs to PIFs based on possible causes of failure and mechanisms for human error
		BBN model used to represent the effects of the influence of PIFs on crew performance and for the estimation of HEPs
3	Ability to cover HFE dependency and recovery	Incorporates a methodology that adequately models and quantifies dependency among HFEs
		The ability of the crew to recovery from an error after it is made (global recovery) is incorporated into the CRT construction, while their ability to immediately realize and recover from an error while making it (local recovery) is incorporated into the conditional probability estimate of that particular failure mode
4	Ability to cover level of detail for various application	The crew is the unit of analysis and level of detail is determined by applying the task analysis guidelines provided[13]
5	Empirical Validity (of HEPs), e.g., having basis in Operational Data, Simulator Experiments, Other Industries	Model parameter estimation using:
		Data from operating experience (German NPP)
		Data from other HRA methods whose data is generated from a variety of sources which include data bases with roots in various industries such as nuclear, oil & gas, manufacturing, power transmission etc
		Expert generated estimates
		Data from future simulator training (SACADA data base)
6	Reliability (Reproducibly, Consistency, Inter- and Intra-rater Reliability)	The CRT provides a systematic coverage of the crew-plant interactions that is consistent with the scope of the analysis defined in the PRA model. It also supports the documentation and reporting of the analysis
		Task analysis guidelines have been provided to support task decomposition that is consistent with the level of detail required in the analysis

[12] The example applications of Phoenix in NPP scenarios can be seen in Ekanem (2013)

[13] Ekanem (2013) provides basic guidelines for task decomposition. In brief, the guidelines state that the level of decomposition can be based on i) the level of detail required in the PRA model; ii) the resources available for modeling and conducting the analysis; iii) the HRA requirements and purpose of the analysis; iv) the amount and type of information available; v) the success criteria for achieving the safety function.

Table 3 - continuation

		BBN modeling and quantification provides a means of obtaining consistent and reproducible estimates because the same results are guaranteed given the same set of inputs
		PIF level assessment methodology provides a means of obtaining consistent and reproducible estimates
7	Traceability/Transparency (ability to reverse engineer analysis)	The integrated model (CRT, fault trees and BBN) provides the ability to go from the HFE (modeled in the CRT) to the PIFs modeled in the BBN and vice-versa
8	Testability (of part or the entire model and analysis)	All steps of the analysis (both qualitative and quantitative) are proceduralized and provide explicit instructions and mechanisms for recording analyst choices and assumption made
9	Capability for Graded Analysis (screening, scoping, detailed analysis)	Hierarchial task analysis structure which is used for task decomposition to reflect the level of detail required in the analysis
		CRT can be constructed to reflect any level of detail, based on the analyst's definition of the safety function
		Hierarchial structure of PIFs provides the ability to incorporate data into the analysis at the required level of detail
10	Usability/Practicality	Examples given to demonstrate applicability in ASP, SDP, event assessment, power and shut down operations

2.5 HRA IN OIL REFINERY AND PETROCHEMICAL PLANT OPERATIONS: STATE OF THE ART

As was previously stated in this thesis, HRA can be considered a relatively new tool in the oil refining industry process safety and risk analysis. In recent years, however, HRA specialists have expressed an awareness in the need of using HRA in oil and gas operations in general. In this sense, some authors have been applying existing first and second generations HRA methods to oil operations scenarios while other studies have aimed at creating a solid and specific HRA method for such industry. This second trend (in which the present work would be categorized) comprises mostly the works related to the Petro-HRA project.

This Petro-HRA project, which is named “Analysis of Human Action as Barriers in Major Accident in the Petroleum Industry, Applicability of Human Reliability Analysis Methods”, is funded by the Research Council of Norway and the PETROMAKS program, with Statoil and DNV

GL as industry partners. The project aims to adapt SPAR-H for use in oil operations. Works that are part of this project include Laumman *et al* (2014), which presents the initial goals of the project; Taylor (2014), which presents considerations on qualitative data collection for HRA in the offshore petroleum industry; and, finally, Boring (2015), which provides an overview of some of the adaptations that would be desirable or necessary as a result of the differences between nuclear energy and oil and gas.

It worth noting, however, that the Petro-HRA project papers have so far indicated a strong focus on offshore installations, i.e. in oil drilling operations, rather than oil refining operations and petrochemical plants. Another strong difference between the present work and Petro-HRA project is the HRA method chosen to serve as a basis. Although SPAR-H has its recognized strengths, as shown in Sub-section 2.2.2.1, we believe that the Phoenix methodology is a stronger and more solid method, for the reasons stated in Section 2.3 and 2.4.

Applications of existing HRA methods in oil operations include the use of SPAR-H, as in Merwe *et al.* (2014) and Palttrinieri *et al* (2016). Both of them, though, in offshore oil platforms. The former presented an application in a hydrocarbon leakage scenario within a platform, and the latter addresses a scenario of drive-off of a semisubmersible drilling unit located in Norwegian shallow waters. Interestingly, Merwe *et al*. (2014) not only presents the application but also elaborates on the lessons learned from direct application of SPAR-H in the case study. The main issues they found were

- there were some challenges in making confident and accurate assessments for the PSFs on the basis of the existing guiding documentation;
- ensuring that PSFs were chosen such that overlap between PSFs was minimized was challenging;
- some PSFs may be too specific to the nuclear industry and may not transfer well to the petroleum industry;
- SPAR-H may inflate HEPs if assessments are made that are too stringent.

Other related works comprehends those in which the authors analyze human factors in oil refineries operations but do not perform full HRA, such as MacKenzie *et al.* (2007), Gould and Lovell (2009), Gholi-Nejad *et al.* (2012).

CHAPTER 3 – HUMAN ERROR IN OIL REFINERIES PAST ACCIDENTS

The petroleum refining industry plays a key role in modern life, providing fuel to a diverse range of essential activities. Petroleum refining processes makes it possible to transform the crude oil into useful product such as gasoline, kerosene and diesel. Refining processes can be classified as physical or chemical conversion ones; and the latter can also be classified as catalytic or thermal chemical conversion. The most important physical separation process is the crude distillation. In the distillation unit the crude oil is desalted and separated, in distillation column, into light and heavy products. The products of this unit follows each a different paths, some of them going through catalytic or thermal conversion in the hydrotreating, isomerization, coking, and other units. Each refinery can have a different configuration, depending on the characteristic of the crude oil to be processed and the desired products. Figure 11 presents a typical configuration of a modern refinery. A brief description of the main processes is laid out below, and details can be seen at Fahim *et al* (2009):

- Crude Distillation Unit: also known as atmospheric distillation unit. It receives crude oil and produces raw products that have to be further processed in downstream units. The crude oil is heated, desalted and partially vaporized, and enter the distillation column, in which the oil is separated into various fractions of different boiling ranges.
- Catalytic Reforming and Isomerization: Catalytic reforming is the process of transforming C7–C10 hydrocarbons with low octane numbers to aromatics and iso-paraffins which have high octane numbers. Isomerization, in its turn, Isomerization is the process in which light straight chain paraffins of low RON (C6, C5 and C4) are transformed with proper catalyst into branched chains with the same carbon number and high octane numbers.
- Thermal Cracking and Coking: Thermal cracking is the cracking of heavy residues under severe Delayed coking is a type of thermal cracking in which the heat required to complete the coking reactions is supplied by a furnace, while coking itself takes place in drums operating continuously on a 24 h filling and 24 h. emptying cycles.thermal conditions.

- Hydroconversion: hydroconversion is a term used to describe all different processes in which hydrocarbon reacts with hydrogen. It includes hydrotreating, hydrocracking and hydrogenation. Hydrotreating is the process of the removal of sulphur, nitrogen and metal impurities in the feedstock by hydrogen in the presence of a catalyst. Hydrocracking is the process of catalytic cracking of feedstock to products with lower boiling points by reacting them with hydrogen. Hydrogenation is used when aromatics are saturated by hydrogen to the corresponding naphthenes. The use of the hydroconversion technique depends on the type of feedstock and the desired products.

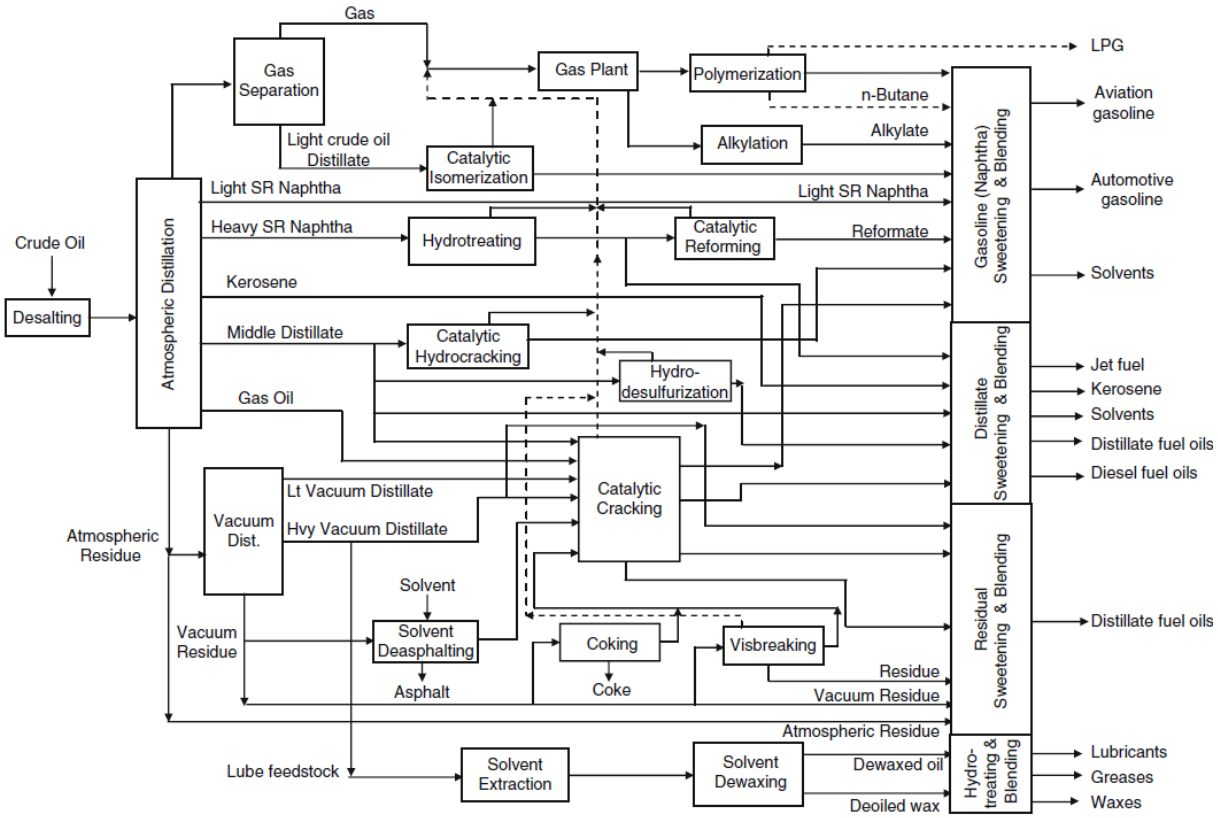


Figure 11: Modern refinery configuration (FAHIM et al., 2009)

Every year, many incidents in oil refineries' installations cause injuries, production delays, and financial loss. The previous chapter explored methods that have been widely used to assess human error. This chapter, in turn, will illustrate the relevance of doing so for oil refining-related installations. I will thus examine and discuss four major accidents that

occurred in refineries in the recent years and explain the role of human behavior in them as well; I will also discuss if a different behavior could have altered the unfortunate results. The four accidents are summarized below, but will be further analyzed throughout this chapter.

- In 1997, a piping suffered a rupture on the Hydrocracker unit at Tosco Avon Refinery in Martinez, California. The rupture released a mixture of light gases starting with methane through butane; light gasoline; heavy gasoline; gas oil and hydrogen, which instantly ignited upon contact with air causing an explosion and fire. The explosion killed a Tosco operator who was checking a field temperature panel at the base of the reactor and injured 46 Tosco and contractor personnel (EPA, 1998)
- As mentioned in the introductory chapter, the accident in BP´s Texas City Refinery in 2005 was one of the worst industrial disaster in recent U.S. history. The overfilling of the raffinate splitter tower during the startup of an isomerization unit resulted in a flammable liquid geyser from a blowdown stack that was not equipped with flares, which lead to an explosion and fire. The accident killed 15 people and injured another 180, and resulted in financial losses exceeding $1,5 billion (CSB, 2007)
- In 2010, the largest fatal accident at a U.S. petroleum refinery since the BP Texas City occurred in Tesoro Anacortes Refinery, Washington. A catastrophic rupture of a heat exchanger in the Catalytic Reformer/Naphta hydrotreter Unit released highly flammable hydrogen and naphta, which ignited and caused an explosion and a fire that lasted for more than three hours. Seven employees were killed in the accident (CSB, 2014a)
- In 2012, a catastrophic pipe rupture in the Crude Unit at Chevron Richmond Refinery released flammable hydrocarbon process fluid, which partially vaporized into a large vapor cloud that engulfed 19 Chevron employees and ignited. All of the employees escaped, narrowly avoiding serious injury. The ignition of the flammable portion of the vapor cloud and subsequent continued burning of the hydrocarbon process fluid resulted in a large plume of particulates and vapor traveling across the Richmond. 15000 people had to look for medical treatment (CSB, 2014b)

Detailed investigations of accidents in oil refineries, however, are not easily found. According to Nolan (2014), there is also an interest from companies not to publicize

information from incidents, except for major incidents during legal proceedings. This is done in order to portray their operations as safe and achieve greater public acceptance of process industry operations. Consequently, not all incidents that occur at these installations are reported. In other cases, still according to Nolan (2014), when incidents are reported they may be described in such fashion that the risks are not fully identified.

When it comes to accidents with serious consequences, though, such as the four ones mentioned above, detailed investigations are available. That is the case especially for recent accidents in the United States. The reason for that is that, since 1998, the U.S. Chemical Safety Board (CSB) operates to investigate accidents and determine the conditions that led up to the event and to identify the cause or causes so that similar events might be prevented. Moreover, their reports are public and available on their website.[14]

However, most investigations and research papers in general primarily analyze deep mechanical and chemical failures, such as corrosion, or other technical issues. In this sense, human failure events that could have contributed to the accident tend to be neglected. Yet, through the analysis and the examination of accident reports, it is possible to identify the causes of accidents and analyze the role human error may have played in them. And, as will be observed throughout the sections of this chapter, human error actually had a very relevant role in the accidents to be analyzed; these included the consequences of fatigue, of companies' lack of a safety culture, of failure to following procedures, and of the lack of adequate procedures, among others. It will be observed that, in some cases, different human actions could have avoided or mitigated the consequences of the mechanical and chemical failures outlined in such reports.

Given their serious consequences and the fact that detailed public accident investigation reports are available, the four accidents mentioned in this introduction will be analyzed in this chapter – these are, namely, the Tosco Avon Refinery accident (1997), the BP Texas City Refinery accident (2005), the Tesoro Anacortes refinery accident (2010) and the Chevron Richmond refinery accident (2012). Each accident will be discussed in detail in the following sections. Sections will not only describe the accident, but also examine the role of human action in its occurrence. This chapter, in this sense, aims at illustrating the relevance of understanding and assessing human error in the context of oil refineries and petrochemical plants. The following chapter, in turn, will explain the HERO HRA Methodology, which aims to do so by building on the Phoenix methodology described in Chapter 2.

[14] www.csb.gov

3.1 THE TOSCO AVON REFINERY ACCIDENT (1997)

The accident in the Tosco Avon Refinery in Martinez, California, was due to a piping rupture on the Hydrocracker unit, on January 21, 1997. The rupture released a mixture of light gases starting with methane through butane; light gasoline; heavy gasoline; gas oil and hydrogen – this instantly ignited upon contact with air, causing an explosion and fire. The explosion killed one Tosco Hydrocracker operator checking a field temperature panel at the base of the reactor; it also injured 46 Tosco and contractor personnel. Thirteen injured personnel were taken to local hospitals, treated and released. There were no reported injuries to the public.

The Refinery processed 140,000 barrels per day of crude oil, producing gasoline, jet fuel, and diesel fuel. Other products generated are coke, sulfur, ammonia, and sulfuric acid. The immediate cause of the rupture was excessively high temperature, likely in excess of 1400^{o}F. This high operating temperature was initiated by a reactor temperature excursion that began in Bed 4 of Reactor 3 and spread through the next catalyst bed, Bed 5. The excessive heat generated in Bed 5 raised the temperature in the reactor effluent pipe. Temperatures above certain limit, as stated in the procedures, require operators to activate a depressuring system, which they did not do. The U.S. Environmental Protection Agency investigated the accident, and the report generated by this investigation - EPA (1998) – is the most detailed document about this accident. The description of the accident in the subsection below is based on this report.

3.1.1 Description of the Accident

The hydrocracking process involves catalytic cracking of hydrocarbon oil in the presence of excess hydrogen at high temperature and pressure. It breaks larger molecules into smaller ones while reacting them with hydrogen. The higher the temperature, the faster the hydrocracking reaction rate. The heat generated from the hydrocracking reaction causes the reactor temperature to increase and accelerates the reaction rate. To control the reaction rate, each reactor has several catalyst beds in between and cool hydrogen is injected as quench gas for temperature control.

The Hydrocracker Unit in the Tosco Avon Refinery included four sections. The first section, a Hydrogen Plant, produces hydrogen for use in the Hydrocracker Unit and other

process units. The second section is the Stage 1 Unit, where the hydrotreating of the refinery gasoils in Reactors A, B and C takes place to remove sulfur, nitrogen compounds and other impurities, in order to prevent fouling of the Stage 2 catalyst. Cracking and hydrogenation happen in the third section, Stage 2 Reactors 1, 2 and 3. The last section is the Gas Plant, which fractionates the hydrocracked product from Stage 2 into propane, butane, light and heavy hydrocrackers, and diesel.

Stage 2 Reactors were monitored and controlled from the control room using board mounted instruments and a personal computer based data logger display. Temperature display panels located underneath the reactors were also used to monitor temperatures; however, this data could not be accessed from the control room. The reactors had a 100 psi per minute (psi/min) and 300 psi/min depressuring systems. These systems were designed to rapidly depressure the reactors to reduce the reaction rate and reduce the high temperatures in emergency situations.

The accident happened at Stage 2 Reactor 3. Figure 12 shows a simplified diagram of the Stage 2 system.

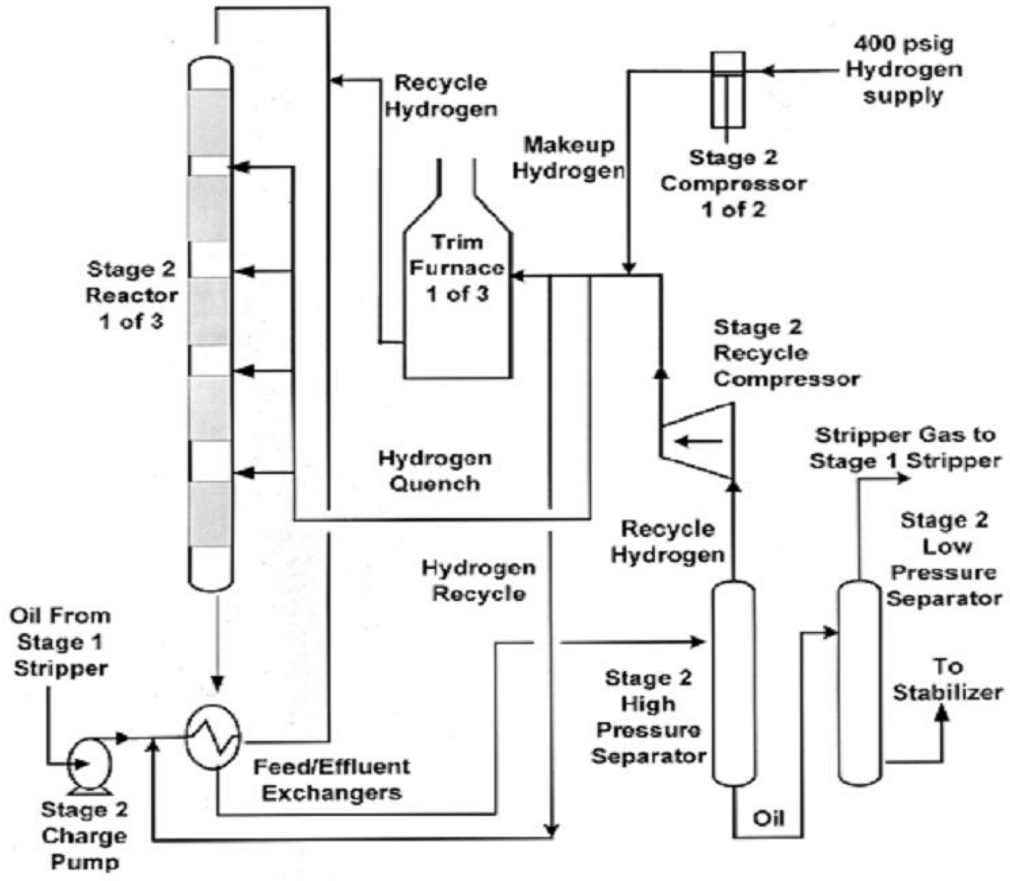


Figure 12: simplified flow diagram of Stage 2 Hydrocracker Unit (EPA, 1998)

The disturbance at the plant started at Stage 1 Reactor A. At about 4:50 am on January 21 1999, a clamp on the flange of the Reactor effluent exchanger began to leak. To stop the leak, the operators diverted the feed from Reactor A to Reactors B and C at about 5:20 am. The extra feed to these reactors lowered their temperatures, limiting the hydrotreating reaction. This caused the nitrogen content in the Stage 1 effluent to rise above the specified limit of 14 ppm: at 8:10 am, the nitrogen content of Stage 1 effluent reached 196 ppm.

According to the swing shift Stage 2 Board Operator, off-test tanks were full at such moment, not being available to receive the nitrogen. The high nitrogen content material from Stage 1 had thus to continue to Stage 2, which poisoned Stage 2 catalyst and declined cracking reaction. By 9:30 am, the quench flows to Stage 2 catalyst beds had begun to drop off, indicating a reduced reaction. Operators adjusted rates and temperatures in Reactors B and C in order to increase the reaction and reduce the nitrogen content in the effluent. At 12:13 pm, the Stage 1 stripper bottom nitrogen analysis was 66 ppm.

An operating plan was written in the shift logbook for the evening of January 21, to prepare for the introduction of oil to Reactor A which would take place the next morning at 8 am, once the leak of the exchanger had been repaired. The plan led operators to continue to raise the temperature in Reactors B and C at a reduced rate in order to get the nitrogen down to 5 ppm or less, and then to increase the rate to these two reactors as much as the nitrogen constraint allowed. In addition, it led operators to gradually increase temperatures in Stage 2 in order to drive the nitrogen off the catalyst.

On the swing shift (2pm to 10pm), two extra operators arrived to help with Stage 1 problems. At the start of the swing shift there were evidences indicating little or no reaction occurring at stage 2 and there were no light products in its low pressure section and only a few quench flow were above 10% of the full-scale flow. Stage 2 bed inlet temperatures varied from approximately 612 to 640^{o}F. At 5:38 pm, the nitrogen analysis for the Stage 1 stripper bottoms was 47 ppm.

At 7:34, it is reported that the Reactor 3 Bed 4 outlet temperature increased from 628^{o}F to 823^{o}F in 40 seconds. The data logger alarm sounded displaying a Bed 4 outlet high temperature and a high Bed 5 inlet temperature. The Stage 2 Board Operator heard the alarms and saw temperatures of about 690^{o}F on Bed 4 outlet and 890^{o}F on the Bed 5 inlet. Reactor 3, Bed 5 inlet temperature had risen from 637^{o}F to 860^{o}F within one minute. The strip recorder on the control panel for Bed 5 inlet temperature went from about 640^{o}F to full scale (800^{o}F).

Once Bed 5 inlet temperature were full scale, the hydrogen quench flow to Bed 5 began to open further to reduce the temperature, reaching 100%. Meanwhile, the makeup hydrogen to Stage 2 began to decrease. At that moment, the Stage 2 Board Operator expressed concern over a potential excursion and two operators joined him in evaluating the control board and data logger readings. They reported seeing the data logger temperatures to have started to bounce up and down, from normal range temperatures to 0 and back again. The Stage 2 Board Operator stated that Bed 4 and 5 temperatures were swinging from 0 to 1200^{o}F, then back to 650^{o}F. The No. 1 Operator stated that they could not trust the figures. At some time prior to 7:37 pm, a No. 2 Operator went to check the temperatures at the field panel under Reactor 3.

The sudden increase in quench flow to Bed 5 caused the hydrogen flow to the trim furnace to fluctuate. This, in turn, caused the hydrogen flow control valve to the trim furnace to open further. Since the trim furnace hydrogen is temperature controlled, this caused an increase in fuel gas flow – to heat additional hydrogen in the trim furnace, which caused a high flow alarm for the hydrogen flow to Reactor 1 trim furnace at 7:36:20pm. Bed 5 outlet temperatures, thus, decreased in response to the Bed 5 quench valve opening.

However, at 7:36:00, the Reactor 3 outlet temperature had increased 9 degrees in 20 seconds, from 641 to 650^{o}F, which the operators apparently did not notice. Operators said that they did not hear any other high temperature alarms. Throughout this time, operators reported that the temperatures on the data logger continued to “bounce up and down”, fluctuating between high, normal, and 0 temperature readings.

Between 7:36 and 7:37 pm, the fuel gas pressure at the Reactor 1 trim furnace had increased to 30 psi (the maximum limit was 28 psi). The extra No. 1 Operator reduced firing in the furnace to prevent overfiring. He took the trim furnace off temperature control and put it on fuel gas pressure control. Concerned about losing temperature in the reactor, the operator switched the Bed 5 quench flow controller from automatic to manual and closed the quench valve to Bed 5. By 7:37 pm, the Bed 5 outlet temperatures had all started to increase in temperature.

Once the Bed 5 outlet temperatures increased, the hydrogen makeup dropped to zero, and the Hydrogen Board Operator alerted the other operators of this change. He said the hydrogen plant was becoming over pressured, and excess hydrogen was directed to the header/flare system to prevent it. Indeed, at 7:39:02 pm, a high flow alarm for the hydrogen

blowdown to the flare occurred. The Stage 2 Board Operator noticed on the control board that the quench flow to Bed 5 had been manually closed, and at 7:38 pm, he re-opened it.

Between 7:38 and 7:39 pm, all four Bed 5 outlet temperatures rose above 780^{o}F, and continued to rise until they defaulted to zero at 7:39:20. At approximately 7:39 pm, operators heard a radio message from the No. 2 Operator, who had just checked the temperatures at the field panel under Reactor 3, but they reported the message was garbled and unclear. The Stage 2 Board Operator thought he heard “1250" on the radio, but he was actually not sure. Two unsuccessful attempts were made to contact him. Two operators (East Pad and extra No. 2 Operator) then went outside to check on him. Meanwhile, the reactor outlet temperature reading on the data logger defaulted to 0 at 7:39:40 pm.

After 7:40 pm, the strip chart readings for the reactor inlet and outlet temperatures continued to read off scale high. The reactor inlet temperature reached a maximum of 1234^{o}F on the data logger at 7:40:40 pm before defaulting to 0. Approximately at that time, the extra No. 1 Operator reached the shift supervisor by phone to request the assistance of an instrument technician to work on the temperature logger on Stage 2. Also at this time, the Stage 2 Board Operator noticed that the reactor inlet temperature had increased to over 800^{o}F.

In response to the increased temperature, the Stage 2 Board Operator reduced firing on the trim furnace and lowered the temperature set points to the top two beds. At 7:41 pm, the highest recorded temperature on the data logger was the Bed 5 Point 2 outlet temperature, which registered 1398^{o}F. At this time, the two outside operators had reached the northwest corner of the control room and the Stage 2 Board Operator was lowering the temperature set point on Bed 3. Finally, at approximately 7:41:20, the explosion occurred and was followed by a fire.

Indeed, a horizontal straight section of 12" diameter Reactor 3 effluent piping had ruptured just upstream of a 12"x 10" diameter reducer. The hydrocarbon and hydrogen mixture released from the pipe rupture apparently autoignited very shortly after the initial release, causing a fireball over 100 feet high. Immediately following the explosion, the 300 psi/min depressuring system was activated and operators began to shut down the unit. The hotspot was most likely caused by poor flow and heat distribution within the catalyst bed. Investigators from EPA could not determine the specific cause of the maldistribution.

The No 2 operator, who was in the process of checking the temperature panel located at the base of Reactor 3, was killed. He was severely burned as a result of being in close

proximity to the fire from the ruptured pipe. In addition, a total of 46 personnel were injured; eight were Tosco employees and 38 were contractor personnel. Injuries consisted of a fractured foot, emotional trauma, headaches, ringing ears, cuts and scrapes, and twisted knees. Thirteen injured personnel were taken by ambulance to local hospitals, treated and released.

3.1.2 Human Action Analysis

This subsection specifically focuses on the crew actions during the accident described above. Figure 13 below thus presents the timeline of Tosco Avon Refinery accident and highlights the human events.

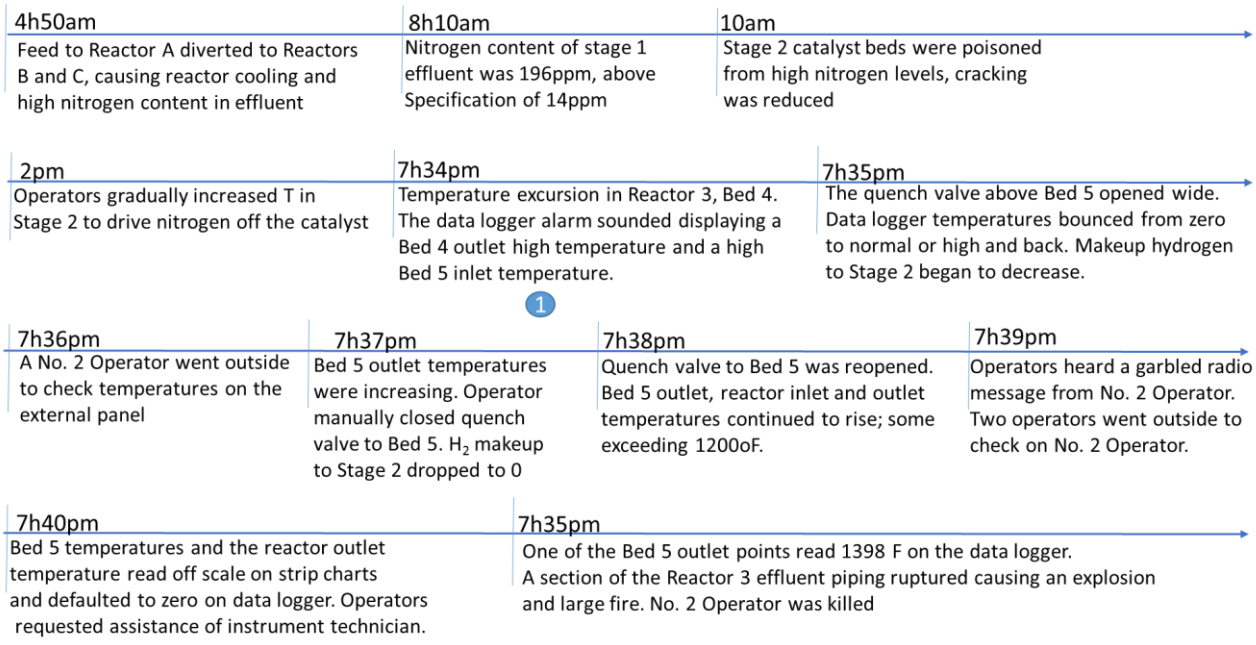


Figure 13: Timeline of Tosco Avon Refinery accident

The number 1 at the timeline represents the HFE: the high temperature alarm sounded, and indicators showed that the temperature was above 800^{o}F. The procedures stated that "for any reactor temperature 50^{o}F above normal or if any reactor temperature exceeds 800^{o}F, immediately activate the 300 psi/minute depressuring system" (EPA, 1998). The operators, however, did not follow the procedures, and did not depressurize the system. Instead, they tried to control the temperature rise by controlling the quench. According to the EPA report, the operators were confused about whether a temperature excursion was actually occurring.

The confusing temperature readings contributed to the operators not to follow the procedure regarding depressurizing the system. Since the data logger temperatures on the control room monitor were fluctuating between high, low, zero and then going back to normal, operators believed the readings were an error. The zero default values, however, potentially represented extremely high temperatures - over 1400^{o}F. Since operators were not well trained for abnormal situations, they did not understand the significance of these "0" readings. Moreover, they did not trust the temperature readings since the data logger had experienced malfunctions at times.

Since not all temperature data were accessible from the control room, the operators typically used the field panels to verify questionable control room readings or temperature excursions. This made Operator 2 go close to the reactors to check the temperature; he was thus there when the explosion occurred. Radio communication did not work well that day, and control room operators were not able to understand the garbled radio transmissions from No. 2 Operator outside. According to the EPA report, if the control room operators had received a report of high temperatures, they would perhaps have activated the depressuring system.

The temperature alarms also did not function well the day of the accident. When Bed 4 outlet and Bed 5 inlet temperatures exceeded the normal alarm setting, operators heard one high temperature. However, despite Bed 5 outlet and reactor inlet and outlet temperatures later exceeding high temperature alarm set points, operators did not receive additional audible high temperature alarms from the data logger. Another finding from the EPA investigation was that procedures were outdated and incomplete. They were not developed for many operations, including obtaining temperature data from outside field panels underneath the reactors. Also, procedures had conflicting differential temperatures limits for catalyst bed operation.

Interestingly, this was not the first time a temperature excursion occurred at the unit. During EPA interviews "many of the operators reported that they have experienced numerous temperature excursions, but most could recall only one instance when the unit was depressured using either the 100 or 300 psi/min system" (EPA, 1998). Their past practice on these situations had been to increase quench, reduce reactor inlet temperatures, and/or stop feed flow to the reactor. This indicates a lack of safety culture. According to the EPA, it was already a dangerous context: given its culture, it was an environment that caused operators to take risks while performing tasks and to continue production despite serious hazardous operating conditions.

Moreover, the operators stated that the depressuring system was not reliable. They said that they had encountered difficulties when it was activated in the past, including grass fires at the flare (and a generation of a cloud of flammable vapor. The lack of trust in the system could have contributed to the operators' reluctance to employ emergency depressuring and reinforced operators' decisions to handle severe temperature excursions by other means). As has been examined in this subsection, human behavior had a significant role in the Tosco Avon refinery accident.

BP Texas City Refinery Accident (2005)

According to CSB (2007), the accident in the BP Texas City Refinery on March 23, 2005, is one of the worst industrial disasters in recent U.S. history. During the startup of an isomerization unit (ISOM), the raffinate tower was overfilled, which led flammable liquid to a blowdown system that was not equipped with a flare, thus resulting in a flammable liquid geyser. The release of flammables led to an explosion and fire. In this accident, 15 persons were killed and 180 were injured. A shelter-in-place order that required 43,000 people to remain indoors was issued. Houses were damaged as far away as three-quarters of a mile from the refinery. The financial losses actually exceeded $1,5 billion. (CSB, 2007)

The BP Texas City Refinery was then the third largest oil refinery in the U.S., producing 10 millions of gallons of gasoline per day. The causes of the accident were a combination of multiple failures at different levels: instrumental, organizational and operational – these will be described in the subsection below, 3.2.1. Once these have been described, I will examine the human failures involved in the accident in Section 3.2.2. The more detailed study of the BP Texas City accident is the Chemical Safety Board Final Investigation Report (CSB, 2007); hence, the description of the accident to follow is a summary of that report.

3.2.1 Description of the accident

The accident took place in the isomerization unit, which was restarting after a period of maintenance. The isomerization process aims to alter the fundamental arrangement of atoms in the molecule. In the BP Texas City Refinery, it would convert straight-chain normal pentane and hexane into higher-octane branched-chain isopentane and isohexane for gasoline

blending and chemical feedstocks. The ISOM unit comprised four section: a desulfurizer, a reactor, a vapor recovery/ liquid recycle unit and a raffinate splitter. The accident happened in the raffinate section, which took raffinate, a non-aromatic, primarily straight-chain hydrocarbon mixture, from the Aromatics Recovery Unit (ARU) and separated it into light and heavy components. Figure 14 illustrates the process.

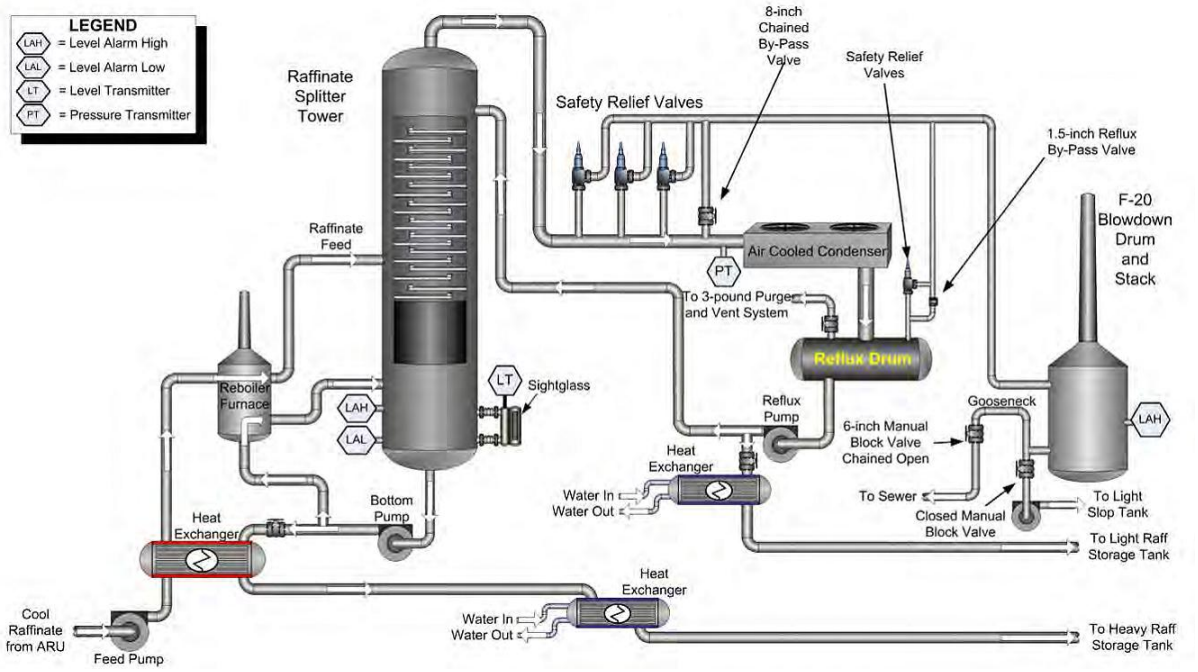


Figure 14: Raffinate Section of BP Texas City Refinery Isomerization Section (CSB, 2007)

The raffinate splitter section was shut down for maintenance and the raffinate splitter tower was drained, purged, and steamed-out to remove hydrocarbons. One month later, on 23 march, 2015, the startup of the section took place at 2:15a.m, and was conducted by the Night Lead Operator. The splitter tower was equipped with a level transmitter that measured the tower's liquid level in a 1.5m span within the bottom 2.7m of the 52m tall tower. It was also equipped with one alarm programmed to sound when the transmitter reading reached 72% of the bottom (2.3m), and a redundant high-level alarm to sound when the reading reached 78% (2.4m). During the startup, the level reached 99% on the transmitter, thus being beyond the set point of both alarms. However, only the first one sounded.

Although it was mentioned on the startup procedures that, during the startup, the level should be established at a 50% transmitter reading, it was not unusual for the operators to fill the bottom of the tower until 99%. They explained to CSB that they used to do it to avoid losing the liquid contents of the tower, which had happened in past startups, and thus avoid damaging any equipment. Once the equipment was filled, the startup stopped, the tower feed, and bottom pumps shut off. Even though startup procedures instructed that after a level was established in the tower, the tower level control valve should be on "automatic" and set as 50%, it remained in the "closed" position.

The Night Lead Operator, who had initiated the startup, left the refinery one hour before his shift ended. He briefly described to his supervisor and the Night Board Operator the actions he had taken during his shift, and added to the control room logbook "ISOM: Brought in some raff to unit, to pack raff with." In this sense, the Day Board Operator started his shift with little information on the state of the unit. The ISOM-experienced Day Supervisor, Supervisor A, arrived for his shift over an hour late, and did not conduct shift turnover with any night shift personnel.

In the early morning, a shift directors' meeting took place to discuss the raffinate startup. At the end of the meeting, it was agreed that the raffinate section would not be started. However, the instruction was not communicated to the ISOM operations personnel. Hence, Day Supervisor A told the operations crew that the raffinate section would be started. The startup resumed at 9:51 a.m. The Day Board Operator did not have the benefit of a written procedure showing him the complete list of the steps that had been initiated to indicate the exact stage of the startup. Yet, he restarted raffinate circulation and introduced feed into the splitter tower, which already had a high liquid level.

The tower instrumentation continued to show a liquid level less than 100% of the range of the transmitter. The tower was equipped with a level sight glass; however, it had been reported as unreadable because of a buildup of dark residue, as has been the case for years. Even though the tower level control valve was not at 50% on "automatic", as was required by the startup procedure, the Day Board Operator said he thought the condition was safe as long as he kept the level within the reading range of the transmitter.

As the unit was heating, the Day Supervisor, an experienced ISOM operator, left the plant at 10:47a.m. due to a family emergency. The second Day Supervisor was devoting most of his attention to the final stages of the ARU (Aromatics Recovery Unit) startup. Given that

he had very little ISOM experience, he did not get involved in the ISOM startup. Even though BP's safety procedures required an experienced supervisor or ISOM technical expert to the raffinate section startup, none was assigned after the Day Supervisor had left.

Around 10a.m. two burners were lit in the raffinate furnace, and approximately at 11a.m., operators lit two additional burners in the furnace. Although the transmitter indicated that the tower level was at 93% (2.64 m) in the bottom of the tower, CSB determined from post-accident analysis that the actual level in the tower was 20m. The fuel to the furnace was increased at 11:50a.m.; and, although the transmitter indicated the level was 88% and decreasing, the actual tower level was 30m.

At 12:41p.m., the tower's pressure rose to 33 psig due to the significant increase in the liquid level compressing the remaining nitrogen in the raffinate system. However, because it had happened in previous startups, the operations crew believed that the high pressure was a result of the tower bottoms overheating. The outside operations crew then opened the 8- inch NPS chain-operated valve that vented directly to the blowdown drum, which then reduced the pressure in the tower. At the time of the pressure upset, the Day Board Operator was concerned about the lack of heavy raffinate flow out of the tower. He thus discussed with the Day Lead Operator the need to remove heavy raffinate from the raffinate splitter tower. At 12:42p.m., the Day Board Operator opened the level control valve. However, heavy raffinate flow had not actually begun until 12:59 p.m.

Opening the valve made it possible for the total quantity of material in the tower to begin to decrease. However, it also heated the feed of the tower, exchanging heat from the hot bottom of the column with the feed through the heat exchanger. Heating the column contents caused the liquid level at the top of the column to continue increasing until it completely filled the column and spilled into the overhead vapor line; this led to the column relief valves and condenser. Heating from the furnace had created a temperature profile in the raffinate splitter column, such that cold liquid was on top and hot liquid was in the lower section, as can be seen in Figure 15.

Indeed, bubbles of hot vapor rising through the column contacted the overlying cold liquid, which rapidly condensed the vapor and heated the liquid. By the time of the accident, most of the column was heating at a fast pace and just a cold layer of liquid remained at the top. As the entire column approached the boiling point of the liquid, the vapor bubbles

accumulated instead of rapidly condensing. The resulting increase in volume from vaporization caused the liquid in the column top to overflow into the vapor line.

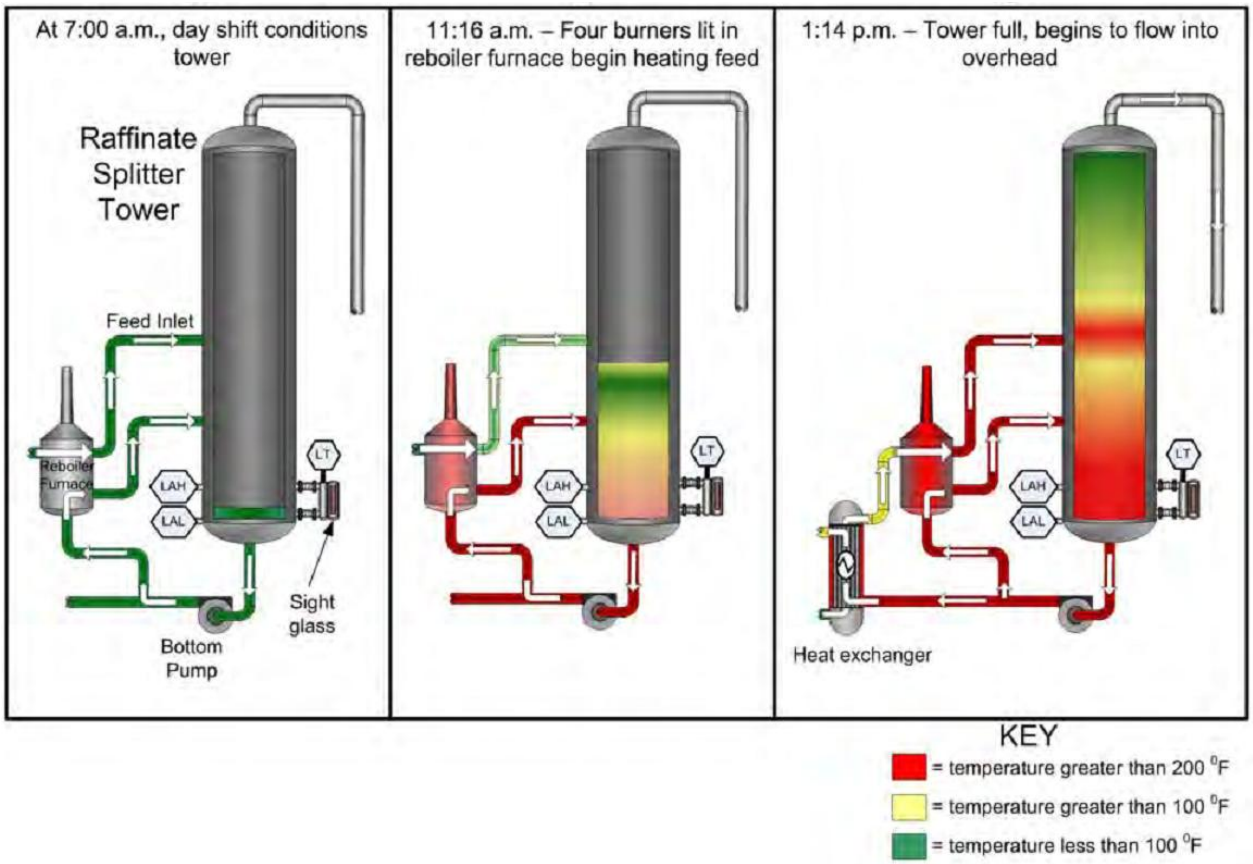


Figure 15: Temperature profile in the tower (CSB, 2007)

As the liquid filled the overhead line, the resulting hydrostatic head in the line increased. The tower pressure then combined with the increased hydrostatic head and exceeded the set pressures of the safety relief valves. The valves opened and discharged liquid raffinate into the raffinate splitter disposal header collection system. The crew was concerned with the high pressure, but noticed that the blowdown drum's high-level alarm had not sounded. They still thought that the overpressure was a result of a buildup of noncondensible gases or lack of reflux.

Given the events abovementioned, the crew fully opened the level control valve to heavy raffinate storage and shut off the fuel gas to the furnace from the satellite control room. As a result, the amount of material and pressure in the tower overhead line decreased. This caused the pressure to drop and the safety relief /valves to close after an estimated 196,500

liters of flammable liquid flowed from the valves into the collection header. The flammable liquid flowed from the overhead vapor line through the safety relief valves into the collection header for 46 seconds then discharged into the blowdown drum. Once the blowdown system filled, flammable liquid discharged to the atmosphere from its stack as a geyser and fell to the ground (Figure 16).

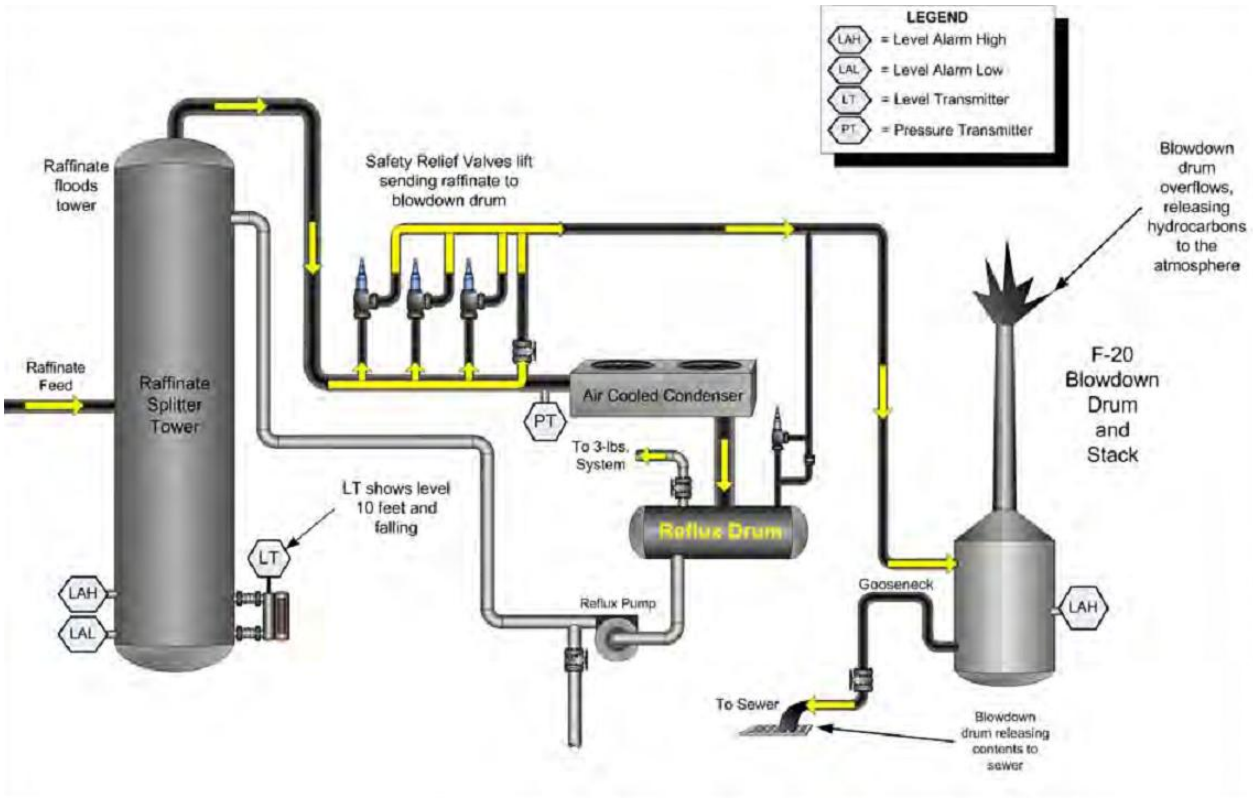


Figure 16: Tower is overfilled and sends hydrocarbons to blowdown drum, which overflows

Post-accident calculations showed that filling the blowdown drum and stack and additional safety relief valve headers took three minutes and 36 seconds; thus, the hydrocarbon liquid reached the top of the blowdown stack four minutes and 22 seconds after the safety relief valves started to flow. Once ignited, the flame rapidly spread through the flammable vapor cloud, compressing the gas ahead of it to create a blast pressure wave. Furthermore, the flame accelerated each time a combination of congestion/confinement and flammable mix allowed, greatly intensifying the blast pressure in certain areas. The burned area was estimated to be approximately 18,581 m^2.

The consequences of the explosion were extremely significant, ranging from small to fatal injuries. Indeed, 15 contract employees working in or near the trailers that were placed in

the surroundings of the ISOM unit were killed. A total of 180 workers in the refinery were injured; out of these, 66 had serious injuries and had to be away from work, adapt to a restricted work activity, and/or had to go through medical treatment.

3.2.2 Human Actions Analysis

The timeline in Figure 17 summarizes the accident described in the previous subsection. It also highlights the crew actions and interaction with the plant.

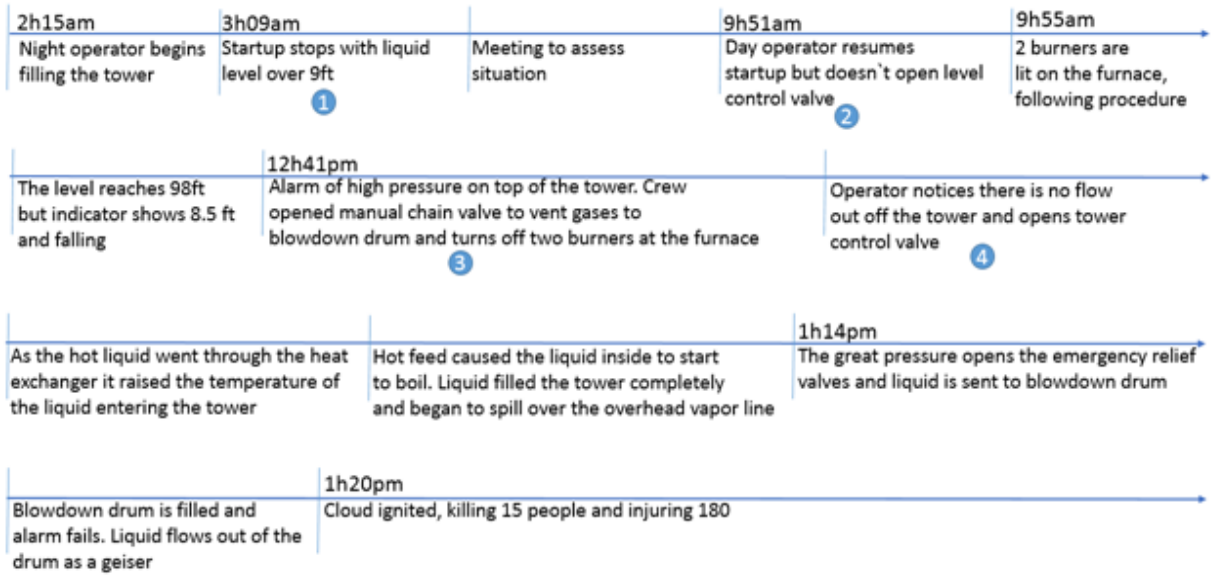


Figure 17: BP Texas City refinery accident timeline

The numbers 1-4 in Figure 17indicate the main human events in the timeline:

Event 1 – During the startup, the operators filled the tower above the level indicated in the procedure. The startup procedure called for the level in the tower to be established at a 50% transmitter reading, but it was filled until 99% of the transmitter reading.

Event 2 – The operator resumed the startup with the control valve closed. The procedures indicated that this valve should be open to control the level at the tower, but the operator received conflicting instructions.

Event 3 – The crew did not know the source of the high pressure and opened the valve to vent gases to blowdown the unit. However, the high pressure was due to the high level of liquid, which was compressing remaining gases on top of the tower.

Event 4 – Operators opened the control valve with the liquid being too hot. The liquid from the bottom of the tower exchanged heat with the feed of the tower. Therefore, opening this valve caused the rise of the temperature of the feed to enter the tower, This led to a high pressure over the emergency valves, which opened and sent the liquid to the blowdown drum.

As can be observed, the Event 1 is related to intentionally not following the procedures. As was previously mentioned, filling the bottom of the tower above 50% of the transmitter reading was not unusual during startups. CSB analyzed data from 5 years of ISOM startup, between 2000 and 2005, and in, most of them, the tower was filled above the value established in the startup procedure. The reason for that is that it was common for the tower to lose level during the startup, which would damage other equipment. The procedure was not updated to reflect this problem, and this can be seen as the most influential factor for this event.

Actually, according to CSB (2007), "when procedures are not updated or do not reflect actual practice, operators and supervisors learn not to rely on procedures for accurate instructions. Other major accident investigations reveal that workers frequently develop work practices to adjust to real conditions not addressed in the formal procedures". Moreover, also important, the management personnel allowed operators to make changes in the procedures without proper Management of Change hazard analysis: "All of these managerial actions (or inactions) sent a strong message to operations personnel: the procedures were not strict instructions but were outdated documents to be used as guidance" (CSB, 2007). This illustrated the weak safety culture of the company, which was also a factor of influence in the decisions of the operators.

The lack of safety culture regarding procedures was also influential for the Event 2 to occur. The procedures called for the level control valve to be put on automatic at 50%. However, the operators decided to close the valve, especially because of a miscommunication: the operator believed that the heavy staff storage tanks were full, and therefore should not send in more product. By relying on their own knowledge of the process, they ended up misdiagnosing the state of the plant: they did not believe that the level was already high and that adding more product could be dangerous.

Some factors strongly influenced the crew's behavior in relying on their own knowledge of the process: the failure of the redundant high-level alarm, and the failure of the level

transmitter, which showed the level decreasing while it was actually increasing. Indeed, the level of the transmitter could have been verified in loco using the sight glass; however, it was as unreadable because of a buildup of dark residue for several years. The tools the crew had to check the tower level were, therefore, unavailable or lacked quality. Moreover, the information on the panel was not adequate to check the imbalance between the input and the output from the tower: "the computerized control system screen that provided the reading of how much liquid raffinate was entering the unit was on a different screen from the one showing how much raffinate product was leaving the unit" (CSB, 2007). In addition to such factors, the operators did not receive adequate training for the hazards of unit startup, including overfill scenarios.

Furthermore, the operators were likely fatigued to be fit and alert enough to deal with an abnormal situation: the Day Board Operator had worked for 29 consecutive days, the Night Lead Operator had worked 33 consecutive days, and the Day Lead Operator – who was training two new operators, dealing with contractors, and working to get a replacement part to finish the ISOM turnaround work – had been on duty for 37 consecutive days. All of these individuals were working 12-hour shifts (CSB, 2007). The board operator, in turn, had his attention divided among other units beside that one; he was in charge of monitoring and controlling 2 other units besides the ISOM unit, which according to CSB report takes approximately 10.5 hours of a 12-hour shift to run under normal conditions. The ISOM unit was starting was an abnormal condition in which "critical thinking and decision-making […] goes beyond normal unit operation" (CSB, 2007).

Event 3 is related to a misdiagnose of the situation: the tower's pressure rose to 228 kPa due to the significant increase in the liquid level compressing the remaining nitrogen in the raffinate system. The operations crew, however, through that the high pressure was result of the tower bottoms overheating, which had not been unusual in previous startups. The majority of the 17 startups of the raffinate splitter tower from April 2000 to March 2005 exhibited abnormally high internal pressures. Fatigue, such as in the Event 2, was likely a big influence in this misdiagnose.

The CSB report illustrates how fatigue influences the crew's behavior. According to the report, they did not spend much time diagnosing why the pressure rose. In the hours preceding the accident the tower experienced multiple pressure spikes. Yet, in each instance, operators focused only on strategies to reduce pressure, rather than also questioning why the pressure spikes were occurring. The CSB report identifies this behavior as cognitive fixation

or cognitive tunnel vision – focused attention on an item or action needed for the execution of a task while disregarding other critical information. Such behavior, according to Rosekind *et al*. (1993), is a typical performance effect of fatigue. That fatigue can be related to BP's lack of culture in safety once again, as CSB highlights that it had no corporate or site-specific fatigue prevention policy or regulations.

Event 4, in turn, indicates the decision for a wrong strategy to fix the problem. At the time of the pressure upset, the Day Board Operator was concerned about the lack of heavy raffinate flow out of the tower. After a discussion with the Day Lead Operator, he opened the splitter level control, which led to rapid heating of the section of the raffinate splitter column above the feed inlet, as showed in Figure 2. Heating the column contents caused the liquid level at the top of the column to continue increasing. It thus completely filled the column and spilled over into the overhead vapor line, leading to the column relief valves and condenser. One of the reasons that affected the operators' decision to open the valve was the lack of awareness about the real situation of the tower level; that happened especially because of the malfunctions of the level indicator and failure of the redundant high level alarm. In addition, as was mentioned in this subsection, the operators' training for abnormal situations was inadequate.

Some factors related to the crew's motivation and commitment also likely affected all Events aforementioned. There are some indications of the lack of commitment such as the fact that the Night Lead Operator left the refinery approximately an hour before his scheduled shift end time; in addition, the ISOM-experienced Day Supervisor, Supervisor A, arrived for his shift at approximately over an hour late. The composition of the team responsible for the startup was not also not ideal. The Day Supervisor A was the only ISOM-experienced one, and, once he left the refinery for a family medical emergency, no technically-trained personnel was assigned to assist and supervise the Board Operator.

Hence, beside factors such as fatigue and lack of commitment, the crew also lacked an ISOM-specialist during the startup. It was unclear who was responsible for the ISOM unit supervision once Day Supervisor A left; thus, the one individual available to provide such supervision lacked the technical knowledge required. In addition, had the second Day Supervisor on shift (Supervisor B) left his work at the Aromatics Recovery Unit to assist in the raffinate startup, his presence in the control room would likely not have been helpful; he also had little technical expertise on the unit. The two Process Technicians (PTs) who had ISOM knowledge and experience were not assigned to assist with the startup.

3.3.TESORO ANACORTES REFINERY ACCIDENT (2010)

The accident regarding the Tesoro Refining and Marketing Company LLC petroleum refinery in Anacortes, Washington ("the Tesoro Anacortes Refinery") was one of the largest fatal accidents at a US petroleum refinery since the BP Texas City accident in 2005. The Tesoro Anacortes Refinery has been in operation since 1955, and had the capacity of 120,000 bpd of crude oil processing. The accident occurred, in short, because a catastrophic rupture of a heat exchanger in the Catalythic Reformer/ Naphta Hydroteater unit (the NHT unit) released highly flammable hydrogen and naphta at more than 500^{o}F. This ignited and caused an explosion and an intense fire that burned for more than 3 hours, killing seven Tesoro employees.

The immediate cause of the rupture of the heat exchanger was a mechanism known as High Temperature Hydrogen Attack (HTHA), which is a damage mechanism that results in fissures and cracking when carbon steel equipment is exposed to hydrogen at high temperatures as pressures. The operators' actions involved in the accident, however, contributed to the final result. The accident will be further detailed in the subsection below, which will be followed by the analysis of the operators' actions. Given that the Chemical Safety Board Investigation Report (CSB, 2014) is the more detailed document on the Tesoro Anacortes refinery accident, the description of the accident was mainly based on such report.

3.3.1 Description of the accident

The Naphta Hydrotreater is a process that removes sulfur, nitrogen and oxygen impurities from naphta through a reaction with hydrogen in the presence of a catalyst. It does so in order to protect the catalysts from contamination and improve the quality and environmental impact of the products. The hydrotreating reactions requires a high temperature which, at Tesoro Anacortes refinery, was attained by the heat exchangers before the reactor and the furnace, as seen in Figure 18. During normal operation, the two banks of heat exchangers, A/B/C and D/E/F, would be in use. However, the heat exchanger would foul during operation, developing a buildup of process contaminant byproducts inside and outside the heat exchangers tubes. These required, then, periodic cleaning.

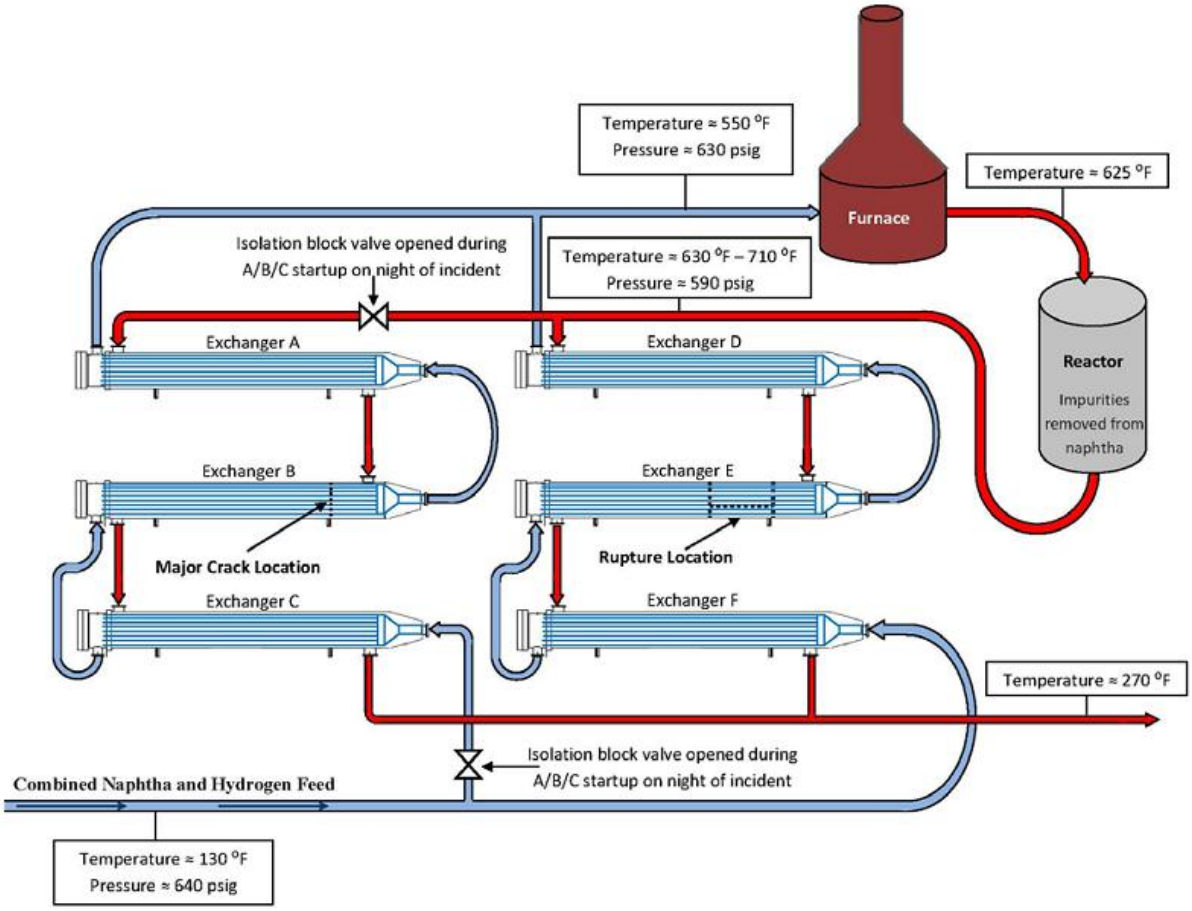


Figure 18: Process flow of the Tesoro Anacortes Refinery Naphta Hydrotreating unit

At the night of the accident, on April 2 2012, the heat exchanger bank A/B/C was being put to work again after a stop for cleaning. The unit staff were made of one board operator and one outside operator. The startup of the heat exchangers, however, was a very difficult assignment for only a single outside operator. The manipulation of the isolation block valves, as stated in the official procedure, needed a significant amount of manual effort to open. The operator had to gradually and concurrently open the valves, so he could not simply stay by each valve until it was fully opened or closed. At approximately 10:30p.m., six additional Tesoro employees joined the outside operator, following the request of the supervisor, to assist in bringing the A/B/C heat exchanger bank online. The startup procedure did not specify defined roles for these six additional personnel.

Two leaks from the heat exchangers were reported during the startup. According to CSB's investigation, leaks during startup of these heat exchangers were frequent and had become a "normal" part of it. Furthermore, based on past operating experience, operators expected these leaks to cease when the heat exchangers reached typical operating temperature.

At 12:30 a.m., while the seven outside personnel were still performing A/B/C heat exchanger bank startup operations, the E heat exchanger on the adjacent, in-service bank catastrophically ruptured. The rupture released a large volume of very hot hydrogen and naphtha. The naphtha and hydrogen likely autoignited upon release into the atmosphere, creating a large fireball. The fireball burned all seven outside operations personnel, and within 22 days of the accident they succumbed to their injuries.

3.3.2 Human Actions Analysis

The root cause of this accident in particular is mainly technical – the corrosion of the heat exchanger by the HTHA. However, had the operators followed startup procedures, there would not be seven people around the heat exchanger. Therefore, if operators had acted differently, they would not have avoided the corrosion and consequent rupture of the equipment, but the human losses would have been smaller. Human error, actually was not unusual in the Tesoro's NHT unit. An inspection of a team from OSHA Petroleum Refinery Process Safety Management National Emphasis Program (NEP) noted that from 2002 to 2007, the Catalytic Reformer and Naphtha Hydrotreater (CR/NHT) area experienced a total of 117 records related to process safety. Out of these, 36% were attributed to equipment failures, 33% human error, and the remaining 31% were attributed to the failure of a process control or safeguard.

Figure 19 presents the timeline of the accident described in the previous subsection. The number 1 indicates the human event.

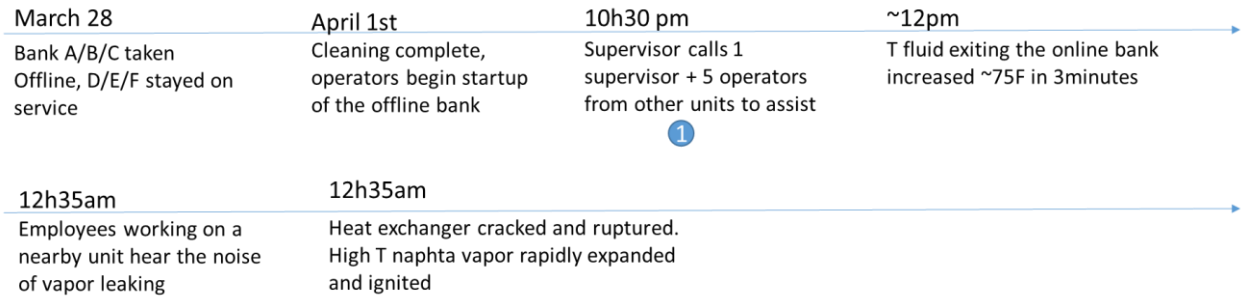


Figure 19: Tesoro Anacortes Refinery accident timeline

The Event 1 is related to not following startup procedures. The use of more personnel than the number called for in the procedure exposed more workers to the high-hazard activity.

According to CSB, an incident report describing a startup of the NHT D/E/F heat exchanger banks in March 2009 – a year before the April 2010 accident – demonstrates that normalization of hazardous conditions had been established at the refinery. The leaking of high temperature and highly flammable process fluids is a serious process safety incident. Nevertheless, it but was not addressed with such seriousness by Tesoro, which illustrated the deficiencies of Tesoro`s safety culture.

In addition, startup procedures actually did not reflect the actual status of the operation: the manipulation of the isolation block valves could not be done by one person, but the procedures would specify roles for only one operator working on the field. The CSB report also points out that the automation of the valves could have limited the role of the single outside NHT operator and thus minimized exposure to hazards. With automation, the task for the outside operator could have been reduced to simply opening the primary isolation block valves for the A/B/C heat exchangers (CSB, 2014).

3.4 CHEVRON RICHMOND REFINERY ACCIDENT (2012)

On August 6, 2012, a catastrophic pipe rupture took place in the Chevron Refinery in Richmond, California. The rupture of the pipe, a 52-inch long, 8-inch diameter carbon steel piping, released flammable hydrocarbon process fluid, which partially vaporized into a large vapor cloud that engulfed 19 Chevron employees and ignited. The ignition of the flammable portion of the vapor cloud and subsequent continued burning of the hydrocarbon process fluid resulted in a large plume of particulates and vapor traveling across the Richmond area. Although all of the employees escaped the explosion, approximately 15,000 people from the surrounding area had to seek medical treatment due to the release.

The immediate cause of the accident can be summarized as a sulfidation corrosion of the pipe, also known as sulfidic corrosion. It is simply a damage mechanism that causes thinning in iron-containing materials due to the reaction between sulfur compounds and iron ranging 450^{o}F to 1000^{o}F. The corrosion, however, was not the only cause of the accident. The analysis of the accident shows human failure events as well as organizational factors. The subsection below describes the accident; it will then be followed by a discussion on the role of human actions in the accident.

3.4.1 Description of the accident

The accident occurred in a distillation unit, with the rupture of one of the sidecuts of the distillation tower, as illustrated in Figure 20. The line operated at a temperature near 640°F and had an operating pressure of approximately 55 psig at the rupture location. At the time of the accident, light gas oil was flowing through the 8-inch line at a rate of approximately 10,800 bpd.

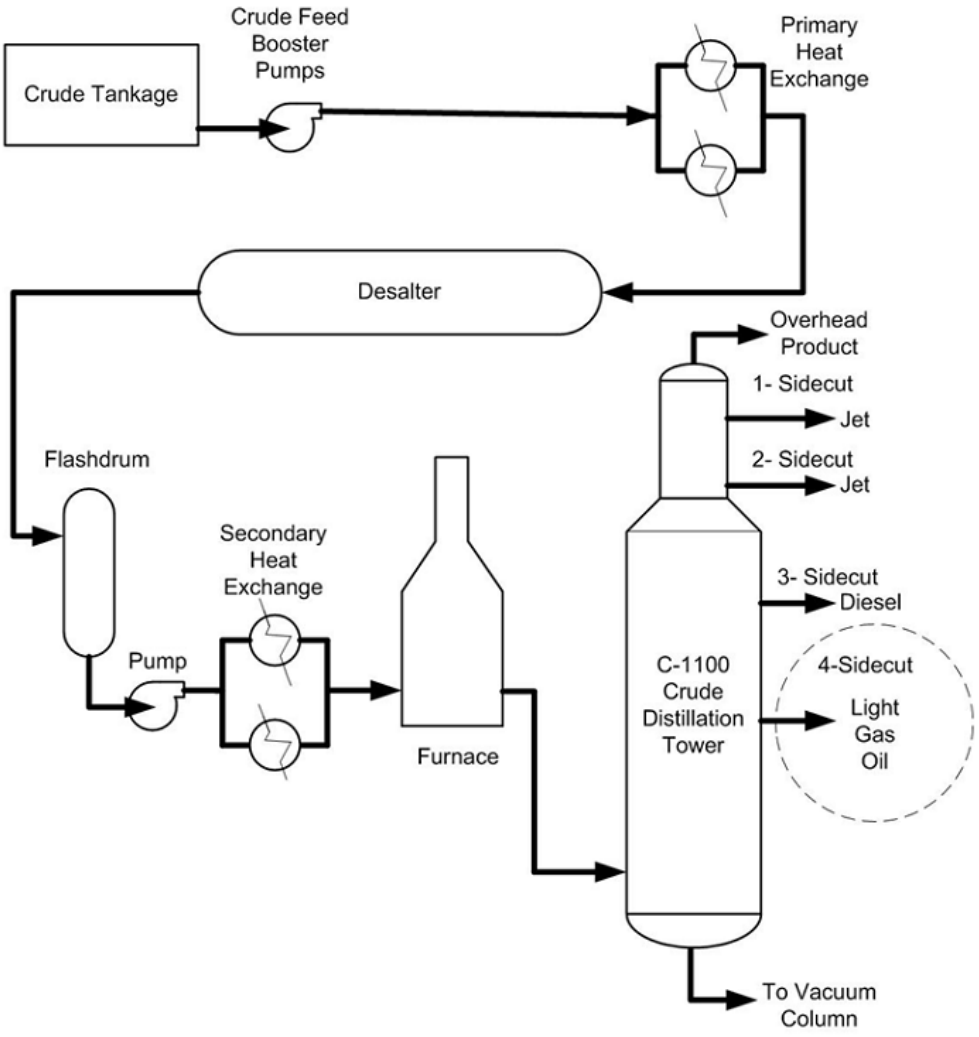


Figure 20: Schematic of Chevron Richmond refinery's Crude unit distillation tower

At approximately 3:50p.m. on August 6, 2012, an outside operator performing routine checks of piping and equipment found a puddle of what appeared to be a diesel-like material on the refinery concrete pad. The leaking pipe was identified to be a portion of the 4-sidecut piping that originated on the Crude Column. By visually analyzing the piping, the operator

determined that the line could not be isolated from the process. The supervisor and the shift team leader then arrived at the leak location. Yet, because the piping was insulated, the individuals gathered near the leak could not identify its precise source. They concluded that the leak was not significant enough to require a shutdown. Shortly after 4:00 p.m., they called the Chevron Fire Department to the scene, a typical practice for refineries when leaks are uncovered.

At approximately 4:15 p.m., many additional personnel were called to the scene of the leak to assist in the leak analysis. Two Chevron inspectors reported to the leak location to provide information on inspection history of the 4-sidecut line. The lead Crude Unit process engineer also arrived at the leak location to determine an estimate of the hole size and the quantity of material leaking so that proper environmental release calculations could be performed. At approximately 5:0p.m., the shift team leader left the scene of the leak and went to the control room. He directed the board operator to reduce the feed to the 4-sidecut line by 5,000 bpd.

The group discussed the options to mitigate or stop the leak. The inspectors informed the group that the 4-sidecut pipe walls were thinning due to sulfidation corrosion, but data collected as recently as two months prior indicated the 4-sidecut line had sufficient wall thickness to last until the next turnaround in 2016. This assessment led the group to believe that a localized mechanism, such as abrasion on the line from a pipe support near the dripping location, was the likely cause of the leak. The group then called the leak repair contractor to the leak location to assess the possibility of clamping the line in an effort to stop the leak.

They reached the decision to remove the insulation from the 4-sidecut pipe to determine the cause of the leak in order to help in deciding either to repair the leak on-line or to shut down the unit. The first attempt to remove insulation was made by pulling on the insulation bands from the ground using a pike pole. This, however, was unsuccessful. Rather, the piping actually moved from the force of the pulling, so the group determined it was too dangerous trying to remove the insulation in that way. The group then decided that scaffolding should be built to provide easy access so that firefighters could manually cut loose the piping insulation. Nevertheless, at this point, shift change was occurring: some individuals left for the day, and some volunteered to stay past their shift end time after their relief showed up. This change resulted in an increase of people standing near the 4-sidecut leak location.

Following this, three scaffold contractors built the scaffold beneath the leaking 4-sidecut pipe. Once the scaffolding was built, two firefighters were directed to climb the scaffold and remove the aluminum sheathing and insulation from the 4-sidecut pipe. The firefighters were ready for the possibility of vapors leaking from under the insulation and mixing with air, leading to a fire as the insulation was removed. Indeed, as the firefighters were removing the sheathing of the 4-sidecut line, white hydrocarbon vapor visibly began to emerge from under the then-exposed insulation material. The firefighters continued to remove the sheathing despite the formation of hydrocarbon vapor. During the continued sheathing removal, insulation that was soaked with hot 4-sidecut hydrocarbon autoignited once exposed to oxygen — only feet away from the firefighters. The hose teams immediately put out the fire, and both firefighters quickly came down from the scaffold.

The firefighters on the scaffolding successfully removed much of the aluminum sheathing surrounding the insulation; however, underlying insulation still obscured the location of the leak. Directed by the operations personnel, the Chevron Fire Department sprayed the insulation by straight streaming the fire hoses in an attempt to knock the insulation off the pipe. The hose teams knocked off the insulation up to the location where the aluminum sheathing had been removed. At this point, they realized that the leak had significantly worsened; hydrocarbon liquid was then spraying from the pipe. Several operations managers present decided to shut the unit down, an action that required hours to complete.

A vapor cloud quickly began to accumulate. The hose teams attempted to keep the cloud at bay by spraying it with firefighting water. Suddenly, the vapor cloud worsened, thus engulfing 19 firefighters and operators standing in both the hot and cold zones in the hot hydrocarbon cloud. One person caught in the cloud told CSB that he could not see his hand if he had held it directly in front of his face. Each person engulfed in the cloud began working their way out of the vapor cloud. At approximately 6:30p.m., two minutes after the large vapor cloud had formed, the light gas oil ignited. Eighteen employees safely escaped from the cloud just before ignition. One employee, a firefighter, was inside a fire engine that was engulfed in the fireball when the light gas oil ignited, but also escaped.

The leak resulted in a large plume of vapor which traveled across the surrounding area. The ignition and subsequent burning of the hydrocarbon process fluid created a large black cloud of smoke, which also swept across the surrounding area. This situation resulted in a Community Warning System (CWS) Level 3 alert, and a shelter-in-place advisory (SIP) was

issued at 6:38 p.m. for Richmond, San Pablo, and North Richmond. In the weeks following the accident, nearby medical facilities received over 15,000 members of the public seeking treatment for ailments including breathing problems, chest pain, shortness of breath, sore throat, and headaches.

3.4.2 Human actions analysis

The timeline of the accident can be summarized as below. The crew actions and interaction with the plant are highlighted and can be observed in Figure 21.

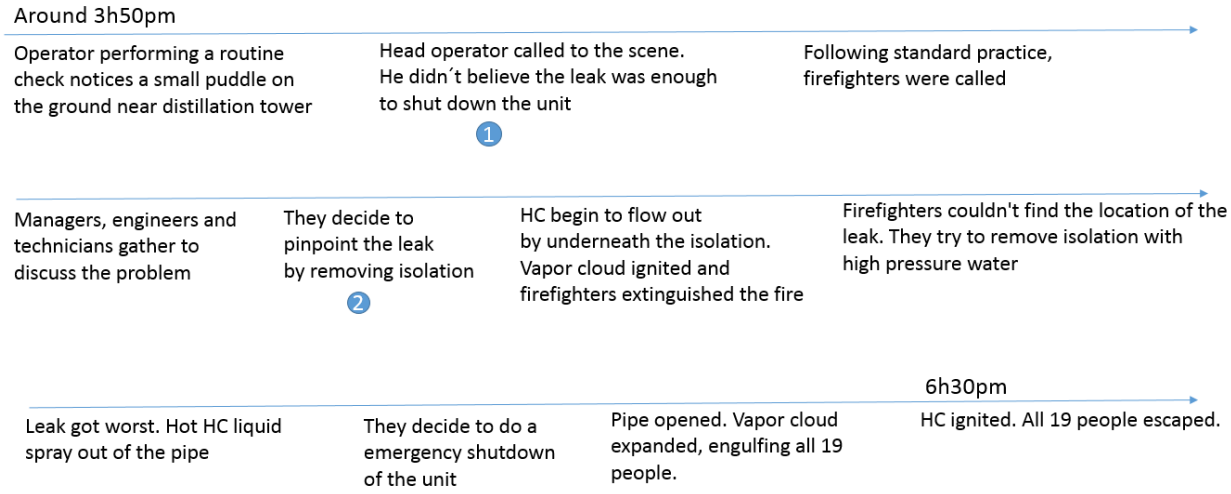


Figure 21: Chevron Richmond refinery accident timeline

The numbers 1-2 in Figure 3 indicate the main human events in the timelines and are related to a crew failure mode:

Event 1 – The head operator misdiagnosed the state of the plant, believing that the leak was not big enough to shut down the unit. He did not realize how corroded was the pipeline.

Event 2 – The crew decided to remove insulation of the pipe, first by pinpointing the leak by and then using high pressure water. This actually made the leak worse since the pipeline walls were already too thin due to corrosion.

Event 1 is related to a misdiagnose of the situation. The supervisor and the team leader arrived at the leak location and could not identify its precise source, because the piping was insulated. They concluded that the leak was not significant enough to require a shutdown, but

was still a serious situation. One of the reasons for this misdiagnose was the lack of awareness about the thickness of the pipe: "the inspectors informed the group that the 4-sidecut pipe walls were thinning due to sulfidation corrosion, but data collected as recently as two months prior indicated the 4-sidecut line had sufficient wall thickness to last until the next turnaround in 2016" (CSB, 2014).

In 2010, there was thus a miscommunication between the design engineer and the inspector in reviewing results of structural minimum thickness. Moreover, at the time of the accident, Chevron did not have procedures that explained when a unit should be shut down. By the new guidelines developed after the accident, if a similar leak were to occur in a Chevron refinery, the unit should be shutdown. The CSB's investigation also suggested a lack of safety culture at Chevron at the time: evidence indicated a type of decision-making that actually encouraged continued operation of a unit despite hazardous leaks.

During Event 2 the team chose an inappropriate strategy to deal with the leak: to remove the insulation in order to determine the cause of the leak and help in the decision either to repair the leak on-line or to shut down the unit. Not having the correct information about the status of the pipe influenced the operators in this decision, as had happened in Event 1. Had they have the correct information in hand, the team could have realized that clamping the pipe was not a viable solution because the pipe likely did not have the structural integrity to support a clamp.

Moreover, several Chevron Fire Department personnel responding to the event were informed that the operating temperature of the line was 130°F rather than the real temperature approaching 640°F. If the responders were aware of the actual operating temperature, some of them could have raised concerns to their supervisors about the safety of performing aggressive leak response actions on a hot pipe. CSB identified that this misunderstanding might have occurred because, during the initial accident response, much of the focus was on determining the flash point of the 4-sidecut fluid.

Safety culture findings from CSB's investigation likely affected both Events. Chevron management made use of "Stop Work Authority" which was defined as "responsibility and authority of any individual to stop work when an unsafe condition or act could result in an undesirable terms". However, the operators were not encouraged to make use of this authority. According to CSB (2014), there are a number of reasons why such a program might fail, especially where shutdowns are being considered: the belief that the Stop Work decision

should be made by someone else higher in the organizational hierarchy, reluctance to speak up, and delay work progress, and fear of reprisal for stopping the job.

3.5 THE IMPORTANCE OF HUMAN ERROR IN PAST OIL REFINERIES ACCIDENTS

As can be seen by the analysis of the accidents in the sessions above, human error is strongly present in recent and severe oil refineries accidents. It can play a “minor” role, as in Tesoro Anacortes accident, which could not have been avoided even if there was no human error, or a major role, as in the BP Texas City accident.

This analysis is extremely important to understand how and why can the operators fail to act to bring the plant back to safety in face of a disturbance, or how and why can themselves initiate a disturbance in the plant - or even enhance it, as in the case of the Chevron Richmond accident.

The analyses of the accidents above will serve as a basis for HERO HRA Methodology development, and the human actions will be referred to when discussing Crew Failure Modes and Performance Influencing Factors in this industry. Moreover, a scenario based on the Chevron Richmond accident will be analyzed using HERO in Chapter 5.

CHAPTER 4 – HUMAN ERROR IN REFINERY OPERATIONS - THE HERO HRA METHODOLOGY

As mentioned in Chapter 1, oil refineries and petrochemical plants present a great potential for small and big accidents – working with flammable and toxic substances may cause injuries, production delays and financial loss. The previous chapters explained and presented several examples and evidence of such. Chapter 1, for instance, provided statistics on accidents; and Chapter 3, in turn, described four big accidents. The examination of those accidents showed that human failure not only was present, but also played a major role. Chapter 2, in turn, explained HRA as a form of assessing the human contribution to accidents and also introduced the Phoenix methodology and its elements.

But, as was also explained in Chapter 2, despite the impact of human actions in oil refineries and petrochemical plants accidents, HRA can be considered a relatively new concept within the petroleum industry. Most commonly used HRA methodologies have largely been developed to support nuclear power control room operations within the context of probabilistic safety assessments. They thus fail in providing the same support for different contexts and their own specificities and particularities. Existing HRA methodologies, in short, have great benefits in analyzing the relevance of human failure, but they fall short in doing so within the context of petroleum refining industry.

Given the impact that applying HRA methodologies can have in the oil sector, this research aims at filling the gap between the analysis of safety of oil processing operations and Human Reliability Analysis. As stated in Chapter 1, I aim to do so by developing a methodology that is tailored for the petroleum refinery context and petrochemical plants. Such framework, which is based on Phoenix Methodology presented in Chapter 2, will be explained in the following sections. It is important to consider that, as shown in Chapter 2, Phoenix is a model-based human reliability analysis methodology that overcomes deficiencies of first- and second-generation methodologies. We consider it to be a robust methodology, which is the reason why the methodology to be presented was developed building on some of the Phoenix's features.

The HERO HRA Methodology to be described in this chapter maintains Phoenix's three-layers structure: the first layer is the Crew Response Tree, the middle layer is the FT

modeling the human response based on IDA, while the final layer is the PIFs connected to the CFMs through BBNs. We consider this structure a strong feature of the Phoenix as it gathers all information necessary about the crew's interactions with the plant, the crew's failure modes, and the influences of the surrounding on it, and provides traceability. Other features, however, will be modified; these refer to elements that reflect the oil refinery context, for instance: the Crew Response Tree construction flowchart, the CFMs, the Fault Trees, the PIFs and the CFM-PIF master BBN model.

The development of the HERO HRA Methodology was based, especially, but not limited to, on studies of past accidents in oil refineries, which were detailed in Chapter 3. It also draws on visitations to the integrated control room of an oil refinery in Brazil, and experts' opinions and feedback obtained through a questionnaire. Even though these sources of information are restricted to refineries, the findings obtained concern both refineries and petrochemical plants as their processing and operation are significantly similar[15]. These sources of information are detailed below:

i) Past accident analysis:

Analyzing accidents that happened in refineries in recent years was not without difficulties. Access to reports with details concerning the operators' actions during accident was the main challenge. Most reports, after all, detail technical failures, such as corrosion mechanisms; the same does not happen for human failure. Brazil, for example, not only does not have reports with the necessary details needed for this research, but there is actually no public database about accidents in refineries. For this reason, the past accident analysis focuses on accidents that happened in the United States. This mitigated the problem as the Chemical Safety Board (CSB) elaborates public investigation on large accidents.

ii) Visitations and informal meetings:

We contacted several engineers and operators, and, as part of Quantitative Risk Analysis project of a Brazilian refinery, it was possible to visit the refinery control room. I was also able to have informal meetings with engineers and operators. These were open and welcomed questions and discussions, which made this step of the study less challenging than the past accident analysis. This was essential for this research as their input and feedback made it possible to gather information

[15] In order to avoid unnecessary repetition, I will hereafter refer to oil refineries; readers, however, should keep in mind that all the discussion and all conclusions of this chapter also extend to petrochemical plants.

about the operators' routine, the control room layout and panel screen and the contextual factors that influence operators' actions.

iii) Experts' opinions:

I obtained experts' opinions through a questionnaire sent online. In fact, we encountered some difficulties in finding specialists on the issue. This challenge was, however, expected since HRA applied to oil refinery operations have not been widely explored until the present moment. We contacted 23 experts from different countries, such as Sweden, Norway, the United States, Brazil, and Italy. Some of them, despite being experts on HRA, declared themselves as having not sufficient expertise with regard to HRA applied to oil refineries and petrochemicals. Hence, we gathered the opinions and feedback of eight of them. The number of specialists did not compromise this research as they are highly trained and extremely experimented in the issue, having between five and forty years of experience. The questionnaire, which can be seen in Appendix A, comprises questions about specialists' field of expertise and years of experience, and an open question about CFMs, namely: "In your knowledge of petrochemical/refinery control room operations, which Crew Failure Modes would be more likely to happen?", and one about PIFs "What are the factors that could affect such operator errors (in your response please specify factors under major categories such as cognitive factors, environmental factors, organizational factors, human-system interface factors, etc.)". The answers of these open questions are of high value as they were gathered before specialists could have an opinion about the Phoenix set. Following this, specialists could judge the applicability of Phoenix CFMs in refinery control rooms regarding frequency, marking them as "extremely rare", "remote", "probable", "frequent"; and PIFs regarding relevance in influencing an operator working on a refinery control room "non relevant", "moderately relevant" and, finally, "highly relevant".

As stated in Chapter 1, this thesis focuses on the qualitative aspect of HERO HRA Methodology. The quantitative framework should remain similar to the Phoenix methodology, which was presented in Chapter 2, Section 2.3.4. This chapter will proceed as follows. First, I will introduce and elaborate on HERO HRA Methodology. I will begin by presenting the general structure followed by the elements of the methodology, namely the CRT, the CFMs, the fault trees, PIFs and the CFM-PIF BBN model. These subsections will

not only present HERO methodology elements, but also explain what was modified in the Phoenix and how the features of HERO fit situations that particularly happen in oil refineries and petrochemical plants. I will then provide the step-by-step on how to apply the methodology using the elements presented in the previous section. This chapter, in short, is the core of this thesis as it presents its main contribution.

4.1 The HERO HRA Methodology elements

The interaction with specialists through questionnaires, the control room visitations and past accident analysis allowed to observe important patterns and situations that occur in oil refineries and petrochemical plants. This section explains the HERO HRA Methodology focusing on its three layers. Hence, each of the next sub-sections presents the elements of these layers and discusses its applicability on oil refinery operation. Some information that has been mentioned in previous chapters will be referred to and discussed once again as they are crucial to understand the changes made in the Phoenix. As stated previously, the three layers structure of Phoenix are maintained in HERO HRA Methodology. Figure 22 presents these three layers and the connections among them.

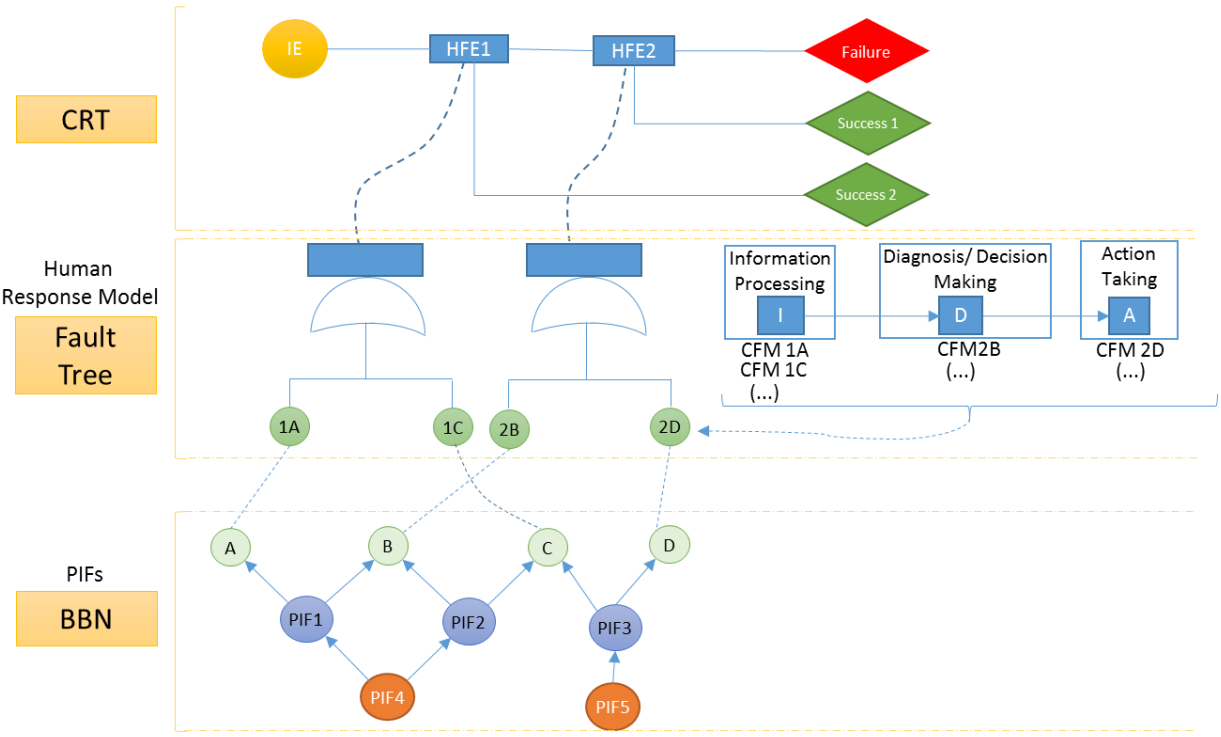


Figure 22: HERO HRA Methodology structure based on Phoenix (Ekanem, 2013)

The first layer is the Crew Response Tree, which is a forward branching tree that provides a systematic coverage of the crew-plant interaction (EKANEN, 2013). The middle layer is the Human Response Model, modeled through Fault Trees, in which the Crew Failure Modes are identified. The cognitive model used for the Human Response Model in HERO HRA Methodology is the Information, Decision and Action Model (IDA), as in Phoenix. The bottom layer consists of the Performance Influencing Factors (PIFs) and its connection with the CFMs, trough Bayesian Belief Networks (BBNs).

Figure 23 presents the building blocks of HERO HRA Methodology. The next sub-sections present and discuss the elements of HERO.

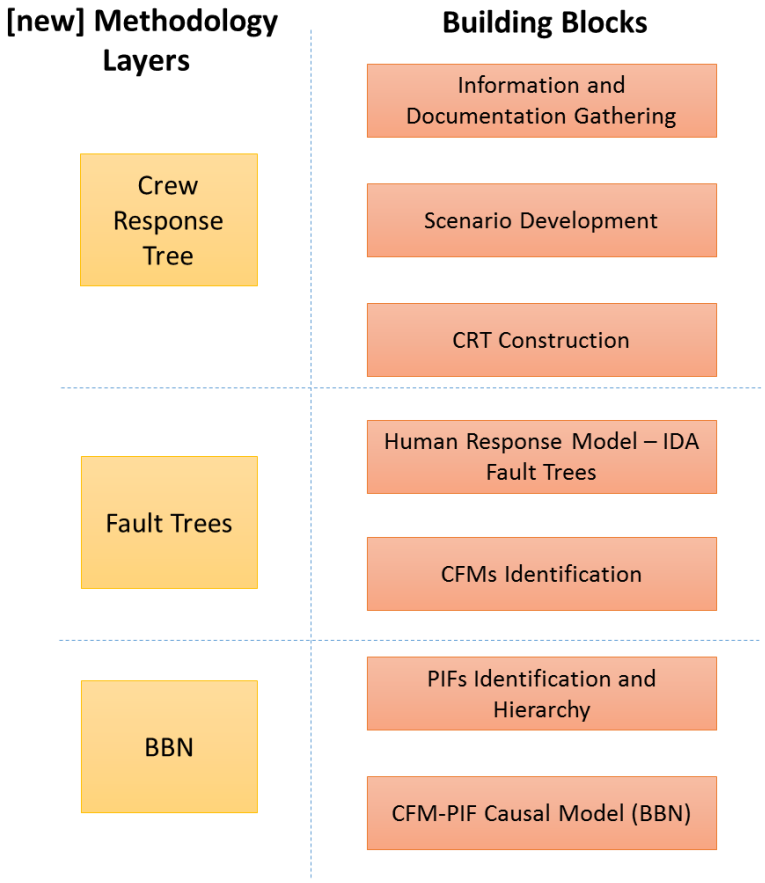


Figure 23: Building Blocks of the HERO HRA Methodology layers (EKANEM, 2013)

4.1.1 Crew Response Tree

The CRT is a crew-centric visual representation of the crew-plant scenarios, also being a roadmap and blueprint that support performing and documenting the qualitative analysis.

Interestingly, CRTs can help both in finding paths to predefined HFEs and possible recoveries and in identifying new HFEs; generally, they model HFEs that refer to a safety function. The process can cover both Errors of Omission and Errors of Commission, thus facilitating the systematic identification of conditions that could allow or lead the crew to follow inadequate paths (Ekanem *et al*, 2016). Yet, CRTs can be constructed for crew response situations that are procedure driven (PD), knowledge driven (KD), or a hybrid of both (HD) (MOSLEH *et al*, 2012).

The safety function is here defined as the main task the crew has to perform to maintain the process on a safe status or bring it back to the safe status when facing an abnormal situation. To identify the safety function, analysts have to evaluate the relevant process variables for the safety of a particular process / task - temperature, pressure, level, flow, and relevant plant conditions, such as pipeline integrity or noises. The safety function will then serve to maintain these variables within the designed range or bring them back to such range.

The CRT is then a tool used for task decomposition of the particular safety function of interest.

Analysts may benefit from some questions to identify the important process variables and the safety function; namely “What abnormal situation can happen at this process / operators’ task?”, “which process variables are relevant to this abnormal situation?”, “what should the operators do when they face this situation to bring the plant to safety?”. For example, in case the scenario analyzed is the operation of the refinery pipelines, analysts might act in accordance to the following guidelines:

- What abnormal situation can happen in this process / operators’ task?

The pipelines may suffer corrosion and leak flammable material;

- Which process variables/plant conditions are relevant to this abnormal situation?

Pipeline integrity, mass flow;

- What should the operators do when they face this situation to bring the plant to safety?

The operators should identify the leak and isolate the pipeline, by closing the valves and stopping the pumps.

The safety function in this case would then be to isolate the pipeline - which is the crew's action to bring the process bring to safety.

Clearly, in order to identify the safety function and construct the CRT the analyst must be familiarized with the scenario, with aid of documentation about the process and the crew and all procedures used to carry out the safety function. A guidance list of needed information and documentation for the analyst is described in Section 4.2.

CRTs, in short, are developed for the different safety functions that exist along the path to the HFE. Note that the HFE is defined in terms of the crew failing to meet the needs of the plant. The use of a flowchart may enhance the consistency when constructing the CRT as questions in the flowchart serve as a guide when it comes to the addition of branches to the CRT. The flowchart, thus, also helps in ensuring the completeness of the CRT (MOSLEH *et al*, 2012). Indeed, the flowchart leads to a skeleton CRT of the main branches that refer to the plant functions. Procedural steps are also part of the flowchart as branch points. The timing of the crew's response may also be included when applicable (in cases in which it has a significant impact on the operator's next actions, for instance). The branch points (BP) of the CRT can include (MOSLEH *et al*, 2012):

1. Operator action options;
2. Operator decision options;
3. Crew member interactions;
4. Relevant plant/system functional states that play a role in defining the context of the operator response.

Phoenix provides a flowchart for the construction of the CRT. This flowchart, however, was developed focusing on Nuclear Power Plant operation. In order to reflect the important variables of oil refinery processing and interactions of refinery operators with the plant, a novel flowchart was developed for use in HERO HRA Methodology. The questions and Branch Points of this flowchart are a result of the past accident analysis, observation of the control room operations and conversation with operators and engineers, and specialists' opinions. Figure 24 presents the CRT construction flowchart. The flowchart questions can be seen in Table 4 and description of success and failure paths for each Branch Point in Table 5.

When following the flowchart, the analyst starts with the first question: "Is the specific function designed to be initiated automatically?" If the answer is yes, the analyst would follow the "yes-arrow" to "Branch Point A (BP A)". At this point, one branch point in the

CRT should be created. The Branch Point A success path is “The safety function is automatically initiated”, and the failure path is “The safety function is not automatically initiated”. If Question 1’s answer is no, the analyst will follow the “no-arrow” that will lead to question number 2. Question number 2 will also be reached if the first question’s answer is “yes”, following BP A failure path. Applying this logic through all the flowchart with the aid of the questions and branch point descriptions, the CRT will be fully created. Next sub-section presents the HERO HRA Methodology CFMs set and discussion.

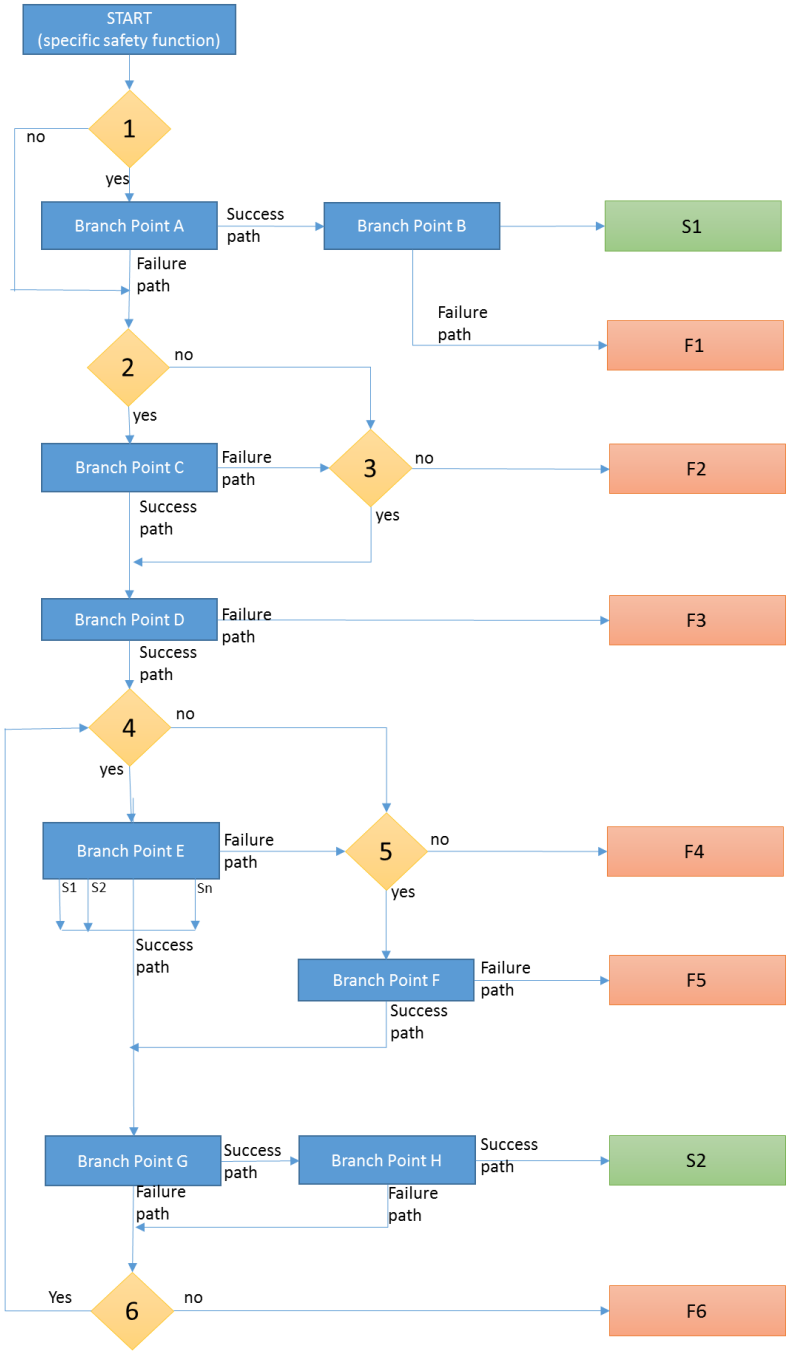


Figure 24: CRT Construction Flowchart

Table 4: Flowchart Questions

No.	Question	Description
1	Is the specific function designed to be initiated automatically?	The control system of the plant may automatically activate the safety function. Ex: Opening a safety valve when the pressure inside a vessel rises above the setpoint.
2	Are there available instruments to indicate relevant process conditions to the operators?	If the alarms/indicators that are relevant to the scenario exist and are available to the operators, the answer is “yes”.
3	Are there other other cues the operators can use to assess the situation?	If there are other cues than alarms/indicators the operators can use to correctly assess the system, the answer is “yes”.
4	Are there procedures instructing the manual activation of the safety function?	If the safety function is not designed to be automatically initiated or the control system and/or instruments/equipments involved at the automatic activation fail, are there instructions to manually activate it?
5	Are there other resources the operators could use to manually activate the safety function?	If there are no procedures instructing to manually activate the safety function, or the operators are not following right procedure, are there other resources operatores can use to assess the situation and activate the safety function? The operators may, for example, rely on their knowledge rather than procedures, or experience with similar situations.
6	Are there additional equipment and manual actions that could be used to provide the specific safety function?	If there are other ways to achieve the same result as the safety function, the answer to this question will be “yes”. If there are no opportunities for such recovery, the answer will be “no”.

Table 5: Description of Branch Points Success and Failure Paths

BP	Success Path	Failure Path
A	The safety function is automatically initiated	The safety function is not automatically initiated
B	Operator does not manually turn off the automatically initiated safety function.	Operator manually turns off the automatically initiated safety function.
C	Relevant instruments work.	Failure of relevant instruments.
D	Operators respond to alarms/indicators or other cues to correctly assess the situation.	Operators do not respond to alarms/indicators or other cues to correctly assess the situation.
E	This branch point considers whether the crew correctly assessed the situation, is in the correct procedure and chooses the right path to manually initiate the safety function. It may	The operator is not in the correct procedure, or the operator is in the correct procedure but chooses the wrong option for the condition, resulting in failure to manually initiate the

	produce multiple branches, each providing a successful path to the critical step to manually initiate the safety function, given the condition. The Success Path corresponds to operator choosing a correct option for the condition and manually initiating the safety function.	safety function.
F	The crew successfully uses other cues to assess the situation and manually activate the safety function.	The crew fails to use other cues to assess the situation and to manually activate the safety function.
G	Safety function is not impaired by equipment (hardware / system) failure.	Safety function is impaired by equipment (hardware / system) failure.
H	Operators successfully initiate the safety function manually.	Operators fail to initiate the safety function manually.

Note that an action of an operator may cause a new disturbance of the process, and provide a new safety function. This is specially the case where there is an abnormal situation in the plant and the crew's response escalates the situation. In this case, one final outcome of the CRT may lead to an another CRT, with the new safety function. For this new CRT the flowchart must be followed once again.

4.1.2 CFMs

The Crew Failure Modes are the generic functional modes of failure of the crew in their interaction with the plant. Phoenix defines the CFMs in each of the I-D-A phases, i.e. they represent the manner in which failures occur in each Information, Decision and Action phase.

The IDA phases, briefly detailed in Chapter 2, are as follows (CHANG; MOSLEH, 2007a):

I - Information pre-processing: This phase refers to the highly automatic process of processing incoming information. It includes information filtering, comprehension and retrieval.

D - Diagnosis/ Decision making: In this phase the crew uses the perceived information and the cues from the previous stage, along with stored memories, knowledge and experience to understand and develop a mental model of the situation. In addition, the crew engages in decision making strategies to plan the appropriate course of action.

A - Action: In this final phase the crew executes the decision made through the D process.

The errors in the “I” phase assume that the crew has failed in detecting, noticing and understanding the plant function(s) they are supposed to be handling. In such phase, the crew can actively collect information or passively receive it. The CFM “Key Alarm Not Responded To” corresponds to passive collection of information, while the other CFMs occur during active information gathering (EKANEM, 2013). Once the crew has the correct information about the plant, they can have correct or incorrect situation assessment, problem solving and decision making.

Errors in the “D” phase, in turn, assume that the crew failed to make a correct assessment of the plant conditions, diagnose, decide and plan the adequate response needed to solve the problem at hand. It is assumed that the CFMs in this phase occur as a result of the crew’s intent (i.e. they are intentional errors). The errors within the “A” phase, finally, assume that there is failure in action execution “A” given correct situation assessment, problem solving and decision making “D” and correct information gathering. It is assumed that the CFMs in this phase are unintentional errors.

According to Ekanem *et al* (2016), the set of CFMs in Phoenix was developed based on aggregated information from nuclear industry operating experience, relevant literature on crew error modes in nuclear power plants, discussions with plant operators and experts, error modes defined in the US Nuclear Regulatory Commission's (NRC) Scenario Authoring, Characterization, and Debriefing Application (SACADA) database project. Phoenix’ CFMs were, then, developed using mainly Nuclear Power Plant operation as base. It is important to note that even though Phoenix’ CFM set was developed to be able to cover a broad range of failure modes, it may not explicitly approach an important crew failure mode for refineries’ operations, or its description may not be clear enough for the analyst to identify it as a refinery CFM. The set of CFMs in the HERO HRA Methodology aims at being easily relatable to oil refinery operations, making it easy and simple for the analyst to identify operators’ actions as CFMs during crew operations in a given situation.

Although most of the original Phoenix CFMs were maintained, the HERO HRA Methodology set contains the new CFM “Procedure not followed”. The addition of this CFM is supported by past accidents analysis and specialist opinions, as discussed as sub-section 4.2.2.1. On the other hand, Phoenix CFM “Decision to Stop Gathering Data” is not explicitly

present in the HERO HRA Methodology CFM set, and has now been included in the description of the CFM “Data not Obtained”. Throughout the analysis of past accidents and meetings with operators and engineers, it seemed to not be a major CFM for refinery operations. Furthermore, most of the specialists marked it as either “extremely rare” or “remote”.

In addition to the changes described above - the inclusion of “Procedure not Followed” and the merging of “Decision to Stop Gathering Data” and “Data not Obtained” - Phoenix CFMs suffered major changes in their description in order to make them relatable to analysts in the oil domain.

It is interesting to note that “Plant/System State Misdiagnosed” was considered one of the major CFMs for refinery operations by the specialists. In the open question on which Crew Failure Modes would be more likely to happen in refinery control room operations, specialists’ answers relate to this CFM through “Failure to understand/decide which scenario they are in” and “Misdiagnosis of plant state”. Moreover, in the questionnaire’s CFM table, most specialists marked such CFM as “probable” or “frequent”. Since refinery operations may involve a large amount of equipment and depend on many processes variables, dealing with an abnormal situation at the plant correctly diagnosing the key root causes is not always that obvious. This CFM is identifiable in the BP Texas City Refinery Accident (2005), when the tower’s pressure rose to 228 kPa due to the significant increase in the liquid level compressing the remaining nitrogen in the raffinate system and crew believed the high pressure to be a result of the tower bottoms overheating (Event 3 at Figure 20, Chapter 3). It also played a major role in the Chevron Richmond Refinery Accident, when the crew misdiagnosed the status of the pipeline, concluding that the leak was not significant enough to require a shutdown (Event 1 at Figure 21, Chapter 3).

Table 6 presents the full set of the HERO HRA Methodology CFMs followed by a discussion on the inclusion of CFM Procedure Not Followed. Sub-section 4.2.2.2 presents the CFMs descriptions and their applicability on oil refinery and petrochemical plants operation. The CFMs are defined based on the particular IDA phase in which they occur.

Table 6: HERO HRA Methodology CFMs Full Set

ID	Crew Failure Modes in "I" Phase	ID	Crew Failure Modes in "D" Phase	ID	Crew Failure Modes in "A" Phase
I1	Key Alarm / Information not Responded to (intentional & unintentional)	**D1**	Plant/System State Misdiagnosed	**A1**	Incorrect Timing of Action
I2	Data Not Obtained (Intentional)	**D2**	Procedure Misinterpreted	**A2**	Incorrect Operation on Component/Object
I3	Data Discounted	**D3**	Failure to Adapt Procedures to the situation	**A3**	Action on Wrong Component / Object
I4	Data Incorrectly Processed	**D4**	Procedure Step Omitted (Intentional)		
I5	Reading Error	**D5**	Procedure not followed		
I6	Information Miscommunicated	**D6**	Inappropriate Procedure Followed		
I7	Wrong Data Source Attended to	**D7**	Decision to Delay Action		
I8	Data Not Checked with Appropriate Frequency	**D8**	Inappropriate Strategy Chosen		

4.2.2.1 Inclusion of CFM Procedure Not Followed

Procedure not Followed is a CFM observed in refineries past accident analysis and which is not explicitly covered in the Phoenix set. The introduction of this new CFM is supported by several evidence. Interestingly, not following procedures in both the Tosco Avon and the Texas City cases was crucial for the accidents to happen. In the Tosco Avon Refinery accident (1998), the procedures stated that when a reactor temperature rose 50^{o}F above normal or if any reactor temperature exceeded 800^{o}F, the operators should immediately activate the 300 psi/minute depressuring system. The operators, however, did not follow the procedure. Instead, they tried to control the temperature rise by controlling the quench (EPA, 1998).

As mentioned, failure in following procedures was also an essential element in the BP Texas City Refinery accident (2005). Although the startup procedure had called for the level in the tower to be established at a 50% transmitter reading, the operators did not follow the guidelines and filled the tower until 99% of the transmitter reading (Event 1 at Figure 6, Chapter 3). Also, when the operators were resuming startup, they did it with the control valve closed when the procedures indicated that this valve should be open to control the level in the tower (Event 2 at Figure 6, Chapter 3). When it comes to the Tesoro Anacortes Refinery Accident (2010), following procedures would not avoid the accident, but could have reduced

human losses, since procedures called for less operators to be present during the startup of the heat exchangers (CSB, 2014b).

The introduction of “Not Following Procedure” as a CFM is also supported by Saurin and Gonzalez (2013) as an important one for refineries. Through the analysis of the control room operations of the logistic area (pipelines) of a refinery, they concluded that there was evidence that actual work often differed from prescribed work. Finally, specialists’ opinions also support this finding: on the questionnaire’s open question “In your knowledge of petrochemical/refinery control room operations, which Crew Failure Modes would be more likely to happen?”, three specialists answered “Failure to follow procedure” while another answered “procedural problem”.

CFM “Not Following Procedure” sums with original Phoenix CFMs related to procedures, which were maintained. CFMs such as “Procedure Misinterpreted”, “Failure to Adapt Procedures to the Situation” and Procedure Step Omitted (Intentional)” were considered important to refinery operations; most specialists marked them as “probable” or “frequent” on the questionnaire. “Inappropriate Transfer to a Different Procedure” was renamed “Inappropriate Procedure Followed”.

4.2.2.2 CFMs Description

I1 - Key Alarm/Information not Responded to (intentional & unintentional)

This CFM is applicable to the case where a key process alarm goes off and the crew fails to respond to it, intentionally or unintentionally. It also covers the case where the operators face a key information about the status of the plant and fail to respond to it.

Refinery operations control system is in most cases highly automatized - the important process variables are constantly monitored, and alarms indicate when the values are above or below the expected in the process (setpoints). For example, a rise in temperature above the setpoint is normally indicated by a High Temperature Alarm, and a level lower than it should be is indicated by a Low Level Alarm. In many refinery processes, there are also redundant alarms.

A key alarm is an alarm that is crucial for the operation being performed. The key alarm should be the most important cue for the identification of abnormal situations, the crew`s response should put them in the path of a successful outcome. The filling of a tower, for example, has the level alarm as a key alarm. If the tower high level alarm goes off and the

crew does not notice the alarm, because they are distracted, or notices it but does not respond to it, because they are busy with another activity, this CFM would apply.

A key information on the status of the plant is also an information crucial for the operation. A key information not responded to covers, for example, a situation where there is a visible leak on a pipe and the field operator fails to visualize it or to respond to it. Another key information may be an abnormal noise of an equipment.

I2 - Data not Obtained (Intentional)

This CFM indicates a situation where the crew understands the need for a certain data but intentionally fails to collect it. The crew may believe the data is incorrect, misleading or unsuitable for the intended purpose. It may also be because they already have similar data which they believe should suffice. For instance, the crew may understand they need a certain temperature, but not trust the temperature indicator and decide not to collect it.

I3 - Data Discounted

It applies to a situation where the crew gathers the data they need but decide to discard it afterwards, not using it to assess the plant state. In other words, they obtain an information but decide not to use it because they assume it is not relevant to the situation they are facing. The crew may, for example, gather information on the state of a valve (open/closed) to assess an abnormal situation of the pressure rise in a tower being filled up but believe the pressure rise is not due to this valve being closed, but due to remaining gases inside the tower, and thus discard the information about the valve status.

I4 - Data Incorrectly Processed

This defines situations in which the crew may possess the correct data to assess the plant status, but misinterpret it or do not interpret it in time. For example, the crew may collect information about temperature in reactor A, but believe it was from reactor B.

I5 - Reading Error

This is the case where the crew makes a simple reading error. It may be an error reading the procedures or a parameter value indicated on the control panel, for example. The operator may, for instance, read the status of a valve as “open” instead of “closed”, or mistake number on a temperature indicator.

I6 - Information Miscommunicated

This CFM indicates a miscommunication of necessary information. This miscommunication may be because the information is not complete or is incorrect, or the information is sent to the wrong person, or at the wrong time. The miscommunication may be, for example, between panel operators working in the same unit, panel operators from different units, panel operator and field operator, or between an operator and a supervisor. This CFM is especially important during shift changes: the operator leaving the shift may not write at the log the information needed for the next operator taking the shift, or do so only orally in a poorly manner, lacking details.

I7 - Wrong Data Source Attended to

This CFM applies to a case where the crew is aware of the information needed but collect it from the wrong source. For example, they may need the temperature from an equipment that is indicated by indicator TI-33005 and collect it from TI-3301 instead, which would be from a different equipment.

I8 - Data Not Checked with Appropriate Frequency

This CFM applies to a situation where the crew should be monitoring some data but fails to do so. For example, the crew may be filling a tower to a determined level and fail to check the level through the indicator with the appropriate frequency, failing to initiate a response in a timely manner.

D1 - Plant/System State Misdiagnosed

Since assessing a refinery process involves dealing with a lot of variables and possibilities, the crew may have all correct and needed information at hand but fail to correctly diagnose the plant state – which describes this CFM. They may, for example, be dealing with a leak on a pipeline and believe the pipeline integrity is better than it really is and that it can be fixed without stopping the process or being isolated.

D2 - Procedure Misinterpreted

This CFM applies to a situation where the crew is following procedures but do not understand it correctly. For example, the crew may fail to interpret the steps to be followed to manually trip a reactor.

D3 - Failure to Adapt Procedures to the Situation

This is applicable to a situation where the crew is following a procedure but fails to adapt it to the situation at hand.

D4 - Procedure Step Omitted

This CFM applies to a situation where the crew is following procedures but intentionally omit one or more of its steps. The crew may decide to postpone the step, planning to complete it later, or believe that a particular step is not relevant or is even incorrect and does not need to be taken. For example, the crew may be starting a unit and following the startup procedures. But they may believe one of the steps is not relevant to successfully start the unit, and decide not to do it.

D5 - Procedure not Followed

This describes a situation where the crew decides to rely on their own knowledge instead of following a procedure. Differently from CFM D4 "Procedure Step Omitted", the crew here is not following any procedure for the operation they are performing. This can be because they believe the procedure is incorrect or is not updated, or because they believe their knowledge and experience is enough to perform the operation. The crew may, for example, start a unit filling a tower above the level indicated at the procedures, because they believe starting the unit with the level indicated in procedures would harm other equipment following the tower.

D6 - Inappropriate Procedure Followed

This is the case where the crew is following a procedure but not the correct one. It also covers the case where the crew follows certain procedure but decides to transfer to another one when they are not supposed to (inappropriate transfer to a different procedure).

D7 - Decision to Delay Action

This CFM applies to the case where the crew assesses the situation correctly, but decide to postpone an action, to the extent that the response is unsuccessful even when it is finally completed. This can be because they are waiting for more information on the plant. The crew may, for example, decide to shut down a unit due to a leak, but postpone the decision waiting for information about a unit that depends on the one they're working at. When they finally shut down the unit the leak is already big enough to cause a fire or explosion.

D8 - Inappropriate Strategy Chosen

The crew may have a correct assessment of the plant condition, but takes a different course of action than the expected one (the one suggested in procedures or in training). For this CFM, the expected course of action is considered to be the success path while the alternate action may result in success or failure. For example, the crew may decide to correct a leak in a pipeline by using an aggressive strategy when the pipeline's wall is already too thin, aggravating the pipeline integrity.

A1 - Incorrect Timing of Action

This is the case where the crew has correct and complete information in hand and makes the right decision, but completes the action either too early or too late. This CFM is considered unintentional. For example, the crew may be in the process of opening a safety valve to relief pressure of a tower, but gest distracted by another member of the crew or by alarms or other information on the control panel and forget to open the valve in time.

A2 - Incorrect Operation of Component/Object

This CFM applies to a situation where the crew makes the right decision and is in the process of performing an action on the right component but performs it incorrectly. It also includes performing actions out of sequence. For example, the crew may be wanting to close a valve but opens it more instead.

A3 - Action on Wrong Component / Object

This CFM applies when the crew performs the right action on the wrong component. For example, the crew makes the decision to shut down reactor R-35001A but, instead, shutdowns reactor R-35001B.

4.1.3 Fault tree

Even though the CRT branches reflect some of the contextual factors and causes of crew error, they do not cover the human failure mechanisms or their causes (EKANEM, 2013). The Human Response Model is the second layer of the HERO HRA Methodology, modeled through Fault Trees. The fault trees are based on salient information from cognitive psychology literature and were first developed in order to bridge the gap between the fields of HRA and psychology/human factors (EKANEM *et al*., 2016). The HERO HRA Methodology presents a set of fault trees to help analysts select the relevant CFMs for each branch point within each scenario. For each CRT branch point there is a set of CFMs that will be

applicable; for example, if the branch point concerns failing to shutdown Reactor B while shutting down Reactor A instead (when the successful path would be to shut down Reactor B), and no alarm is set to indicate it, the CFM "Key Alarm Not Responded to" does not apply.

The Fault Tree identifies the Human Failure Event as a failure in one of the IDA phases: Failure in Collect Necessary Information, Failure in Making the Correct Decision Even if Necessary Information is Collected, Failure in Taking the Correct Action Even is the Correct Decision is Made. In this view, failures in I, D, or A are "minimal cutsets" of the human failure events (MOSLEH *et al*, 2012). Figure 25 represents the logic behind the Fault Tree. Each of the parts the HFE is broken down into detailed FTs.

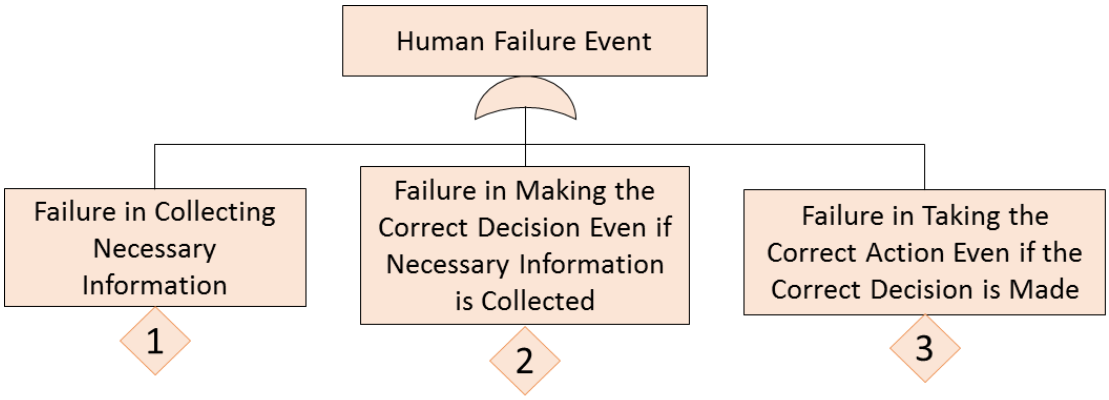


Figure 25: Human Failure Event in Terms of IDA Phase (MOSLEH *et al*, 2012)

The fault trees help the analyst to trace the context related to the CRT branch point assessed until the CFMs, which are the end points of the fault trees (lowest level of the FTs). Given the nested structure of IDA, explained in Section 2.3.2.1, each phase can be decomposed into further I-D-A structures. Thus, the I phase can be sub-divided into the following: I-in-I, which is related with information being perceived and recognized, D-in-I, which involves deciding what to do with the received information (ex. discard it or keep it), and A-in-I, which involves the actions taken after the decision is made. The same follows for D and A phases.

The sub-sections below present the FTs connected to the main FT in Figure 25. To use the FTs in a practical manner, the analyst should begin determining the nature of the branch point being analyzed to identify if the HFE is due to information error and/or decision error and/or action error. The HFE may be dominated by information and decision errors, for

example, and the action error path may be ignored. The FTs contain flags that permit the related fault tree branch to be completely ignored depending on its status. For example, in a branch point, if the primary information is not applicable, then "Primary Information Not Available (Yes=0, No=1)" should be set to 0 and the whole sub-branch of the fault tree may be ignored (OXSTRAND *et al*, 2012).

4.1.3.1 Failure in Collecting Necessary Information

The necessary information consists of primary and secondary information. Primary information is collected from the direct source, e.g., a temperature value read from a temperature indicator. Secondary information, on the other hand, is the information obtained indirectly. For example, the crew may follow the rise of a temperature, but the instruments necessary are unavailable. They may then deduct information about the temperature from the changes in the pressure values.

To fail in collecting necessary information, therefore, the crew had to fail to collect primary and secondary information (AND gate at the FT). Figure 26 presents the FT for Failure in Collecting Necessary Information (Part 1 of the FT in Figure 25). The description below walks through the "Failed to Collect Primary Information" path of the FT. The path "Failed to Collect Secondary Information" follows the same logic. Both paths contain a flag about the availability of information (primary or secondary). If primary information is not available, its status should be set to zero and the sub-branch may be ignored.

The failure in collecting primary information can be due to failure in information source, failure in decision to collect information or failure in the execution to collect information (OR gate in the FT). Note that these indicate the nested I-D-A phases in I phase. The information sources in the refinery operation can be instruments whose value can be read at the control panel or the field, documents such as procedures, and a crew member. Crew members may refer to a member in another physical area (one member in the field and another one in the control room), in the same area (two members in the control room working together in the same unit or in different units), or a member from a different shift.

The instrument path has a flag about its availability, and if the relevant instruments are not available for the operators the sub-branch "Instrumentation Failure" may be ignored. If the instrument is available, then, for it to fail as an information source, there should be instrumentation failure (such as a temperature indicator broken, or indicating the wrong

temperature). The relevant documents may also not be available (flag at the FT). If they are available, they can be outdated or present incorrect information (for example, a procedure that was not updated after a change in a process will lead to incorrect information).

The use of a crew member as a source of information depends on the communication among members. A member can give the incorrect or incomplete information because a relevant instrument is not available or because of instrumentation failure. For example, an operator in the control room may contact an operator in the field to verify a level in a tower, but the sight glass is obstructed (instrumentation not available), or to verify a reactor temperature indicated in the field but the indicator is indicating an incorrect temperature (instrumentation failure). In addition, there can be miscommunication between crew members. An operator finishing a shift can give unclear instructions to the next shift operator, for example. This failure would be the CFM "Information Miscommunicated". The CFM in the FT is indicated by a red circle underneath it.

Figure 27 presents the FT for "Failed in Decision to Collect Information", part 4 of the main FT of Failure in Collecting Necessary Information" of Figure 26. Note that the crew may be following procedures and/or their own knowledge in this phase. The "Following Procedure as Strategy" path has two flags, Incomplete/Incorrect Procedure Guidance and the Flag of Following Operators' Knowledge. When following procedure, the operators may fail to collect active information. The FT at this point leads to the CFMs "Data Not Checked with Appropriate Frequency", "Data not Obtained" and "Data Discounted". If one of these CFMs occurs, it leads to failure to collect active information (OR gate at the FT).

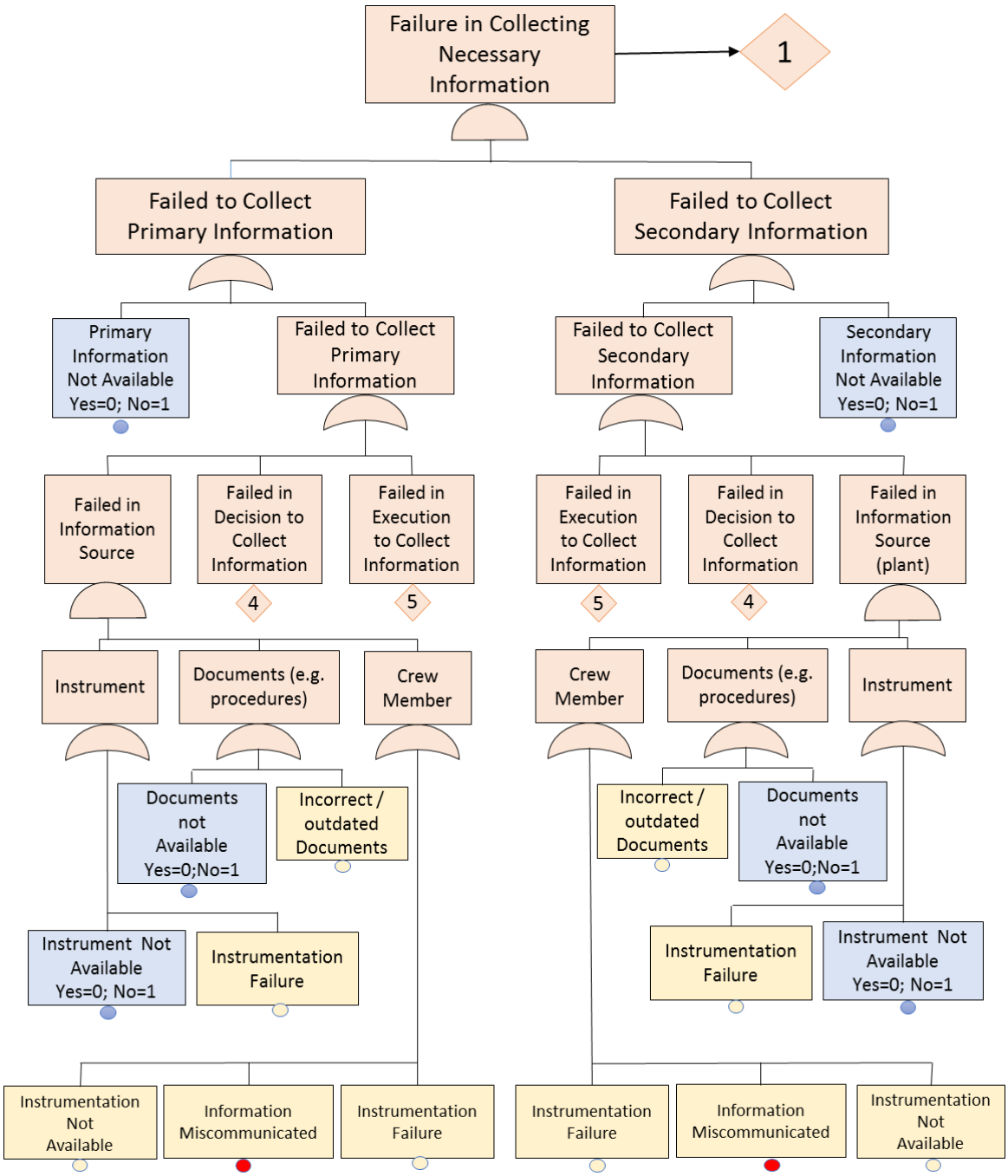


Figure 26: Fault Tree for Failure in Collecting Necessary Information

When the crew is following their knowledge, they can fail to collect passive information when they do not respond to a key alarm (CFM "Key Alarm not Responded to". They can also fail to collect passive information if they collect the data but then decide to discard it - CFM "Data Discounted" or if they do not check the relevant data with the necessary frequency - CFM "Data not Checked with Appropriate Frequency".

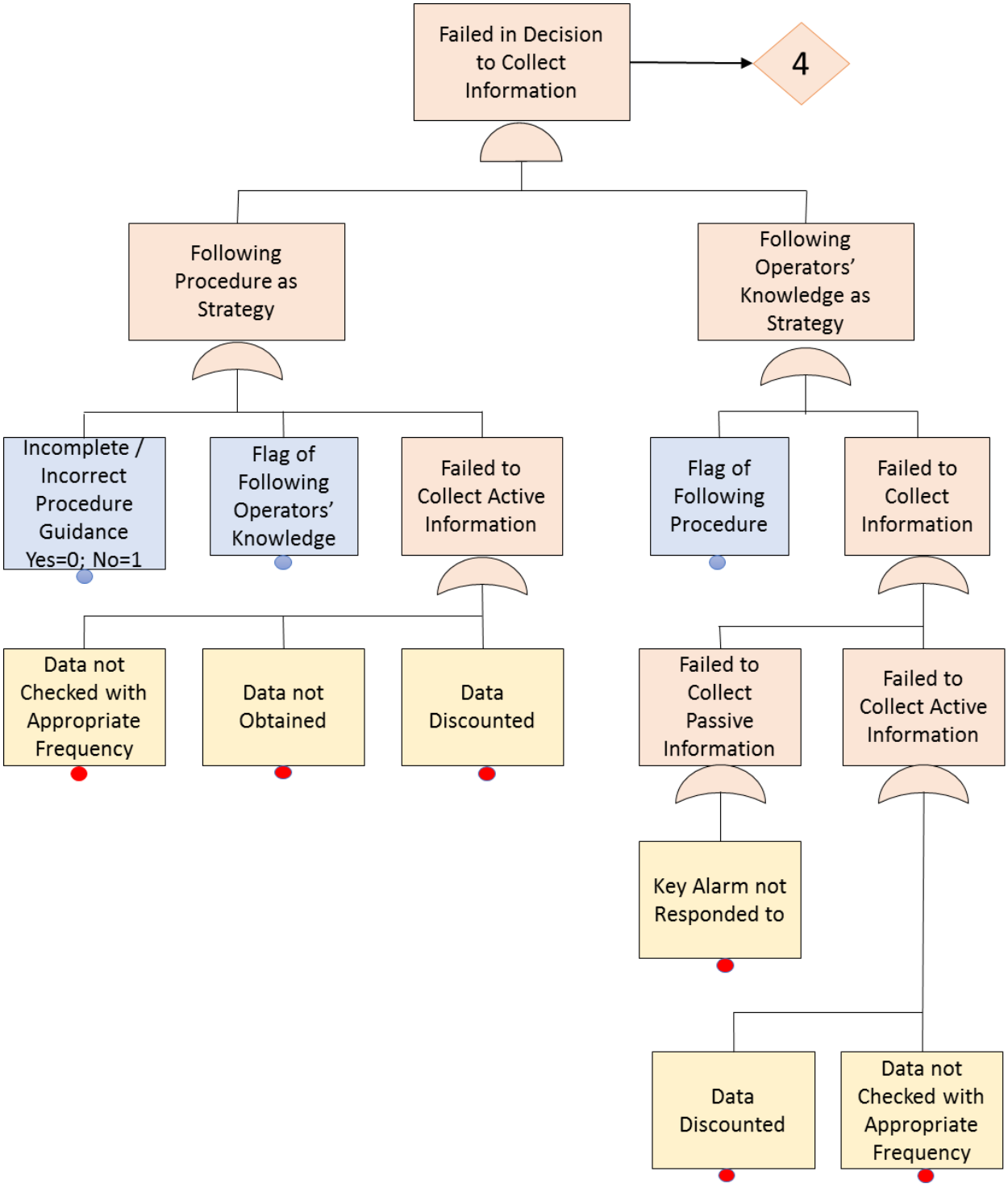


Figure 27: Fault Tree for Failed to Collect Decision branch

Failure in the execution to collect information can be due to failure to collect active information or failure to collect passive information, as shown in Figure 28. The CFMs in this phase are "Data not Checked with Appropriate Frequency", "Wrong Data Source Attended

to", "Reading Error" and "Data Incorrectly Processed" in failure to collect active information and "Key Alarm not Responded to" in failure to collect passive information.

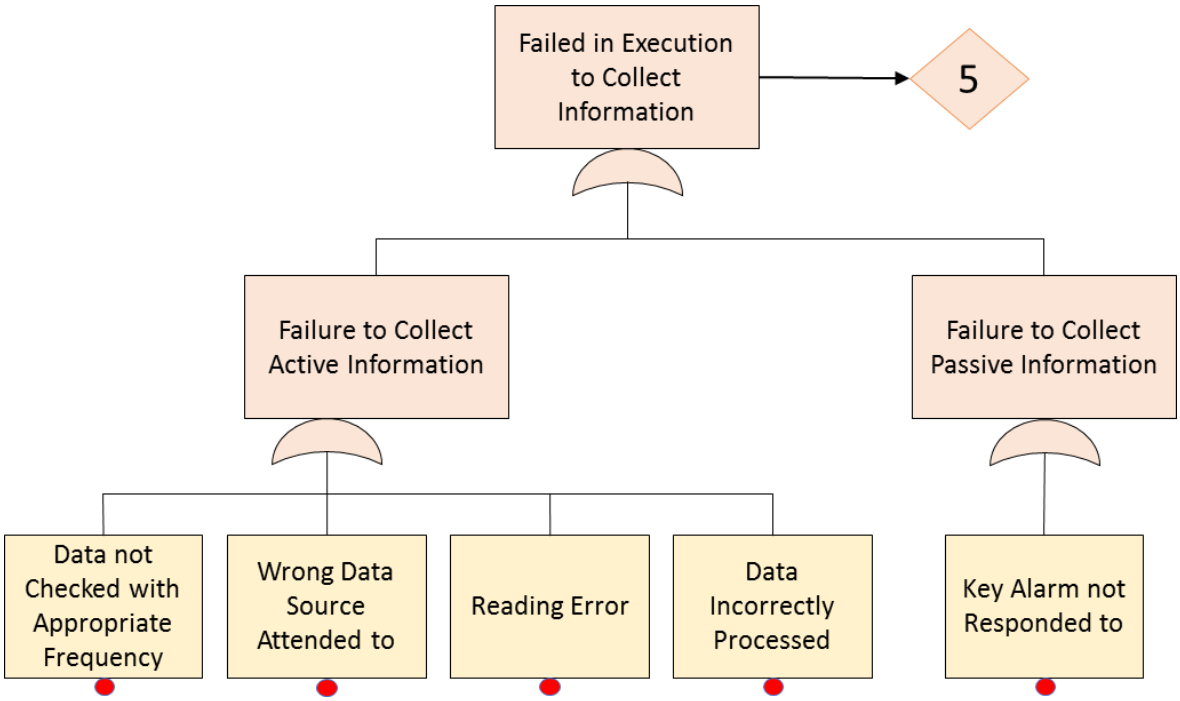


Figure 28: Fault Tree for Failed in Execution to Collect Information branch

It is important to observe that there may be different paths for one CFM. When there is an information to be checked with determined frequency, for example, the crew may decide that the frequency may be lowered without loss in the safety or efficiency of the process, or the crew may decide to check it with appropriate frequency but be interrupted because of another task to be performed. This CFM, thus, happens in the path of "failure in decision to collect information" or "failure in execution to collect information". The same logic may be applied for the remaining CFMs that appear more than once in the FT.

4.1.3.2 Failure in Making the Right Decision

The crew can fail in making the right decision even if necessary information is collected when following procedure and/or relying on their own knowledge (Figure 29). When the strategy is for the crew to follow procedure, the crew may make a wrong decision because they misinterpreted the procedure, omitted a step of the procedure, deviated from it or decided to not follow it at all. The deviation from the procedure may be for three different reasons, as it can be seen in Figure 29. One of them is when the crew transfers to a different procedure

they should not. A second reason for such is when the crew commits an error in assessing the situation, such as misdiagnosing the plant or failing to adapt the procedure to the situation. The third reason that may lead to deviation from the procedure is when the crew makes an error in action decision, such as choosing an inappropriate strategy to deal with the situation or deciding to delay the action.

These same CFMs from action decision when following procedure may happen when following operator's knowledge, causing failure in problem solving and decision making. Failed in problem solving and decision making can also be due to error in situational assessment, which, on its turn, can be due to the CFMs "failure to adapt procedure to the situation" and "Plant/System State Misdiagnosed".

4.1.3.3 Failure in Taking the Correct Action

When the correct decision has been chosen by the crew, they can still fail to take the correct decision. This may happen because the correct action is made on the wrong component, the correct action is made on correct component but in incorrect timing, or the action is incorrect, as seen in Figure 30.

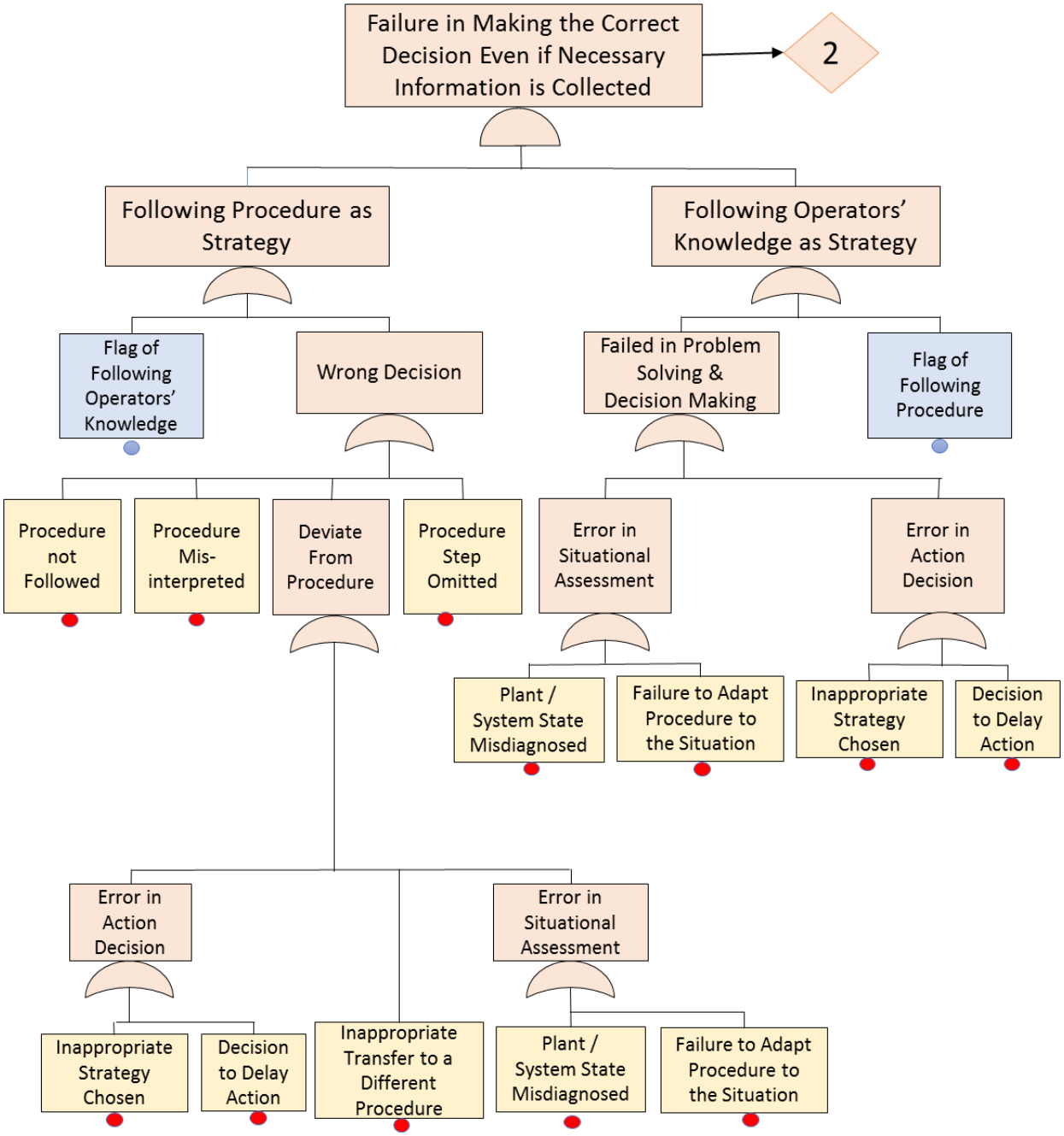


Figure 29: Fault Tree for Failure in Making the Correct Decision Even if Necessary Information is Collected

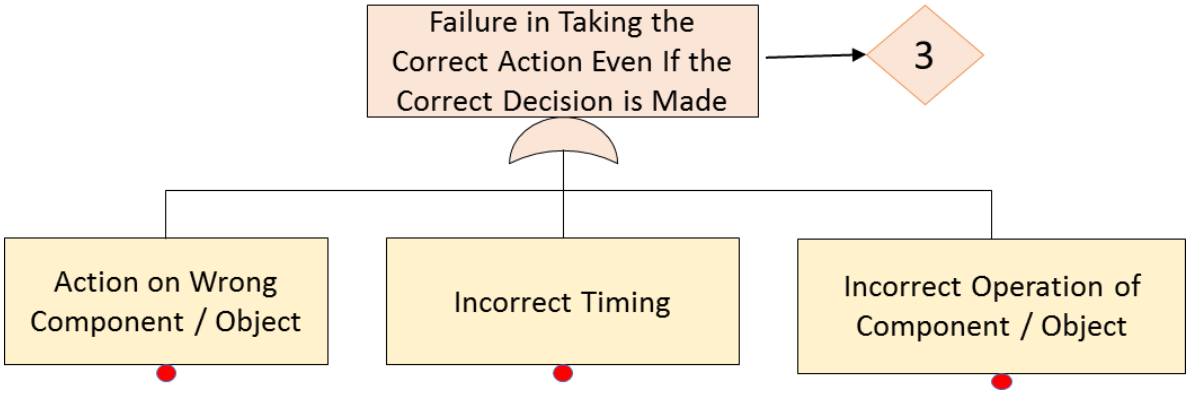


Figure 30: Fault Tree for Failure in Taking the Correct Action Even if the Correct Decision is Made

4.1.4 PIFs

Phoenix' set of PIFs was primarily based on the set proposed by Groth (2009) and Groth and Mosleh (2012) and expanded to meet the necessary requirements indicated in the US NRC's Good Practice for HRA, (KOLACZKOWSKI *et al*., 2005). It also incorporates the error causes defined in the US Nuclear regulatory commission's (NRC's) Scenario Authoring, Characterization, and Debriefing Application (SACADA) database. Phoenix set of PIFs overcomes several deficiencies of PIFs from other HRA methods, as described in Chapter 2, in order to fit model quantification; it is thus not only designed to be assessed by experts (EKANEM, 2013). It was, however, mainly based in Nuclear Power Plant operation contextual factors.

As previously mentioned, the HERO's set of PIFs is based on Phoenix original set, but it is fully adapted for use in refinery operation. The changes comprise inclusion of new PIFs, exclusion of others, and total modification of names and/or descriptions. The result is a set of PIFs that has all the advantages of the phoenix, but is easily relatable for refinery operations.

Two new PIFs were considered to be important in refinery operations and were not present at Phoenix original set: Procedure Updating and Knowledge of Plant Conditions. The importance of these PIFs in refinery operations is discussed in sub-section 4.1.4.1. Time Constraint, a PIF present in Phoenix original set, is now considered a factor in Stress due to Perceived Situation Urgency. Safety Culture also suffered changes, and is not an explicit PIF anymore. We consider Safety Culture to be evaluated through other PIFs, such as Human Machine Interface, Procedure, Resources, among other, which all indicated the safety culture of an organization.

HERO HRA Methodology PIFs set have been organized into nine (8) main groups, which are also individually considered as PIFs - “Primary or level 1 PIFs”. The groups are Knowledge/Abilities and Bias which maps to cognitive response of the crew, Stress maps to emotional response, while Procedures, Resources, Team Effectiveness, Human Machine Interface (HMI) and Task Load all maps to physical world. Also important, the PIFs are classified into levels within the groups, thus forming a hierarchical structure, which can be fully expanded for use in qualitative analysis as well as collapsed for use in quantitative analysis. In this hierarchy, Level 1 PIFs affect directly the CFMs. Level 2 PIFs affect level 1 PIFs, and level 3 PIFs affect Level 2.

HERO`s full set is presented in Table 7 below. The description of the PIFs and their applicability in refinery operation is discussed in sub-section 4.1.4.2.

Table 7: HERO HRA Methodology PIF set

HMI	**Procedures**	**Resources**	**Team Effectiveness**	**Knowledge / Abilities**	**Bias**	**Stress**	**Task Load**
HMI Input	Procedure Content	Tools	Communication	Knowledge / Experience / Skill (content)	Motivation/ Commitment	Stress due to Situation Perception	Cognitive Complexity
HMI Output	Procedure Updating	Tool Availability	Communication Quality	Task Training	Confidence in Instruments	Perceived Situation Urgency	Inherent Cognitive Complexity
	Procedure Availability	Tool Quality	Communication Availability	Knowledge of Plant Conditions	Familiarity with of Recency of Situation	Perceived Situation Severity	Cognitive Complexity due to External Factors
		Workplace Adequacy	Team Coordination	Knowledge / Experience / Skill (access)	Competing or Conflicting Goals	Stress due to Decision	Execution Complexity
			Leadership	Attention			Inherent Execution Complexity
			Team Cohesion	Fitness for Duty			Execution Complexity due to External Factors
			Responsibility Awareness				Extra Work Load

Table 7 – continuation

			Team Composition				Passive Information Load
			Team Training				

Key	Meaning
	Level 1 PIFS
	Level 2 PIFS
	Level 3PIFS

4.1.4.1 PIFs Description and applicability in an oil refinery context

This sub-section presents a discussion on the applicability of the HERO HRA Methodology PIFs in an oil refinery context, and the PIFs description. These findings are the basis for the changes performed in original Phoenix set. The discussion below makes reference to the accidents analysis presented in Chapter 3 and the questionnaire for specialist opinions.

HMI Group

The Human Machine Interface group is comprised of HMI input and HMI output. The former refers to interaction between the operator and the system with respect to the inputs provided by the crew; the latter, in turn, refers to the information obtained by the crew with respect to the plant through the system. In most refinery control rooms HMI are comprised by a control panel that provides information on process variables such as temperature, pressure, flow rate, level, and status of equipment (such as valves and pumps). Most control parameters are highly automatized, but allow the operator to change control from automatic to manual in case of need.

Although the number of physical elements in the control room is small, operators actually interact with a large number of elements in the virtual sphere. Saurin and Gonzalez (2013), who analyzed the control room operations of the logistic area of a Brazilian oil refinery, observed that there were 2260 items of information online about the status of the operations back in 2013. There were available on the computer screens in the control room, and, at any given moment, an operator had access to 11 of the 121 existing screens. From the control room, the operator could remotely control 271 pumps, 412 valves, and 71 switches to

turn equipment on or off. A good HMI is crucial to prevent errors in order for all these variables to be perfectly operated.

Indeed, there is a consensus when it comes to the relevance of HMI. Most specialists actually assume, in the questionnaire, that HMI input and output are moderately or highly relevant for operator behavior in a refinery control room. In addition, two specialists had answers related to HMI for the questionnaire open question "What are the factors that could affect such operator errors? (crew failure modes of operators working in refineries control room)". Interestingly, HMI output was particularly significant during the BP Texas City Refinery accident (2005). During the filling of the tower, the information on the panel was not adequate to check the imbalance between the input and the output from the tower (Event 2 at Figure 6, Chapter 3). The control system screen that provided the reading of how much liquid raffinate was entering the unit was on a different screen from the one showing how much raffinate product was leaving the unit.

During the Tosco Avon Refinery accident (1997) investigation, in turn, HMI output was also found inadequate and an important influencing factor for the accident. Not all temperature data were accessible from the control room, some of the readings could only be obtained at the field panels outside underneath the reactors. This caused Operator 2 to go close to the reactors to check the temperature, being there when the explosion occurred (Event 1 in Figure 2, Chapter 3). Informal discussion with control room operators in the refinery visited for this research, HMI input was pointed as a cause of a recent error. In one of the examples mentioned, an operator was supposed to shut down a boiler B, but, given that the panel interface was not clear enough about which boiler he/se was operating, the operator shut down boiler A instead, which caused a relevant production delay.

Koffskey *et al* (2013) also highlight the importance of HMI on operators' actions in control rooms in petrochemical plants. Using a state-of-the-art interface against a poor interface to assess the impact on performance of control room operators in terms of operator speed and accuracy when addressing simulated events within a crude refining unit, they concluded that operators were significantly faster and more accurate addressing alarms using the good interface compared to the poor interface. The interface that used more efficient methods of presenting information and more agreeable color schemes resulted in better performance (faster speed and higher accuracy in responding to alarms).

Procedures group

The procedures group is comprised of Procedure Availability, Procedure Content and Procedure Updating. One of the specialists highlighted that an important source of error is that "procedures are not updated to reflect changed operation" as an answer to the questionnaire open question "What are the factors that could affect such operator errors?". Indeed, most specialists marked Procedure Quality as having a highly relevant influence to operators' actions in a refinery control room (Procedure Quality is divided here into Content and Updating).

The EPA investigation of the Tosco Avon Refinery accident (EPA, 1998) pointed procedures updating and content as sources of error. The procedures had not been updated as changes were made to operating equipment and the process itself (Procedure Updating). Also, they were not developed for many operations, including obtaining temperature data from outside field panels underneath the reactor, and presenting conflicting differential temperatures limits for catalyst bed operation (Procedure Content).

Procedure updating played a major role in the BP accident (2005). The first human event of the accident (Event 1 at Figure 6, Chapter 3), related to not following procedures, had as an important cause the fact that procedures were not updated. The operators did not follow the startup procedure because they felt that it was common for the tower to lose level during startup, which would damage other equipment. The procedure was not updated to reflect this problem, and this can be considered to be the most influential factor for this event.

During the Tesoro Anarcotes Refinery accident (2012), startup procedures were also not updated to reflect the actual status of the operation: The manipulation of the isolation block valves could not be done by only one person at the field, but the procedures would specify roles for only one operator working at the field. Saurin and Gonzalez (2013) stress that the large number of interdependent procedures used in refinery operations can make it difficult to anticipate the system-wide impacts of individual actions or decisions. The control room operations of the logistic area of Brazilian oil refinery analyzed in the work required the use of 43 procedures, as well as nine manuals containing details about equipment operation and safety standards at work, which apply to all the areas of the refinery.

Still according to Saurin and Gonzalez (2013), having so many interdependent procedures aggravates the adaptation of one of them as a source of operators' error because the adaptation of a procedure may cause difficulty in following other interdependent ones.

Figure 31 shows the relationship between procedures used in control room of the logistics area:

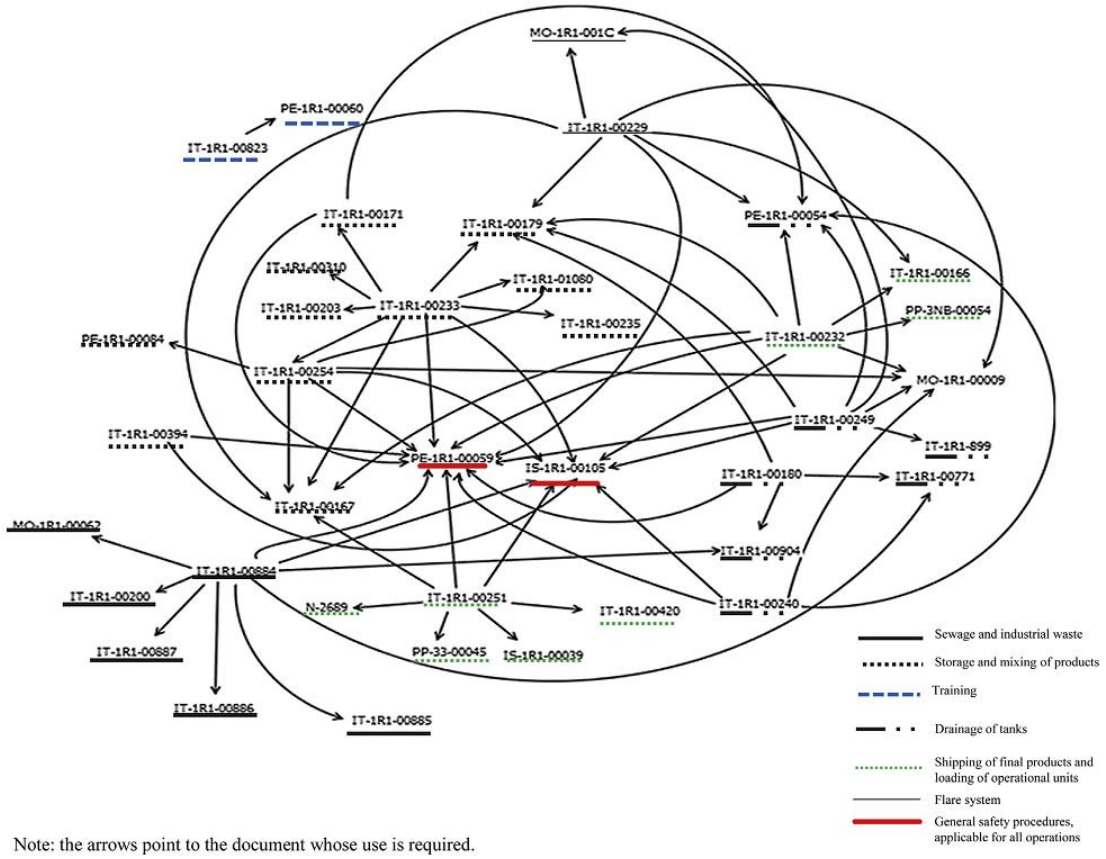


Figure 31: Relationship between procedures used in the control room of the logistics area (SAURIN and GONZALEZ, 2013)

When it comes to Procedure Availability, it is noticeable that it played an important role in the Chevron Richmond refinery accident (2012). At the time of the accident, Chevron did not have procedures to direct when a unit should be shut down, which made it difficult for operators to make the decision to shut down the unit due to the leak. In the investigation report, CSB states that if a similar leak was to occur in a Chevron refinery the unit would be shut down if the new guidelines developed after the accident were followed (CSB, 2014b).

Resources group

Resources group is comprised of the PIFs Tool Availability and Tool Quality and Workplace Adequacy. Safety of oil refinery operation depends mainly of the process variables being within the designed range for appropriate operation. Thus, tools like indicators of temperature, pressure, level, and flow are particularly important to oil refinery proper

operation. If the operators have no access to the values of such parameters (tool is unavailable) or if they have access to incorrect values (tool lacks quality), they are unable to correctly assess the situation and make the right decisions. Indeed, tool availability was marked as "highly relevant" to operators' action in refinery control room by most of the specialists interviewed.

The evidence of the relevance of Tool Quality can be observed in some of the accidents analyzed in Chapter 3. In the Tosco Avon Refinery Accident, the malfunction of temperature was an important PIF for the operators' error. The data logger temperatures on the control room monitor were fluctuating between high, low, zero and then back to normal, and the confusing temperature readings contributed for the operators not to follow the procedure regarding depressurizing the system (EPA, 1998). Tool quality was also crucial at BP Texas City refinery accident. The level transmitter of the Raffinate Splitter Tower showed a decreasing level to operators when it was actually increasing (Event 2 at Figure 17, Chapter 3). Moreover, the tower redundant high-level alarm failed to initiate. When the blowdown drum was being overfilled (Event 4 at Figure 17 , Chapter 3), its high-level alarm also failed to initiate, and the crew was not aware of the overfill. At that point, an available tool also played a major role for the operators to end up to overfill the tower: The level could also have been verified at site using the sight glass; however, it was as unreadable because of a buildup of dark residue for several years. The tools the crew had to check the tower level were, therefore, unavailable or lacking quality.

When it comes to workplace adequacy, one of the specialists answered "poor Ergonomics of Control rooms" to the questionnaire open question "What are the factors that could affect such operator errors?". It is intuitive that the adequacy of the control room regarding ergonomic factors is an important PIF for any industry, including oil refineries. Also, since most refineries currently have a centralized control room, where all units are controlled, it is important for the control room to have a design that makes it easier for operators to communicate along different units while preserving a distraction free work environment, that incentivizes operators' concentration and focus.

Team Effectiveness group

Team Effectiveness is evaluated in reference to communication and team coordination. Since the HERO HRA Methodology is developed by having the crew as a unit of analysis instead of a single operator, these PIFs are intuitively relevant. Also, two

specialists highlighted communication problems (“poor quality of communication” and “lack of communication”) when they answered the open question about the factors that could affect operator errors. Indeed, most specialists marked communication quality and communication availability as “highly relevant” to operators’ actions in refinery control rooms.

In Tosco Avon Refinery Accident (1997), radio communication did not work properly between the outside operator and the operators in the control room. Hence, operators in the control room could not be sure about what temperature the outside operator could read on the field panel. This malfunctioning communication equipment would refer to the PIF Communication Quality. Communication Quality also played an important role also in BP Texas City refinery accident, when the Night Lead Operator left the refinery one hour before his shift end and put an unclear information at the logbook about his shift operation. The Day Board Operator thus started his shift with little information on the state of the unit. Interestingly, two specialists highlighted communication during shift handover as important PIFs in the questionnaire.

Most specialists marked the PIFs comprised in Team Coordination - leadership, team cohesion, responsibility (role) awareness, team composition, team training - as highly relevant. These PIFs were indeed very relevant in the Chevron Richmond refinery accident (2012). Operators would not use Stop Work Authority as they thought the decision should be made by someone else who would be higher in the organizational hierarchy (poor Responsibility Awareness and leadership).

The CSB investigation of the BP Texas City refinery accident (CSB, 2007) also pointed poor team effectiveness as an important PIF. Indeed, Team Composition was not ideal, since after Day Supervisor A left no technically trained personnel was assigned to assist and supervise the Board Operator. The crew was then lacking an ISOM-specialist during the startup. The two Process Technicians (PTs) who had ISOM knowledge and experience were not assigned to assist with the startup. Responsibility Awareness was also deficient and it was unclear who was responsible for ISOM unit supervision once Day Supervisor A left, and the one individual available to provide such supervision lacked technical knowledge of the unit. Had the second Day Supervisor on shift (Supervisor B) left his work at the Aromatics Recovery Unit to assist in the raffinate startup, his presence in the control room would likely not have been helpful, as he had little technical expertise on the unit.

Knowledge/Abilities group

Most specialists marked the PIFs within knowledge/abilities group - Task Training, Attention, and Fitness for Duty (Physical Abilities and Readiness) – as "highly relevant". This group also comprises the PIF Knowledge of Plant Conditions.

In Tosco Avon refinery accident, Task Training played an important role behind operators' errors. According to EPA investigation (EPA, 1998), operators were not well-trained for abnormal situations. In the BP Texas City accident refinery, the same was pointed by CSB (2007): The operators did not receive adequate training for the hazards of unit startup, including overfill scenarios.

The PIF Fitness for Duty also played a major role in the BP accident. The operators were likely to be fatigued, being far from ideal to deal with an abnormal situation since they were on duty for more than 29 consecutive days. Also, when the pressure inside the tower raised, operators focused only on strategies to reduce pressure rather than also question why the pressure spikes occurred. CSB report identified this behavior as a cognitive fixation or a cognitive tunnel vision - focused attention on an item or action to the exclusion of other critical information, which is a typical performance effect of fatigue, according to Rosekind *et al*. (1993).

Knowledge of Plant Conditions played a major role in the Chevron Richmond refinery accident (2012). One of the reasons for the misdiagnose was the lack of awareness about the thickness of the pipe. "The inspectors informed the group that the 4-sidecut pipe walls were thinning due to sulfidation corrosion, but data collected as recently as two months prior indicated the 4-sidecut line had sufficient wall thickness to last until the next turnaround in 2016" (CSB, 2014b).

Bias group

Bias group is composed by Motivation/ Commitment, Confidence in Instruments, Familiarity with Stituation. Motivation/Commitment was an important PIF in the BP Texas City refinery accident (2005), and probably affected all Human Failure Events committed in the accident. Indications of the lack of commitment are the fact that the Night Lead Operator left the refinery approximately an hour before his scheduled shift end time, and the ISOM-experienced Day Supervisor, Supervisor A, arrived for his shift at approximately more than an hour late.

Confidence in Instruments can also have a great impact on operators' actions. They often do not trust the information coming from temperature and pressure indicators, for example. It is not about the instrument being reliable or not, it is about the operators believing it is reliable or not. The mistrust happens mainly because that instrument did not work well in the past. This PIF was clear in the Tosco Avon refinery accident, when the operators did not trust the temperature readings. This PIF was also observed during the visitation of a refinery control room, where an alarm was sounding but the operator did not answer to it and replied that he did not trust the temperature indicator, which he believed was probably wrong.

Familiarity with the situation is well related to near misses events. This probably is one of the main reasons for operators not to follow procedures as well as procedures not being updated. In the accident investigations, it is very common to find out that the situation happened before, and operators dealt with it as they found adequate. Since, in the past, no big accident occurred, they continue to deal with it the same way they had until then (which is the incorrect way). During the BP accident, for example, filling the bottom of the tower above 50% of the transmitter reading was not unusual during startups and did not lead to a big problem until it did. The same can be seen during the Tesoro Anacortes refinery accident (2010): It was common to call for more people to assist at the task of startup the offline bank of heat exchangers. Most specialists marked this PIF as "highly relevant". Finally, Competing or Conflicting goals is also a major PIF in refinery operations as the operators have to balance many competing goals between production and safety.

Stress group

The stress group is comprised of stress due to situation perception (perceived situation urgency and perceived situation severity) and stress due to decision. Stress due to Decision can be seen whenever the operators face the possibility of having to shut down the unit or stop an operation. Since refinery process is comprised by a series of units that depend on one another, operators know the consequences in production may be major when they face the decision to shut down a unit. CSB (2014) considers that this was one of the reasons for operators not to use "Stop Work Authority" to shut down the unit due to the leak: Operators were reluctant to speak up and delay work progress, and feared the reprisal they would face if they stopped the job.

Perceived Situation Urgency was seen as highly relevant to operators' actions by most of the specialists. This PIF is especially important to refinery operations because it is related

to how fast a disturbance at the plant can turn into a disaster. A leak of hydrocarbon, for example, may form an explosive cloud minutes after it happens. The stress due to perceived situation urgency is also related to time constraint: The crew's perception of the time available to complete the task. Most of the specialists marked this PIF as "highly relevant".

The fact that a disturbance in the plant can turn into a disaster also relates to perceived situation severity. The awareness of working with flammable, explosive and toxic fluids and the potential disasters that may happen at the plant rises the stress of the operators, which can influence their behavior when facing a dangerous situation. Ardakani *et al*. (2013) actually performed a study about stress with 100 workers of an oil refinery control room and concluded that approximately 62% of the workers presented a high level of stress.

Task Load group

The task load group is comprised of cognitive complexity, execution complexity, extra work load, and passive information load. Refinery operations are normally complex due to the amount of variables to be observed and adjusted to situations of abnormal condition of the plant. Some operations are particularly complex. These include, for example, the startup or shutdown of a unit. CSB (2007) states that startup and shutdown are two of the most critical periods of plant operations, and that these critical periods experience unexpected and unusual situations. Because of that, BP's process safety guidelines recommended that "supplementary assistance" should be provided, such as experienced supervisors, operating specialists, or technically trained personnel during unit startups and shutdowns (which was not followed during the startup of the isomerization unit leading to the accident in 2005). Besides, startup and shutdown can also present a high level of Execution complexity, with many steps to be followed.

In answering the open question about factors that could affect operators' action, one of the specialists highlighted "too many demands on the operators time at critical part of procedure" and another "Extra work that has to be performed in addition to the main tasks" – both are related to extra work load. This PIF was especially relevant to the accident in BP Texas city refinery. The board operator who started the Isomerization unit divided his attention with other units. This situation is not uncommon, especially during economic crisis, as they may reduce costs. This was what happened in the BP refinery. In 1999, the BP cut fixed costs nearly 25 percent, resulting in plant-wide staffing reductions, and combined and

consolidated from two to one the board operator positions for the AU2 and ISOM units (CSB, 2007).

Passive information load was also highlighted by specialists in the questionnaire, especially regarding the amount of alarms that can sound at the same time (alarm avalanche). Interestingly, a questionnaire survey was conducted for the Health and Safety Executive (HSE) in 13 process plants which include oil refineries, chemical plants, and power stations (BRANSBY; JEKINSON, 1997). The study stated that operators felt distracted by the alarm flood which contains many nuisance alarms; operators were then used to give a minimum attention to these little operational value alarms and silence them in order to only investigate them once the plant was stabilized. The authors noticed that in general, there were more problems with alarm systems in the plants equipped with modern computer based distributed control systems than some of the older plants, which use individual alarm fascia. Most operators complained that the alarm flood was unmanageable during plant upsets and sometimes they accept the alarms without even reading and understanding them.

4.2.4.2 CFM-PIF BBN

The CFM-PIF model is the third layer of the HERO HRA Methodology. Through BBNs, it is possible to model the relationships between the PIFs and the CFMs, and between PIFs of different levels. At the BBN, the nodes represent the variables (CFMs and PIFs) and the directed arcs represent the direct causal relationship between them, forming and acyclic directed graph.

As explained in Chapter 2, a BBN symbolizes the structure of the network, i.e. the arrangement of the nodes and arcs to show the causal relationship between them. Quantitatively, the BBN involves the quantification of the strength of the causal relationship between the nodes probabilistically (EKANEM, 2013). This sub-section focuses on the qualitative aspect of the CFM-PIF BBN model.

Figure 32 shows the causal relationship between CFM and PIFS. Level 1 PIFs (blue nodes) have direct influence on the CFMs (green nodes). It is considered that each CFM can be influenced by all PIFs. The BBN also represents the PIF grouping and hierarchy: the blue nodes represent Level 1 PIFs, the orange nodes represent Level 2 PIFs, and the yellow ones refer to level 3 PIFs.

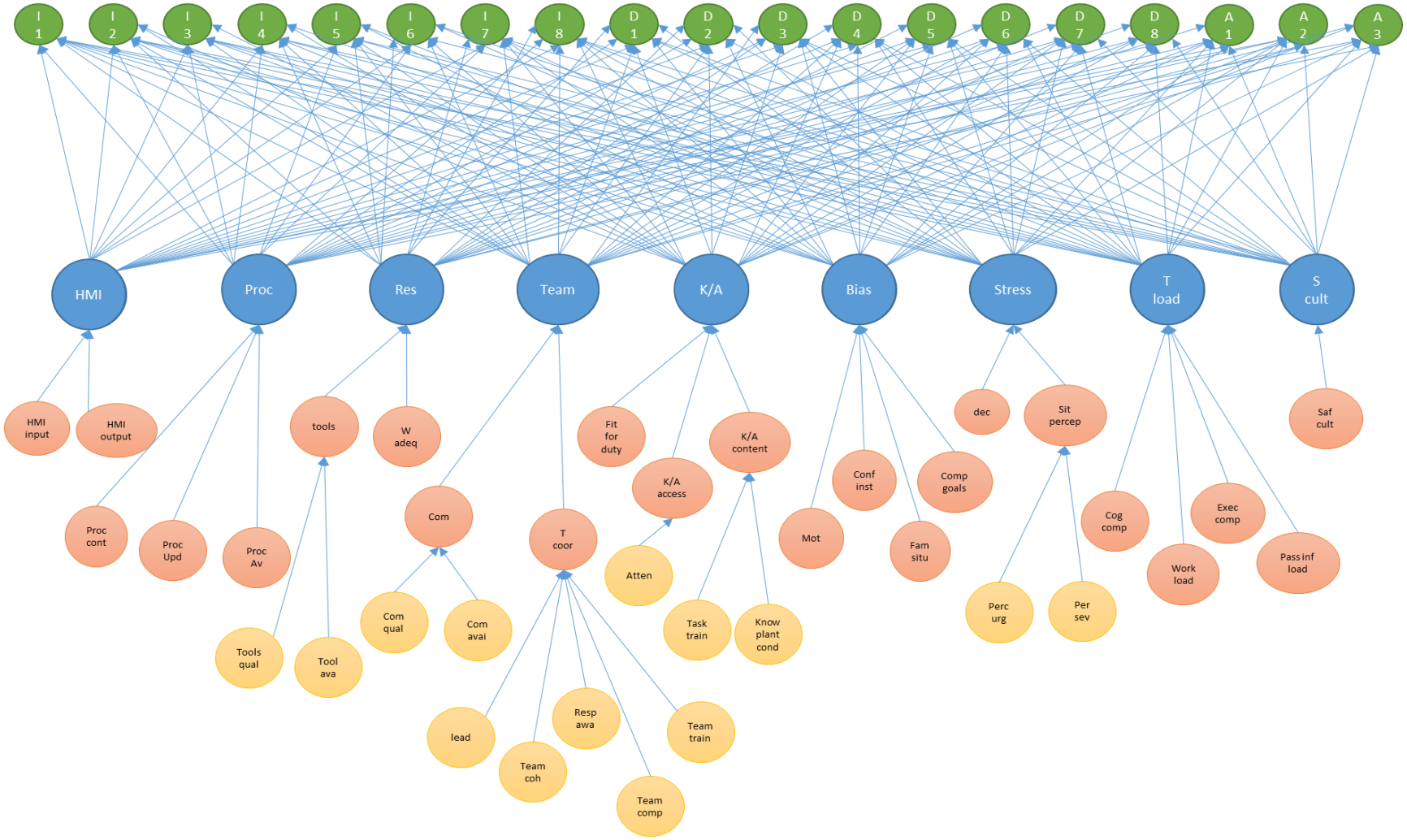


Figure 32: Master CFN-PIFs BBN

The CFMs in are indicated by their ID, as referred in Table 6. The PIFs names are abbreviated, and can be fully seen in Table 7.

During the analysis of a scenario, a BBN model can be developed to model the effects of PIFs on each CFM (this implies building 19 BBN models in this case), or developing a single BBN model that includes all the CFMs. The second approach is recommended to use in the HERO HRA Methodology since it considers the effect of interdependency among the PIFs and CFMs, which should not be ignored in HRA (EKANEM, 2013).

4.2 HERO HRA METHODOLOGY MANUAL STEP BY STEP

This section introduces how to apply HERO HRA Methodology step by step, presenting the steps to qualitatively connect all elements discussed in the previous section. The result is the identification of the Human Failure Events, a Crew Response Tree, the Fault Trees and identification of the relevant CFMs and the identification of the PIFs, forming the three layers of the methodology. At the end of this qualitative analysis the analysts will have a complete knowledge of the scenario in terms of human actions and possible failures.

The steps to apply HERO HRA Methodology to a scenario consist of the following:

- Step 1: Scenario Development/Familiarization

Figure 33: Master CFM-PIF BBN

- Step 2: Development of Crew Response Tree
- Step 3: Identification of Crew Failure Modes for CRT Branches and Development of Fault Trees
- Step 4: Identification of relevant PIFs for the CFMs and construction of BBN models
- Step 5: Model integration and analysis of HFE Scenarios, Development of Narratives, and Identification of Dependencies

STEP 1 - SCENARIO DEVELOPMENT / FAMILIARIZATION

The first step to apply the HERO HRA Methodology is to develop the scenario that will be analyzed. The latter may be running a limited part of the process, for example, or a specific task that the crew is to perform. For instance, in a case where analysts perform risk analysis of the Hydrogen Generation Unit, they can delimit running part of the process to perform Human Reliability Analysis, such as the reaction section. It is also possible that they are interested in a task the crew has to perform, such as starting a unit or putting a heat exchanger bank back online after maintenance.

For the familiarization with the scenario, analysts must gather information about the process and interaction between the crew and the system in addition to information about the control room and operators' routines. The list below presents a guidance for the documentation and information analysts need. Depending on the scenario, analysts may need information not present on the list or may not need all documentation listed. In addition to the information and documents of the list, plant walk-throughs and visitations to the control room may give valuable information to the analyst about the scenario.

- Process Flow Diagram
- Piping and Instrumentation Diagrams (P&IDs)
- System / equipment design specifications from installation manuals
- Operating Procedures and Emergency Procedures
- Control system documentation, such as cause and effect matrix
- Control panel screens or a list of the variables the panel operator has access to
- Documents about the control room, such as layout
- Reports on recent incidents that relate to the scenario analyzed
- HAZOP and QRA reports that relate to the scenario analyzed
- Interview with relevant plant personnel
- Existing task analysis from analysis reports
- Training programs from training manuals
- Crew composition in terms of size, experience level, through interviews with plant management & plant personnel
- Information about crew shifts

STEP 2: DEVELOPMENT OF CREW RESPONSE TREE

Once there has been a familiarization with the scenario as well as with the process and the crew, analysts have to identify the safety function, which is defined as the main task the crew has to perform to maintain the process on a safe status or bring it back to the safe status when facing an abnormal situation. To identify the safety function, analysts have to evaluate the relevant process variables for the safety of a particular process / task - temperature, pressure, level, flow, and relevant plant conditions such as pipes integrity. The safety function will then serve to maintain these variables within the designed range or bring them back to such range.

Analysts may benefit from some questions to identify the important process variables and the safety function; namely "What abnormal situation can happen at this process / operators' task?", "which process variables are relevant to this abnormal situation?", "what should the operators do when face this situation to bring the plant to safety?". For example, in case the scenario analyzed is the operation of the refinery pipelines, analysts might act in accordance to the following guidelines:

- What abnormal situation can happen in this process / operators' task?

The pipelines may suffer corrosion and leak flammable material

- Which process variables/plant conditions are relevant to this abnormal situation?

Pipeline integrity, mass flow

- What should the operators do when faced with this situation to bring the plant to safety?

The operators would have to identify the leak and isolate the pipeline, by closing the valves and stopping the pumps.

The safety function in this case would then be to isolate the pipeline - which is the crew's action to bring the process bring to safety.

After identifying the safety function, analysts have to follow the flowchart presented in Section 4.1.1 to construct the CRT, answering the questions from Table 4 and establishing the Branch Points as indicated by Table 5.

STEP 3: IDENTIFY CREW FAILURE MODES

This step consists of tracing the causal model for the CRT branch points through Fault Trees to identify the CFMs related to each HFE. For further information on the Fault Trees, see Section 4.1.3; for further information on the CFMs, see Section 4.1.2.

STEP 4: IDENTIFICATION OF RELEVANT PIFS FOR THE CFMS AND CONSTRUCTION OF BBN MODELS

This step consists of identifying the relevant PIFs for the CFMs and modeling the relationship between them through BBN models. For each CFM the analysts can identify the contextual factors that would influence the crew's actions and recognize them as one of the HERO HRA Methodology PIFs from Table 7. Having the relevant CFMs and PIFs in hand, the analysts can proceed to connect them through BBNs.

STEP 5: MODEL INTEGRATION AND ANALYSIS OF HFE SCENARIOS, DEVELOPMENT OF NARRATIVES, AND IDENTIFICATION OF DEPENDENCIES

Step 5 is the final step. It initially consists of linking the CRT, the FT and the BBN to complete the three layers of HERO HRA Methodology, as shown in Figure 22. After the three layers of the model are complete and linked, analysts have access to the operators' possible actions in the scenario, the possible failure modes, and the contextual factors for these failure modes. The analyst is able, then, to develop a narrative version of the event to describe the causal chain and the role of context factors that lead to the HFEs.

CHAPTER 5 – HERO HRA METHODOLOGY APPLICATIONS TO REFINERY ACCIDENTAL SCENARIOS

HERO HRA Methodology was presented and discussed in Chapter 4. This Chapter will thus present three applications of HERO within the refinery operations context. The first of them will be in the Hydrogen Generation unit, which is the unit responsible for producing Hydrogen in the refinery especially for the reactions of the Hydrotreater Units. As will be explained, this scenario was based on the Qualitative Risk Analysis of the unit and was chosen for being the one with the most serious consequences. It consists of the rupture of the reactor tubes, which leads to leaking process gas into the radiation chamber. This scenario was qualitatively analyzed in details, applying the steps described in Chapter 4, Section 4.2

The second scenario to be presented in this chapter, in sub-section 5.2, is a past refinery accident scenario. This scenario was based on the Chevron Refinery accident in Richmond, California (USA), in 2012, which was described in Chapter 3, Section 3.4. The qualitative analysis of this scenario will be outlined and discussed in Section 5.2, also following the steps described in Chapter 4. Finally, the third scenario, to be presented in Section 5.3 , centers on a leak of a pipe of the Hydrotreating unit. Just as the first scenario, it was developed based on the qualitative risk analysis of the refinery. In addition to the qualitative HRA of this scenario, I will present how to integrate the HRA in a Quantitative Risk Analysis. This will illustrate the strength of using HERO when performing a QRA of a refinery, thus highlighting its potential.

5.1 HERO HRA METHODOLOGY: HYDROGEN GENERATION UNIT SCENARIO

Hydrogen production is mainly obtained through hydrocarbons reforming, especially natural gas reforming. In a petroleum refinery, the Hydrogen Generation Unit (HGU) produces the hydrogen to be provided mainly to Hydrotreater Units. These demand a large amount of hydrogen for its reactions. An HGU is usually made of the following sections: Desulphurization, Reforming, CO conversion, Purification by PSA unit, Steam generation and Process condensate treatment. This process is briefly described below.

The HGU feed is, in general, Natural Gas, Natphta or a mix of both. The feed is mixed with hydrogen and goes through Sulphur removal in the desulphurization section. Once it has been through desulphurization, the product goes to the reforming section, where the hydrogen is produced at last. The latter is then purified in the PSA unit. The reforming reactions produce CO, which is converted into CO_2 in the CO conversion section. The HGU can also produce steam to be used in this unit or other refinery units, in the steam generation section.

Figure 34 illustrates the reforming section of the HGU unit analyzed in this case study.

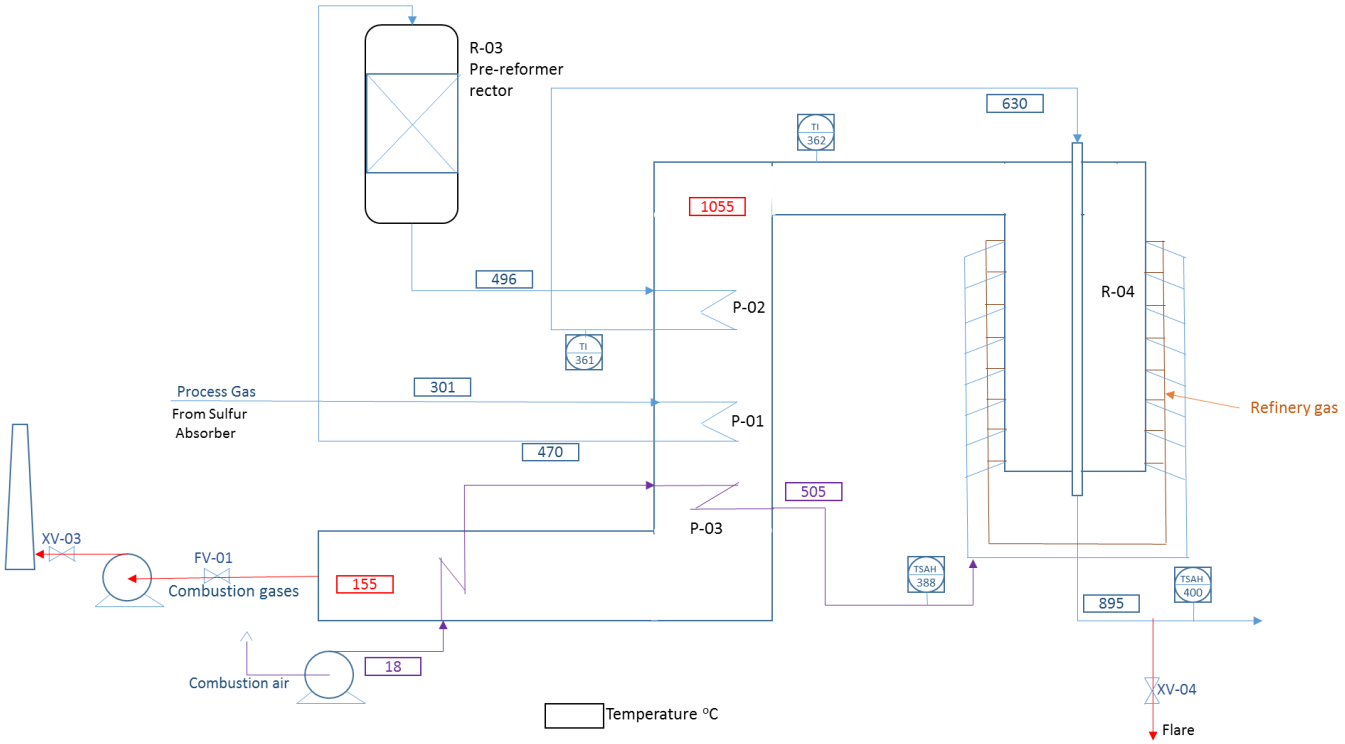


Figure 34: Reforming Section of the Hydrogen Generation Unit

This unit makes use of a pre-reformer reactor (R-03). Indeed, since this unit can use Naphta as feed, the installation of an adiabatic pre-reformer upstream of a tubular reformer (R-04) is suitable. This design is not uncommon in naphtha based plants and plant operating on fuel gases with higher concentrations of higher hydrocarbons: the pre-reformer reactions convert the higher hydrocarbons (equation 1 below), and the inlet temperature in the reformer can be increased, which reduces the size of the tubular reformer (UNDERGAARD, 2004).

The reformer reactor (R-04) uses a furnace to provide heat of reaction since the steam reforming reactions are overall endothermic. Therefore, the steam reformer is not simply a

catalyst reactor; it is a combination of catalyst reactor and heat exchanger. The steam reformer, in turn, consists of two main sections: furnace or radiant section and convection section. Equations 1, 2 and 3 describes the reforming reactions. Reactions (3) and (4) are endothermic whereas reaction (5) is exothermic.

$C_nH_m + nH_2O \rightarrow nCO + (n+m/2)H_2$ -Heat

(3)

$CH_4 + H_2O \rightleftarrows CO + 3H_2$ - Heat

(4)

$CO + H_2O \rightleftarrows CO_2 + H_2$ + Heat

(5)

All higher hydrocarbons are completely converted by reaction (1) in the pre-reformer R-03; reactions (2) and (3) will be almost equilibrated. The flow leaving the pre-reformer reactor no longer has higher hydrocarbons; it can thus be heated without risk of carbon formation due to thermal cracking. Reaction (2) takes place mainly in the tubular reformer, R-03. Some of the CO produced is also converted into CO_2 in the reformer, in accordance with reaction (3); most of it, however, actually happens in the CO conversion section. Reaction (2) is strongly endothermic and the heat of reaction is supplied indirectly by firing in the radiant section of the reformer.

The process gas enters the tubular reformer through the top of the vertical tubes and flows downwards. The flue gas collector passes the flue gas from the radiant chamber to the flue gas waste heat recovery section where the sensible heat of the flue gas is used to preheat the feed through heat exchangers P-01 and P-02 and the combustion air through P-03 and P-04. The flue gas leaving the waste heat recovery section is then sent to the stack through C-01. Given that this section has described the hydrogen unit scenario, the following subsection will describe the HRA scenario and I will analyze the hydrocarbon unit through HERO HRA Methodology, applying the steps described in the previous chapter.

5.1.1. HRA Scenario

The application of the HERO HRA Methodology consists of five main steps, as described in Section 4.2. Once again, these are the following: 1) Scenario Development/Familiarization, 2) Development of the Crew Response Tree, 3) Identification of Crew Failure Modes for CRT Branches and Development of Fault Trees, 4) Identification of relevant PIFs for the CFMs and construction of BBN models and 5) Model integration and analysis of HFE Scenarios, Development of Narratives, and Identification of Dependencies. In this subsection, each of these steps will be applied to the case of a hydrogen unit.

Step 1: Scenario Development/Familiarization

The scenario to be analyzed consists of a leak of process gas inside the radiation chambers of the reformer due to a leak at the reactor tubes (as indicated in Figure 35) . This scenario was chosen based on the QRA of this HGU; this particular scenario, among all the scenarios listed in the HAZOP, presented the more severe consequence: the risk of explosion.

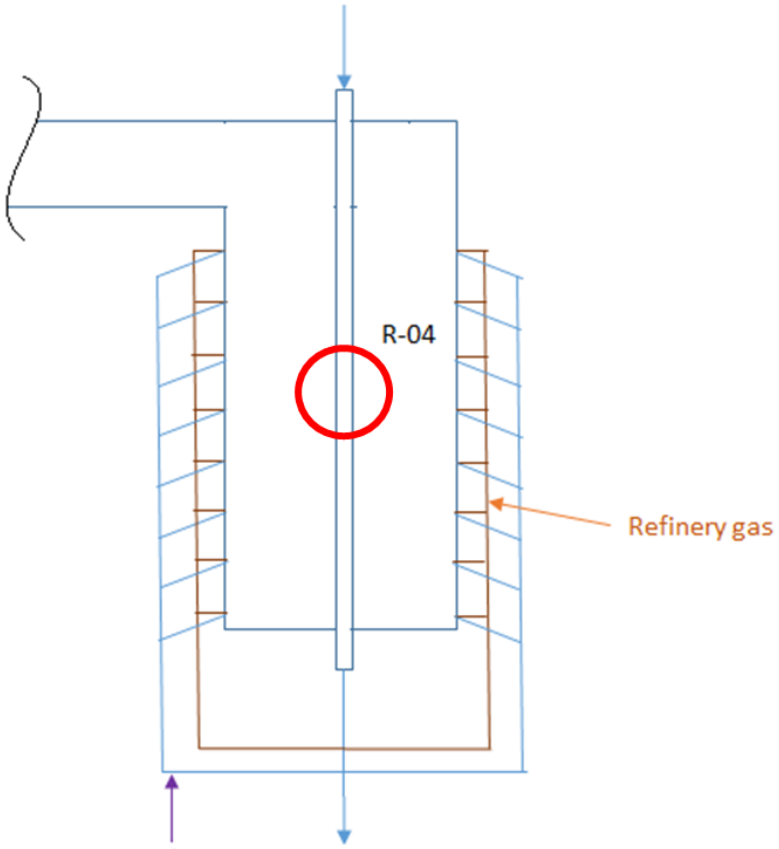


Figure 35: HGU Scenario - Leak location

For the familiarization with the scenario, we followed the guide list presented in Chapter 4 to obtain the necessary information. These included the process flow diagram, the P&ID diagram and information about the control system, information about the process and interaction between the crew and the system, and, finally, information about the control room and operators' routines and access to QRA and HAZOP reports. The Hazop extract for this scenario is as outlined in Table 8.

Table 8: HAZOP Table for the Scenario Analyzed

Guideword	Cause	Consequence	Safeguard
Contamination	-Leak on reformer tubes	-Increase of combustion gases temperature -Risk of explosion	-TSAH 400 -TI 362 -TI 361 -TI 388

A small hole in the reformer tubes could leak process gas into the radiation chamber of the reformer. The content of the process gas, especially the hydrogen, could then react with the oxygen still present in the combustion gases, which is a very exothermic reaction. The heat produced would thus increase the temperature of the combustion gases, which, in turn, would heat even more the feed going through the heat exchangers P-01 and P-02 and the combustion air going through P-03. The temperature indicators TI-362, TI-361, and TI-388 would therefore indicate higher temperatures than normal process temperatures, which would be visible to the operator, and the associated High Temperature Alarms (HTA) would sound. The exit temperature of the process gas, indicated by TSAH-400, would also be higher than normal.

According to the automatic control of this unit, TSAH-400 actually activates the trip of the reformer. The trip consists of shutting off all air combustion and refinery gas to the burners, stopping the feed to the reforming section, depressurizing the furnace and the reformer, and opening XV-04 to send process gas from the reformer to the flare. The scenario established in this paper considers the failure of the automatic trip of the reformer. The operator would then have to understand the cues and trip the reformer manually. It also considers that the HTA of TI-361/362/388 will function.

In a case in which the operator does not trip the reformer, the heat generated by the exothermic reactions could increase the temperature above the design temperature of the

reformer tubes. This would lead to a catastrophic rupture of the tubes, and a high amount of process gas would rapidly leak into the radiation chamber, which would cause an explosion.

Step 2: Development of Crew Response Tree

Once we have been through a familiarization with the scenario as well as with the process and the crew, we have to identify the safety function. The safety function is defined as the main task the crew has to perform to maintain the process on a safe status or bring it back to the safe status when facing an abnormal situation. In case the scenario is extracted from a HAZOP, the abnormal situation is already identified; in this case, it is of a leak of process gas inside the radiation chambers of the reformer due to a leak at the reactor tubes. The main task to bring back the process to a safe status would be to manually trip the reactor.

The safety function could also be identified following the guide questions presented in Chapter 4, namely:

- What abnormal situation can happen in this process / operators' task?

A leak at the reactor tuber, leading process gas inside the reaction chambers of the refomer

- Which process variables/plant conditions are relevant to this abnormal situation?

Temperature, integrity

- What should the operators do when they face this situation in order to bring the plant to safety?

The operators would have to identify the leak and trip the reformer.

The safety function is then to trip the reformer.

The next step to construct the CRT is to answer the questions of the flowchart presented in Figure 3, chapter 3. Table 9 presents the answers, followed by the description of the Branch points in Table 10 and the CRT at Figure 36.

Table 9: Flowchart questions and answers for HGU scenario

No.	Question	Answer
1	Is the specific function designed to be initiated automatically?	Yes
2	Are there available instruments to indicate relevant process conditions to the operators?	Yes, the temperature is a relevant process condition and can be indicated by TSAH 400, TI 362, TI 361 and TI 388
3	Are there other other cues the operators can use to assess the situation?	No. If all the instruments fail ther operator can not assess the situation.
4	Are there procedures instructing the manual activation of the safety function?	Yes. The procedures indicate that in case of leak inside the radiation chamber the crew shoud trip the reactor.
5	Are there other resources the operators could use to manually activate the safety function?	Yes, operators can relate the unbalanced temperatures to an unbalanced combustion and decide to trip the furnace.
6	Are there additional equipment and manual actions that could be used to provide the specific safety function?	No.

Table 10: Description of Branch Points of HGU scenario

BP	Description	Application on CRT
A	Automatic trip of the furnace due to TSAH-400	Success path: automatic trip Failure path: failure of the automatic trip
B	Manually turning off the trip would not be applicable at this scenario.	NA
C	Relevant instruments: temperature indicators and alarms.	Success path: Temperature indicators and alarms work Failure path: Temperature indicators alarms fail
D	Operators can respond to alarms/indicators or not.	Success path: Operators respond to alarms/indicators to correctly assess the situation. Failure path: : Operators don’t respond to alarms/indicators

Table 10 – Continuation

E	This branch point considers whether the crew is in the correct procedure and chooses the right path to manually initiate the safety function.	Success path: crew relates it to a leak and follow procedure to trip the furnace Failure path: crew doesn't relate it to a leak
F	The operators can relate the unbalanced temperatures to an unbalanced combustion and decide to trip the furnace.	Success path: operators believe there's unbalanced combustion and decides to trip the furnace Failure path: Operators don't identify the reason for the temperatures rise
G	Safety function is not impaired by equipment (hardware / system) failure.	This BP is ignored because of the low probability of this event. Therefore this BP is not created
H1	After relating the abnormal condition to the right cause, operators successfully initiate the safety function manually	Success path: Operators successfully trip the reactor Failure path: Operators fail to trip the reactor
H2	After relating the abnormal condition to the another possible cause, operators successfully initiate the safety function manually.	Success path: Operators successfully trip the reactor Failure path: Operators fail to trip the reactor

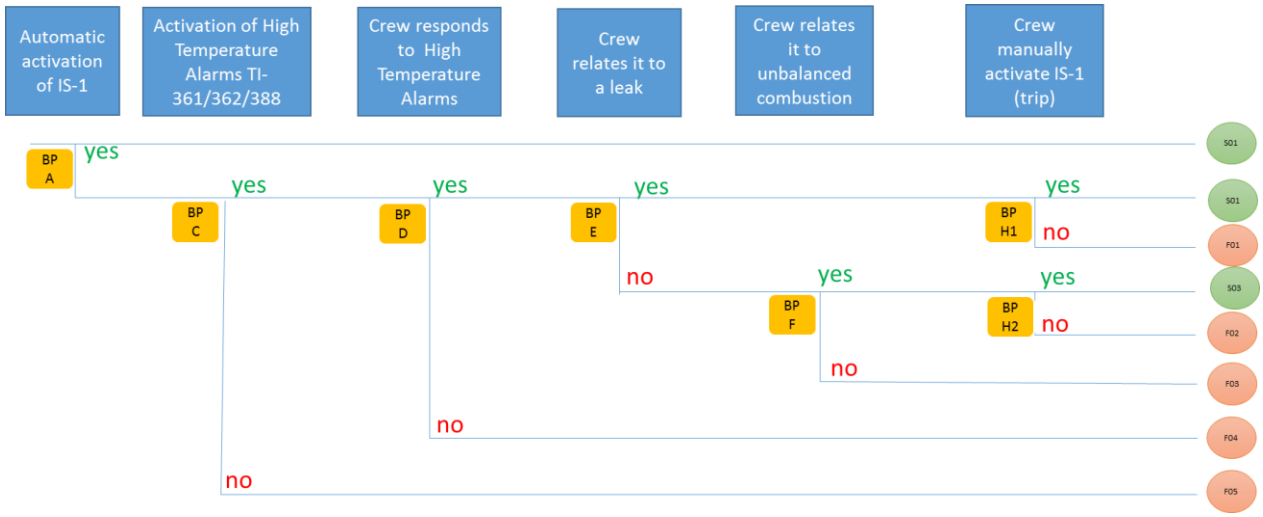


Figure 36: CRT of HGU scenario

The possible outcomes for the scenario are the following:

S01: Automatic activation of IS-1 (automatic trip of the reformer)

S02: Failure of IS-1, but crew notices HTA, relates it to the right cause and successfully trips the reformer

F01: Risk of explosion: crew notices HTA, relates it to the right cause but fails to trip the reformer

S03: Crew notices HTA, relates it to unbalanced combustion, trips the reformer

F02: Risk of explosion: crew notices HTA, relates it to unbalanced combustion but fails to trip the reformer

F03: Risk of explosion: crew notices HTA, can't find the cause and therefore doesn't trip the reformer

F04: Risk of explosion: crew does not notice HTA

F05: Risk of explosion: temperature indicators and alarm fail

Step 3: Identification of Crew Failure Modes for CRT Branches and Development of Fault Trees

Each branch point BP at the event tree related to human events can be related to one or more CFM (note that BPs A and C ate not related to human events, but to the system). BP D is related to whether the crew responds to the HTA or not. The HTA are key alarms for this scenario, since they are the most important cue for the correct assessment of the plant, and for the identification of abnormal situations. In HERO HRA Methodology, the fault in noticing and responding to the alarms is described by the CFM "Key Alarm Not Responded to" (I1).

As was described in Chapter 4, the CFM abovementioned includes failure to detect, notice and understand the alarm, as well as not perceiving the alarm or intentionally ignoring it. This CFM is in the I phase of IDAC, and the FT leading to it is in Figure 37, Figure 38, Figure 39 and Figure 40 where the red lines indicate the path for the CFM. This CFM can happen if the crew fails to decide to collect information (i.e. they decide to not respond to the alarms) and if the crew fails to collect information (i.e. they intent to respond to these alarms fait fail in executing it).

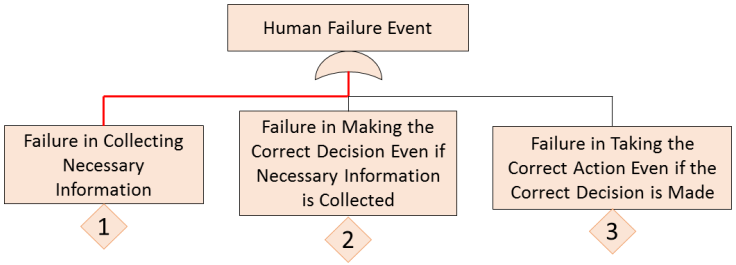


Figure 37: FT for BP D in HGU Scenario - Part 1

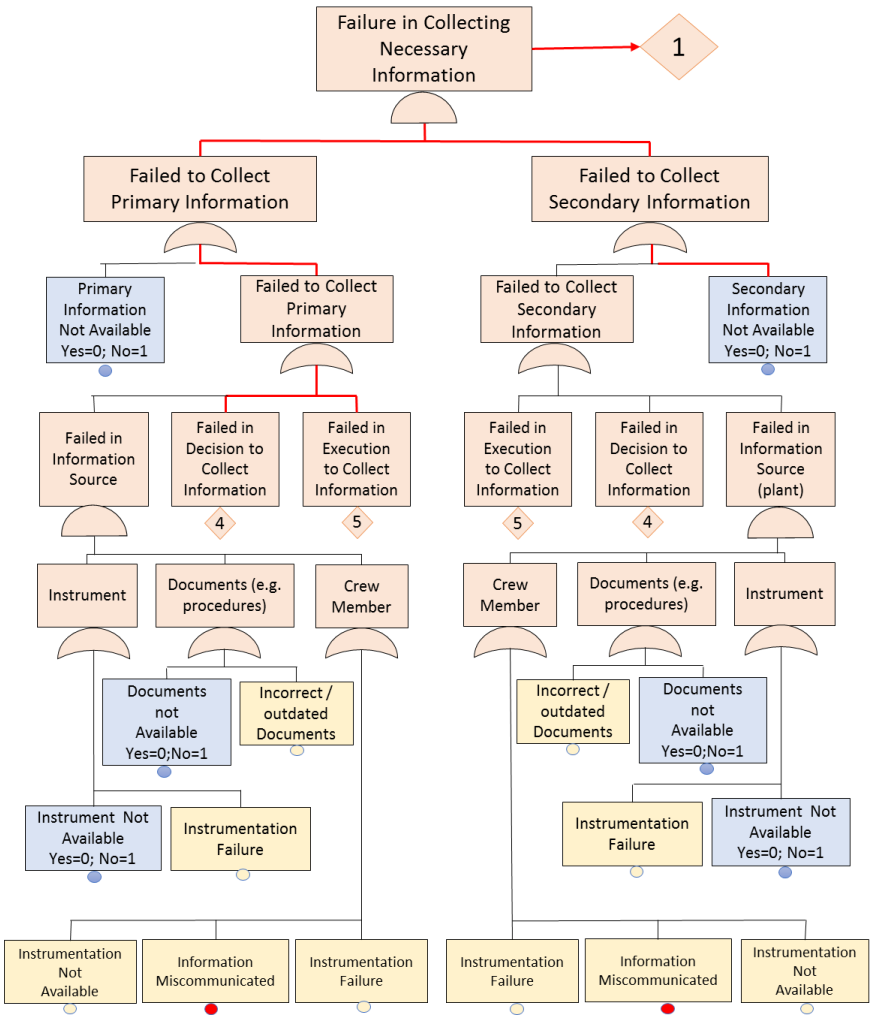


Figure 38: FT for BPD in HGU Scenario - Part 2

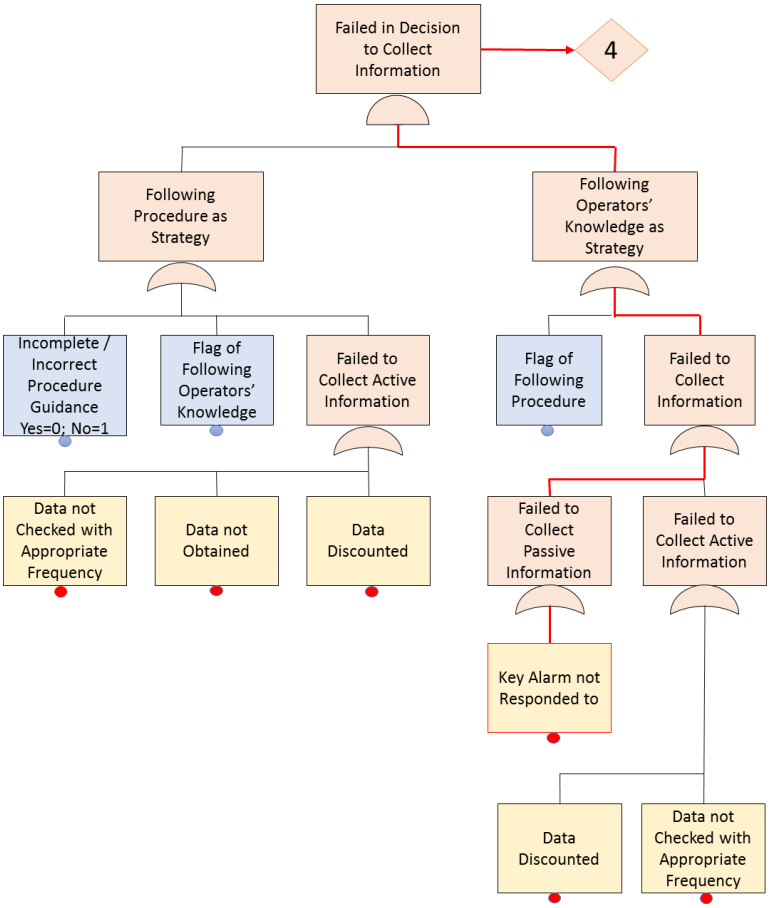


Figure 39: FT for BP D in HGU Scenario - Part 3

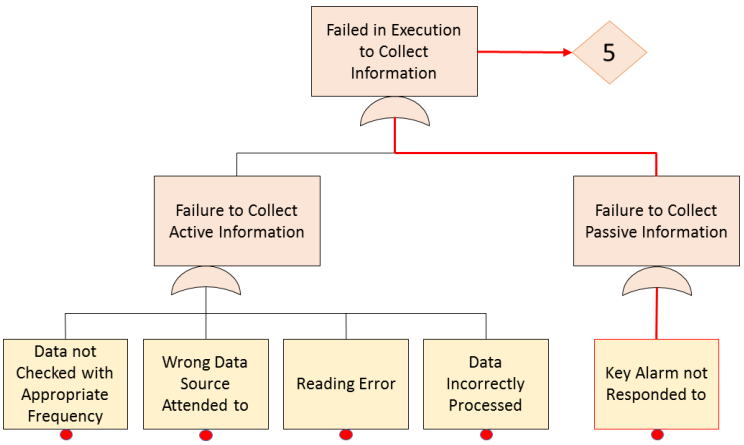


Figure 40: FT for BP D in HGU Scenario - Part 4

Branch Point E is related to correctly assessing the situation and identifying the source of the temperature rises, which is a leak inside the radiation chamber. This action would be in the D phase of IDA. The correspondent CFM is "Plant/System State Misdiagnosed" (D1), and the FT leading to that CFM is illustrated in Figure 41 and Figure 42.

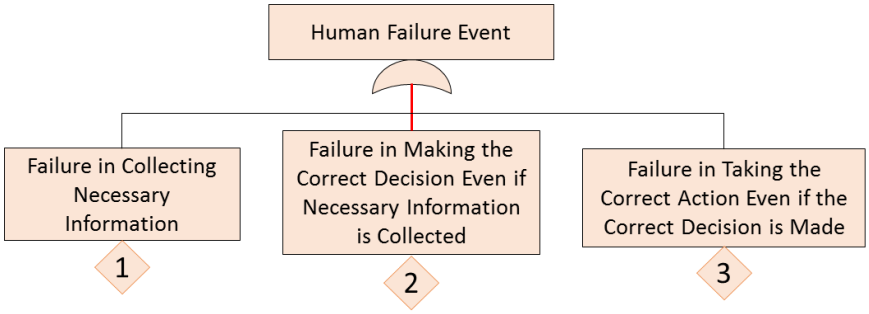


Figure 41: FT for BP E in HGU Scenario - part 1

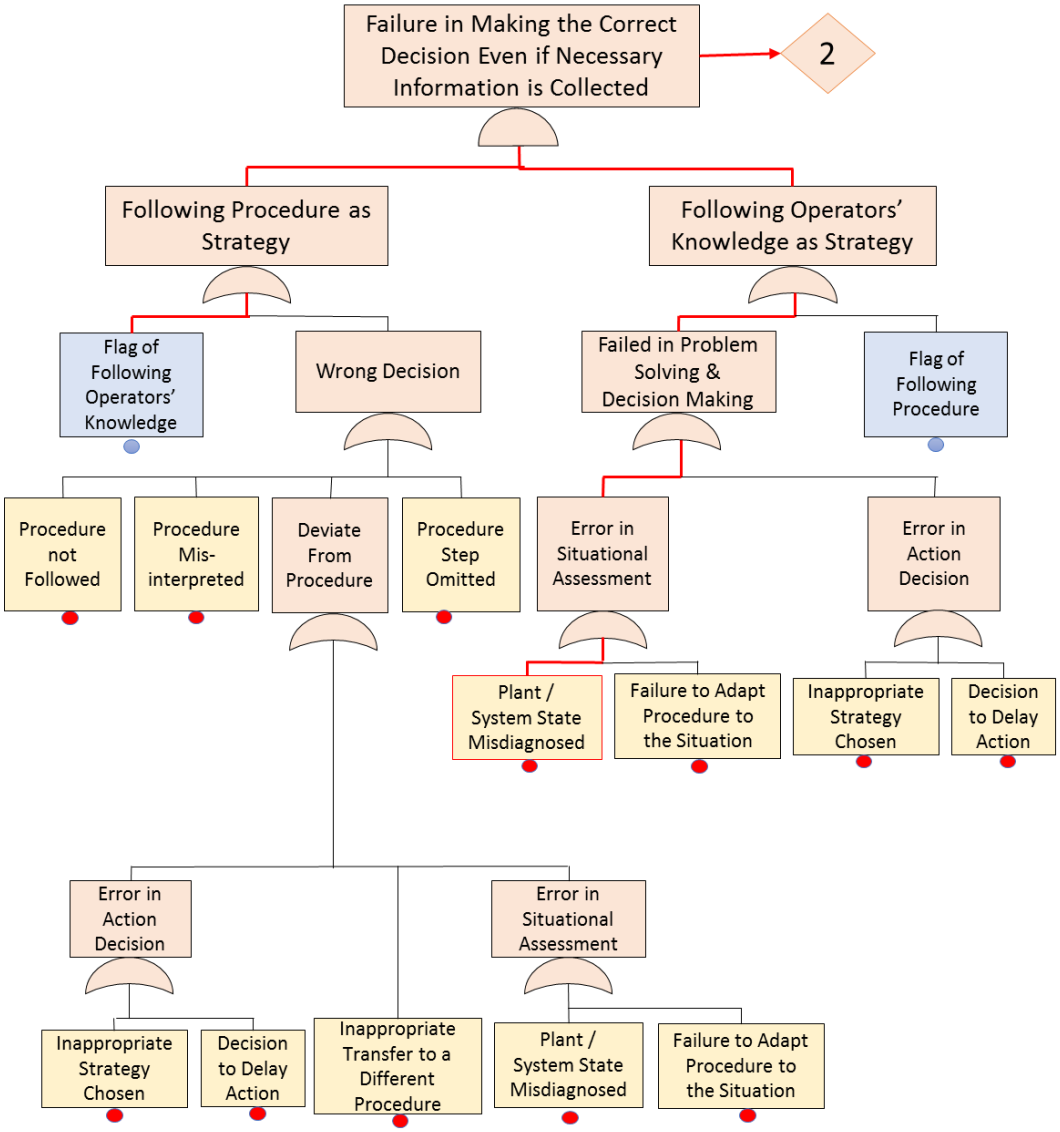


Figure 42: FT for PB E in HGU Scenario - part 2

The failure path in BP F is related to the crew not identifying the reason for the HTAs. The correspondent CFM is in “D” phase of the HRM, namely “Decision to Delay Action” (D7)., because the operators decided to identify a cause for the HTAs instead of acting on it. The FTs for these CFMs are illustrated in Figure 43 and Figure 44.

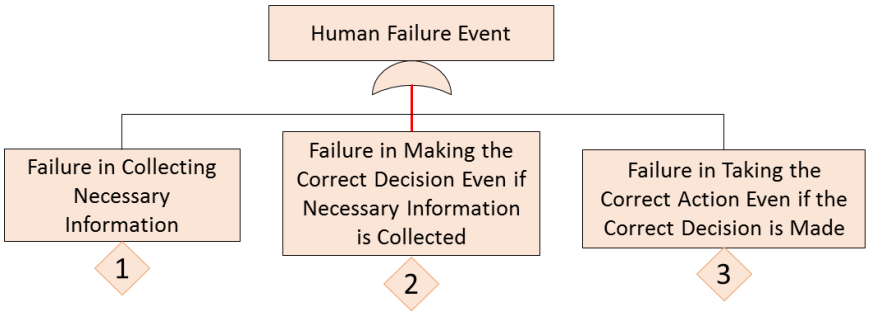


Figure 43: FT for BP F in HGU Scenario - part 1

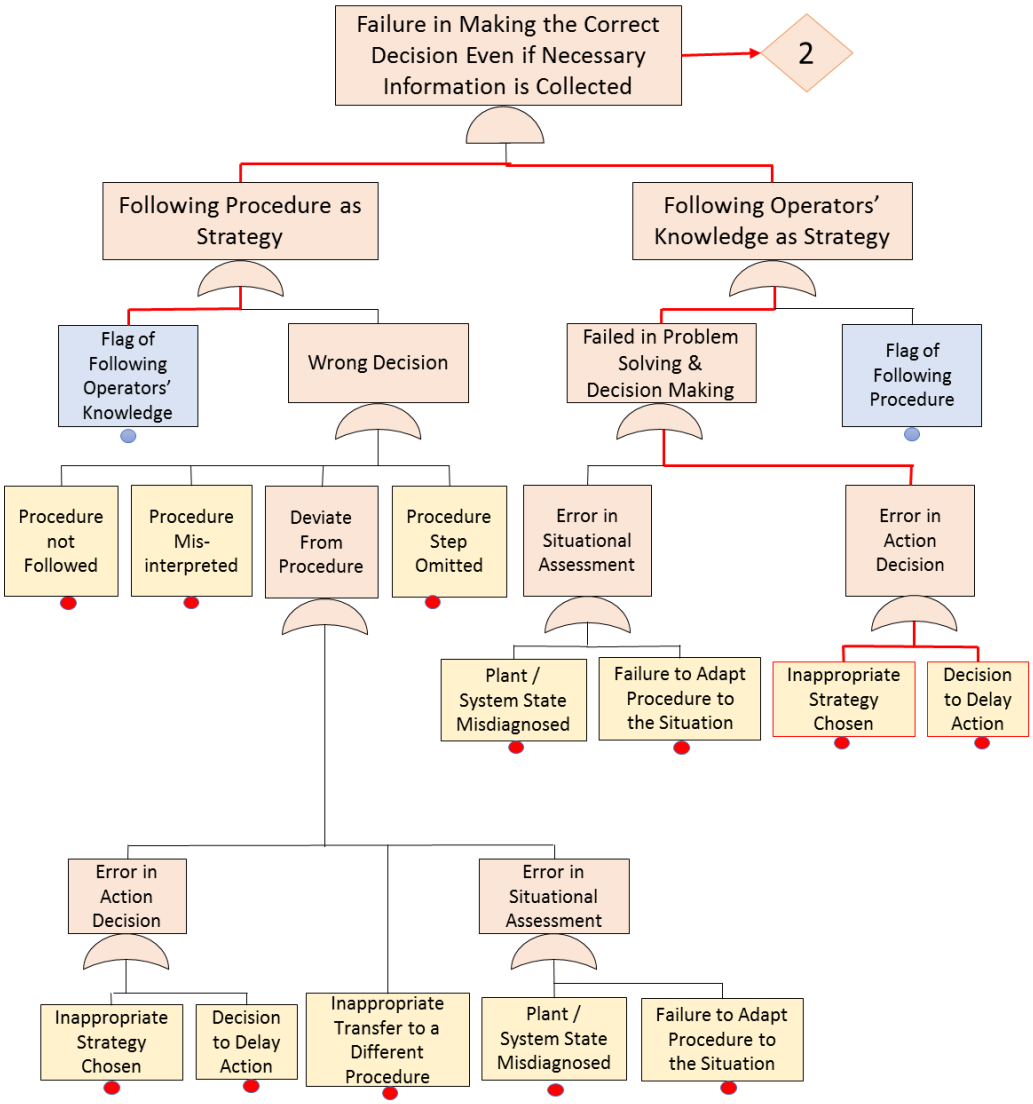


Figure 44: FT for BP F in HGU Scenario - part 2

Failure in BPs H1 and H2, in turn, are related to not successfully activate IS-1 (trip the reactor). This may be because the crew performs the action on the wrong system - "Action on Wrong Component / Object" (A3), or trips it too late - "Incorrect Timing of Action" (A1). The FTs for theses BPs are as follows in Figure 45, Figure 46, Figure 47, Figure 48:

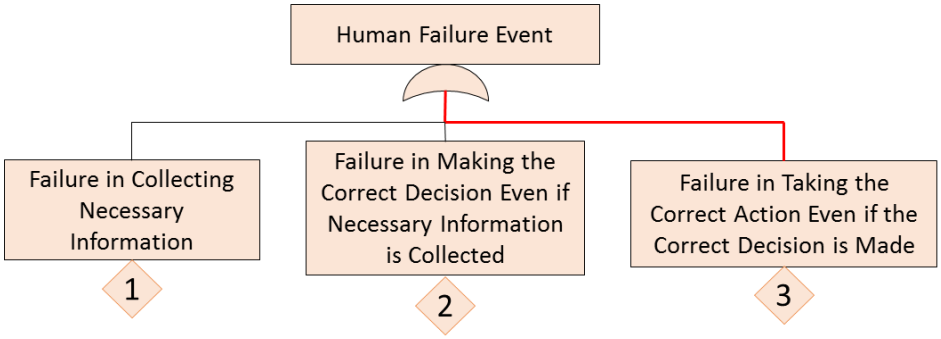


Figure 45: FT for BP H1 in HGU Scenario - part 1

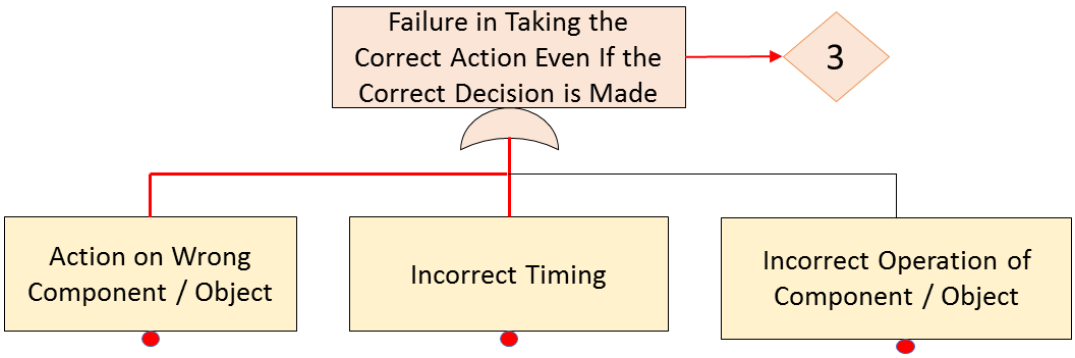


Figure 46: FT for BP H1 in HGU Scenario - part 2

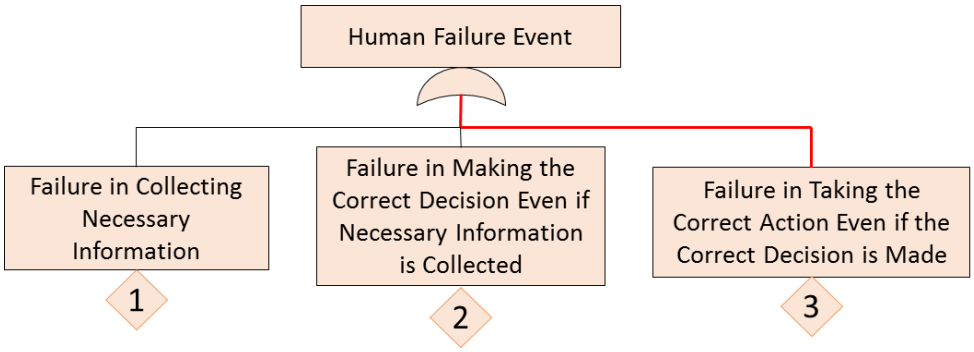


Figure 47: FT for BP H2 in HGU Scenario - part 1

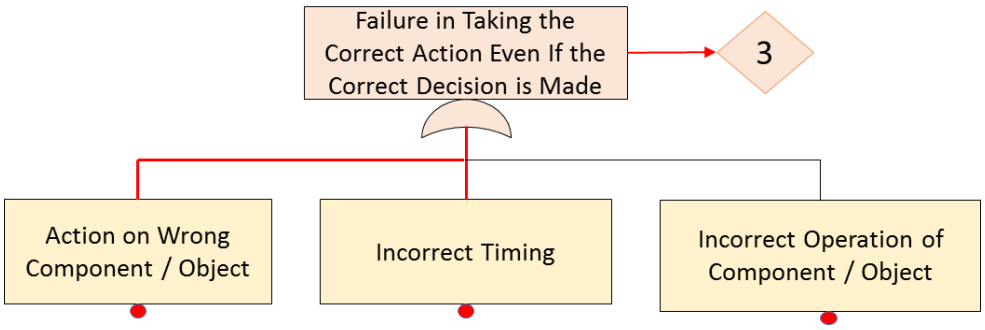


Figure 48: FT for BP H2 in HGU Scenario - part 2

Step 4: Identification of relevant PIFs for the CFMs and construction of BBN models

In this step, the possible factors leading to each CFM are analyzed as one of HERO's PIFs. The PIFs and the CFMs, in turn, are modeled through BBNs, turning into the 3rd layer of the methodology.

Table 11, Table 12, Table 13 and Table 14 below present the main PIFs for the CFMs of this scenario. The identification of these PIFs was made through an extensive discussion with analysts and engineers combined with visitations to the control room of this refinery and the observation of its operation. Note that these are the main PIFs for these specific CFMs, and other PIFs may be identified as having smaller influence on these CFMs.

Table 11: Main PIFs for CFM "Key Alarm not Responded to" (BP D) HGU Scenario

Possible reasons for the operators not to notice the alarms	**HERO HRA Methodology corresponding PIFs**
Too many alarms at the environment at the same time	Passive Information Load
Inadequate panel interface	HMI Output
Operator not attentive/tired	Attention
Operators working also on another unit	Extra work load
Not defined who should be paying attention to the alarms	Responsibility awareness, Leadership, Team Training
Too much ambient noise	Workplace Adequacy
Operator absent at the moment	Motivation/Commitment
Operator believes the temperature indicator may be incorrect	Confidence in Instruments

Table 12: Main PIFs for CFM "Plant/System State Misdiagnosed" (BD E), HGU Scenario

Possible reasons for the operators to misdiagnose the plant/system state	**HERO HRA Methodology corresponding PIFs**
The crew has no training in dealing with these HTA to identify the right cause for it	Task Training
The crew has no knowledge the tubes may already be suffering corrosion	Knowledge of plant conditions
The crew is not attentive/tired	Attention
The crew has no operator specialist in this unit	Team Composition
The operators are suffering from fatigue, for working too many days in a row	Fitness for Duty
The crew realizes the HTAs may be connected to a serious situations and get stressed	Perceived Situation Severity
To identify why the HTAs went off and identify that the automatic trip of the reactor failed is cognitive complex	Inherent Cognitive Complexity

Table 13: Main PIFs for CFMs "Decision to Delay Action" (BP F), HGU Scenario

Possible reasons for the operators decide to delay action / chose inappropriate strategy	**HERO HRA Methodology corresponding PIFs**
Operators cannot come to an agreement on how to proceed	Team Cohesion
Operators are not commited with safe operation of the plant	Motivation / Commitment
Operators are divided between safe operation and continuity of production	Competing of Conflicting Goals

Table 14: Main PIFs for CFMs "Action on Wrong Component/Object" and "Incorrect Timing" (BPs H1 and H2), HGU Scenario

Possible reasons for the operators to perform action on wrong component / in incorrect timing	**HERO HRA Methodology corresponding PIFs**
The panel is not clear enough on which component is on screen	HMI output
It is not clear which operator should do it	Responsibility Awareness
Operators are stressed about the decision to trip the reactor	Stress due to Decision
Operators working also on another unit or other section of this unit	Extra Work Load

Step 5: Model integration and analysis of HFE Scenarios, Development of Narratives, and Identification of Dependencies

When we integrate the FTs (Figure 37 to Figure 48) to the respective BPs in the CRT (Figure 36), it is possible to obtain the CFM cut-sets for the HFE scenario of interest. The HFEs scenarios can be identified as one of the outcomes in the CRT (F01, F02, F03, F04). For each of the outcomes the CFM cut-sets are as follows:

F01: A3+A1

F02: D1*(A1+A3) = D1A1 + D1A3

F03: D1*D7

F04: D1

All of these HFE scenarios contribute to the final HFE, which is the failure to trip the reformer in the case of a leak in the reactor tubes. The narratives, therefore, can be written as:

- The crew respond to the HTAs, relates it to a leak but, when tripping the reactor, they do so in the wrong object (A3 CFM)
- The crew respond to the HTAs, relates it to a leak but they trip the reactor too late A1 CFM)
- The crew respond to the HTAs; however, they relates it not to a leak but to an unbalanced combustion. Although this requires the tripping of the reformer as well, the crew do it in the wrong object (D1A1 CFM combination)
- The crew respond to the HTAs; however, they relates it not to a leak but to an unbalanced combustion. Although this would also require them to to trip the reformer, the crew do it too late (D1A3 CFM combination)
- The crew respond to the HTAs, but do not identify the reason for it. They choose the inappropriate strategy to deal with the situation and decide to search for more cues to identify a reason for the HTAs (D1D8 CFM combination)
- The crew respond to the HTAs, but do not relate it to a leak. The decide to delay any action on it (D1D7 CFM combination)
- The crew do no respond to the HTAs (D1 CFM).

Moreover, we know that these CFMs were enhanced by the factors listed in Table 11 to Table 14. Through the integration of the CRT BPs to the FTs, and the CFMs of the FTs to

the PIFs – thus completing the HERO HRA Methodology framework – it is possible to know how, given a leak on the reformer tubes, the reformer can suffer an explosion because of the crew' inadequate actions. We can also identify which factors would lead the crew to these inadequate actions. And, it is important to bear in mind that only with the knowledge of these paths and factors it may be possible to develop strategies to prevent them to happen.

5.2 HERO HRA METHODOLOGY: THE CHEVRON RICHMOND REFINERY ACCIDENT (2012)

This section analyzes a past accident using HERO HRA Methodology: The Chevron Richmond Refinery Accident. This accident, which was described in details in Section 3.4, was due to a catastrophic pipe rupture in a distillation unit, which released flammable hydrocarbon process fluid that partially vaporized into a large vapor cloud that engulfed 19 Chevron employees and turned to ignite. The immediate cause of the accident was a sulfidation corrosion of the pipe. The analysis of the accident shows that human failure events as well as organizational factors were also causes of the accident, as was highlighted in sub-section 3.4.2.

5.2.1 HRA Scenario

Step 1: Scenario Development/Familiarization

In this case, the scenario involves running a delimited part of the process: the distillation column and its pipes. In order to go through a familiarization with the scenario, we required documents that involved the Process Flow Diagram, the P&ID, the Operating and Emergency Procedures, the Control System Documentation, and, finally, documentation on the crew, such as training programs, crew composition. Since we are basing this specific scenario on the Chevron Richmond Refinery Accident, we will actually limit ourselves to focus on one of the pipes exiting the distillation column, as indicated in Figure 49.

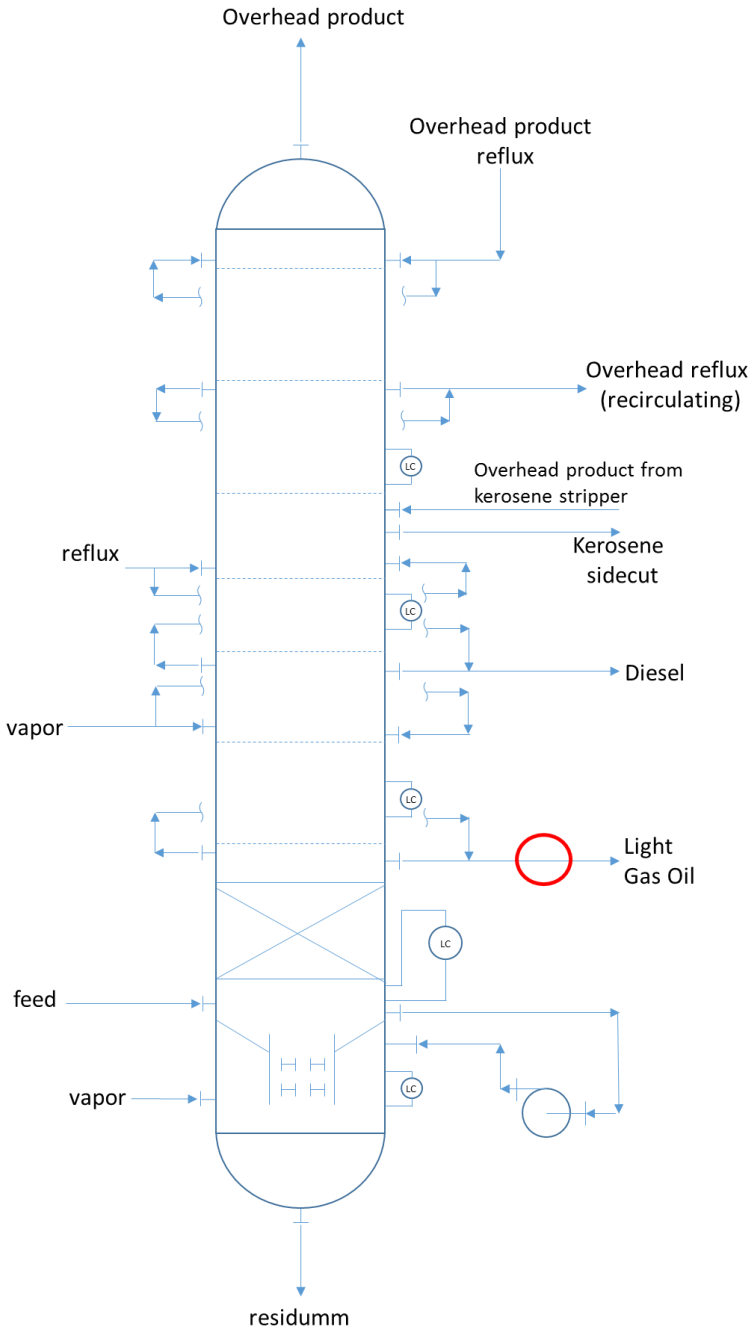


Figure 49: Distillation Unit Scenario - leak location

In the 4th side-cut of the column, light gas oil exits the column to be further refined and processed. This side-cut is not isolated by valves; therefore, if a leak occurs in this pipe, an operator could actually not block this section to repair it while the unit is operating. In terms of detection, it should be noticed that there was no flow indicator in this section nor hydrocarbons detectors in the field. And, since it is a small leak, even if there was a flow indicator, it would perhaps not detect such a small change between the flow in the beginning

of the pipe and in its end. In this sense, we consider hereafter that the detection could only happen visually.

Once a leak is identified in such circumstances, operators actually have two choices; they can either repair the leak while the unit it operating or they can decide to shut down the unit to fix/replace the leak. The report of the Chevron Richmond Refinery accident shows that the pipe walls were already too damaged by sulfidation corrosion; hence, the repair could not be easily done. Indeed, anything could increase the leak, making the situation worse - which is what happened during the accident used as the basis for this section.

Step 2: Development of Crew Response Tree

In order to identify the safety function, we can follow the guide questions:

- What abnormal situation can happen in this process / operators' task?

Since it is the operators' task to run the unit with safety and to focus on the pipes exiting the distillation column, the abnormal situation is a leak at the pipes.

- Which process variables/plant conditions are relevant to this abnormal situation?

Integrity of the pipes walls

- What should the operators do when they face such situation in order to bring the plant to safety?

The operators have to identify the leak and deal with it successfully. Since the pipe cannot be isolated by valves, the operators have two choices: repair it while the unit is running or shut down the unit to fix it and bring the plant back to safety. Since the pipe walls are actually too thin to go through a repair, the safety function is to identify the leak and shut down the unit to fix it. Once the safety function – identity the leak and shut down the unit – has been identified, the analyst can build the CRT (Figure 50) , with the aid of Table 15 and Table 16.

Table 15: Flowchart questions and answers for Chevron Richmond Refinery Accident (2012)

No.	Question	Answer
1	Is the specific function designed to be initiated automatically?	No. There is no control loop to shut down the distilation section in case of a leak in the pipes. Go to Question 2.
2	Are there available instruments to indicate relevant process conditions to the operators?	No. Go to Question 3.
3	Are there other other cues the operators can use to assess the situation?	Yes. The operators can visualize the leak in the field. Go to BP D.
4	Are there procedures instructing the manual activation of the safety function?	No. The procedures do not instruct to shut down the unit in case of a leak. Go to Question 5.
5	Are there other resources the operators could use to manually activate the safety function?	Yes. The operators can rely on their own knowledge to decide to shutdown the distilation section to fix the leak. Go to BP F.
6	Are there additional equipment and manual actions that could be used to provide the specific safety function?	No.

Table 16: Description of Branch Points of Chevron Richmond Refinery Accident (2012)

BP	Description	Application on CRT
A	NA	NA
B	NA	NA
C	NA	NA
D	Operators can visualize the leak and respond to it or not.	Success path: Operators visualize the leak and respond to it. Failure path: Operators don't visualize the leak or don't respond to it.
E	NA	NA
F	The operators assess the situation according to the leak.	Success path: operators believe the pipe damage is enough to require the shut down of the unit Failure path: Operators don't believe the damage is enough, and believe the leak can be fixed while the unit is operating

Table 16 - continuaton

G	Safety function is not impaired by equipment (hardware / system) failure.	This BP is ignored because of the low probability of this event. Therefore this BP is not created
H	After correctly assessing the situation, the operators can successfully shut down the unit	Success path: Operators successfully shut down the unit Failure path: Operators fail to shut down the unit

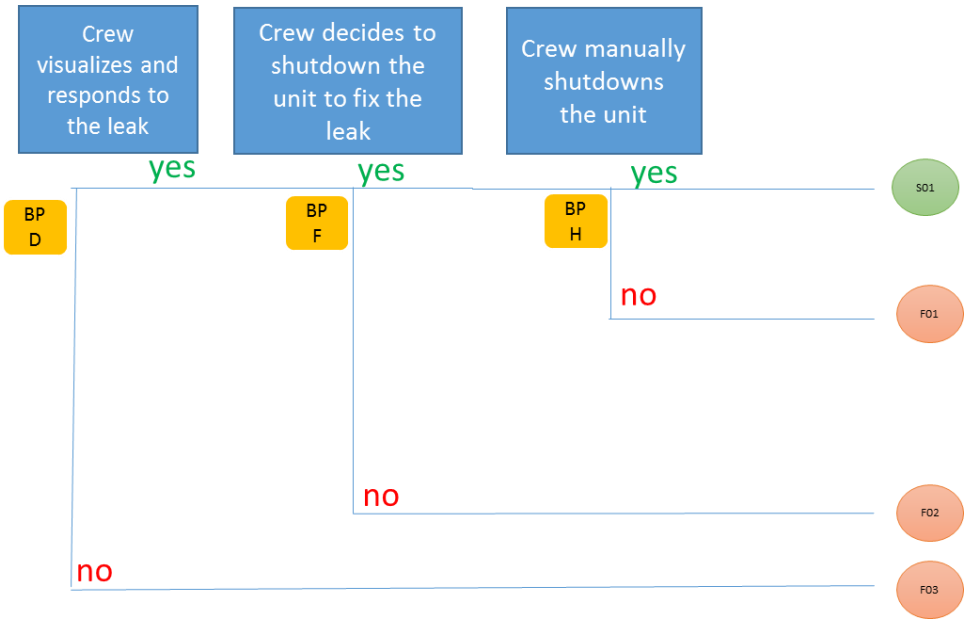


Figure 50: CRT for Chevron Richmond Refinery Accident (2012)

The possible outcomes are as follows:

S01: the crew visualize the leak and decide to shut down the unit and successfully does so

F01: The crew visualize the leak and decide to shut down the unit but fails to do so

F02: the crew visualize the leak, but decides for something other than shutting down the unit

F03: the crew does not visualize the leak.

Step 3: Identification of Crew Failure Modes for CRT Branches and Development of Fault Trees

BP D is related to visualizing and responding to the leak. The CFMs related to this BP are in the Information phase of IDA. A reason the crew may not respond to the leak is a case

in which the field operator fails to correctly communicate the existence of the leak to the panel operator, which relates to the CFM “Information Miscommunicated” (I6). Also, the field operator may not visually check the status of the plant with the adequate frequency, which is linked to the CFM “Data not Checked with Appropriate Frequency” (I8), where the data would be the pipelines condition. Finally, the field operator may not pass by the leak and not visualize it. In this particular case, the leak is a key information on the status of the plant, and a failure in visualizing it is related to the CFM “Key Alarm/Information not Responded to” (I1). Figure 51, Figure 52 and Figure 53 show the FTs leading to these CFMs.

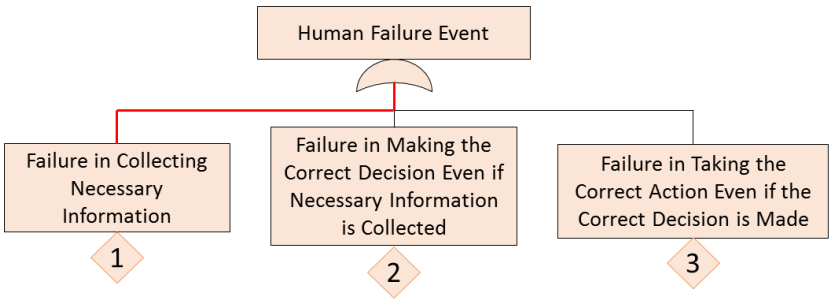


Figure 51: FT for BP D in Chevron Richmond accident Scenario - Part 1

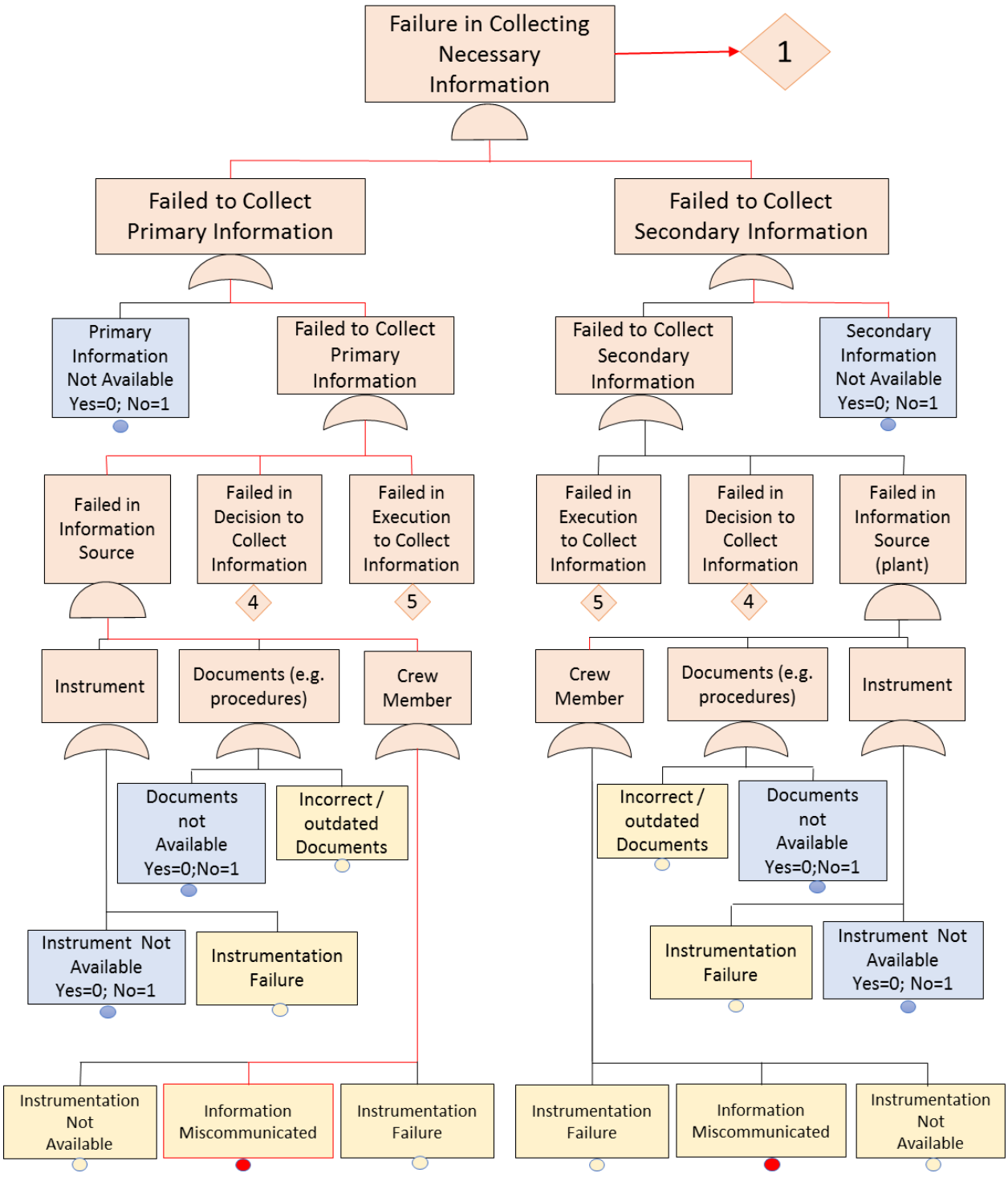


Figure 52: FT for BP D in Chevron Richmond accident Scenario - Part 2

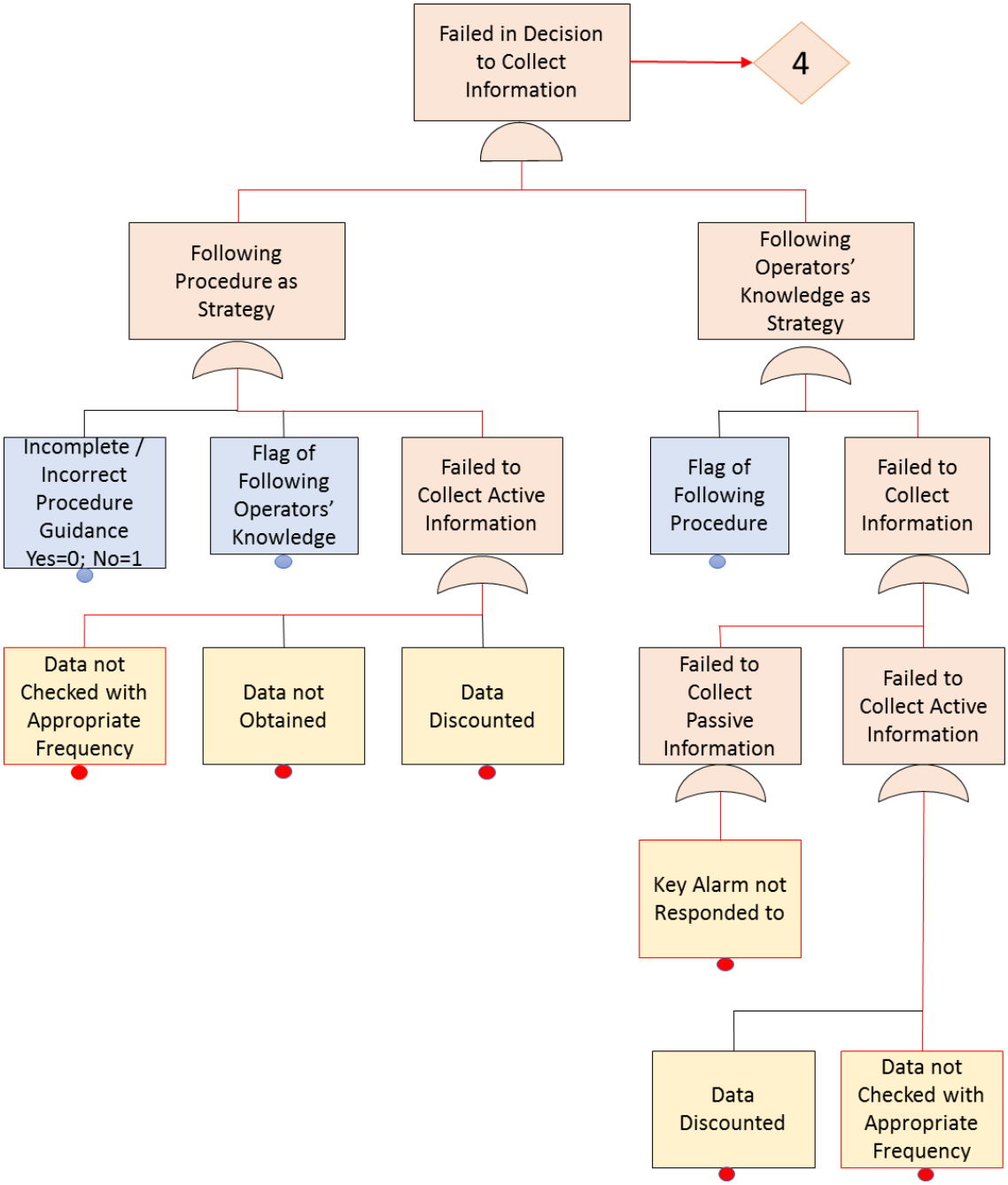


Figure 53: FT for BP D in Chevron Richmond accident Scenario - Part 3

Branch Point F is related to assessing the plant condition. Having visualized the leak, the crew would have to assess the situation accordingly and shut down the unit to fix the leak, repairing the pipe or replacing it, if necessary. A failure in correctly assessing the situation is related to the CFM "Plant/system state misdiagnosed" (D1), shown in the FTs in Figure 54 and Figure 55.

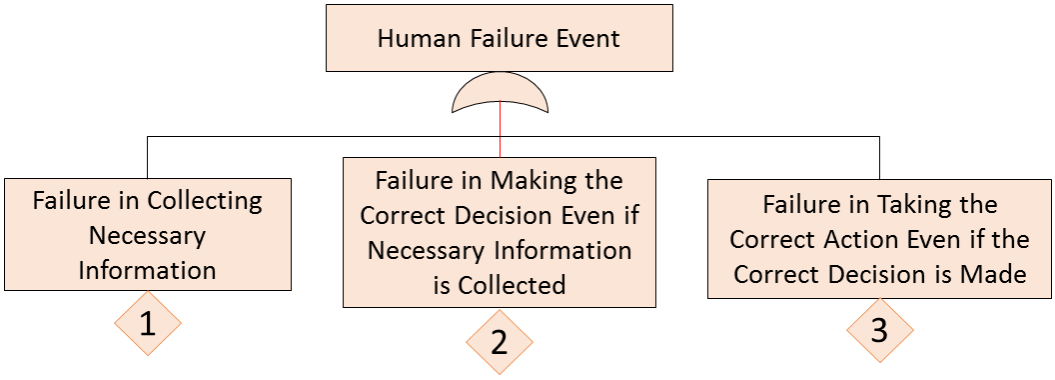


Figure 54: FT for BP E in Chevron Richmond accident Scenario - Part 1

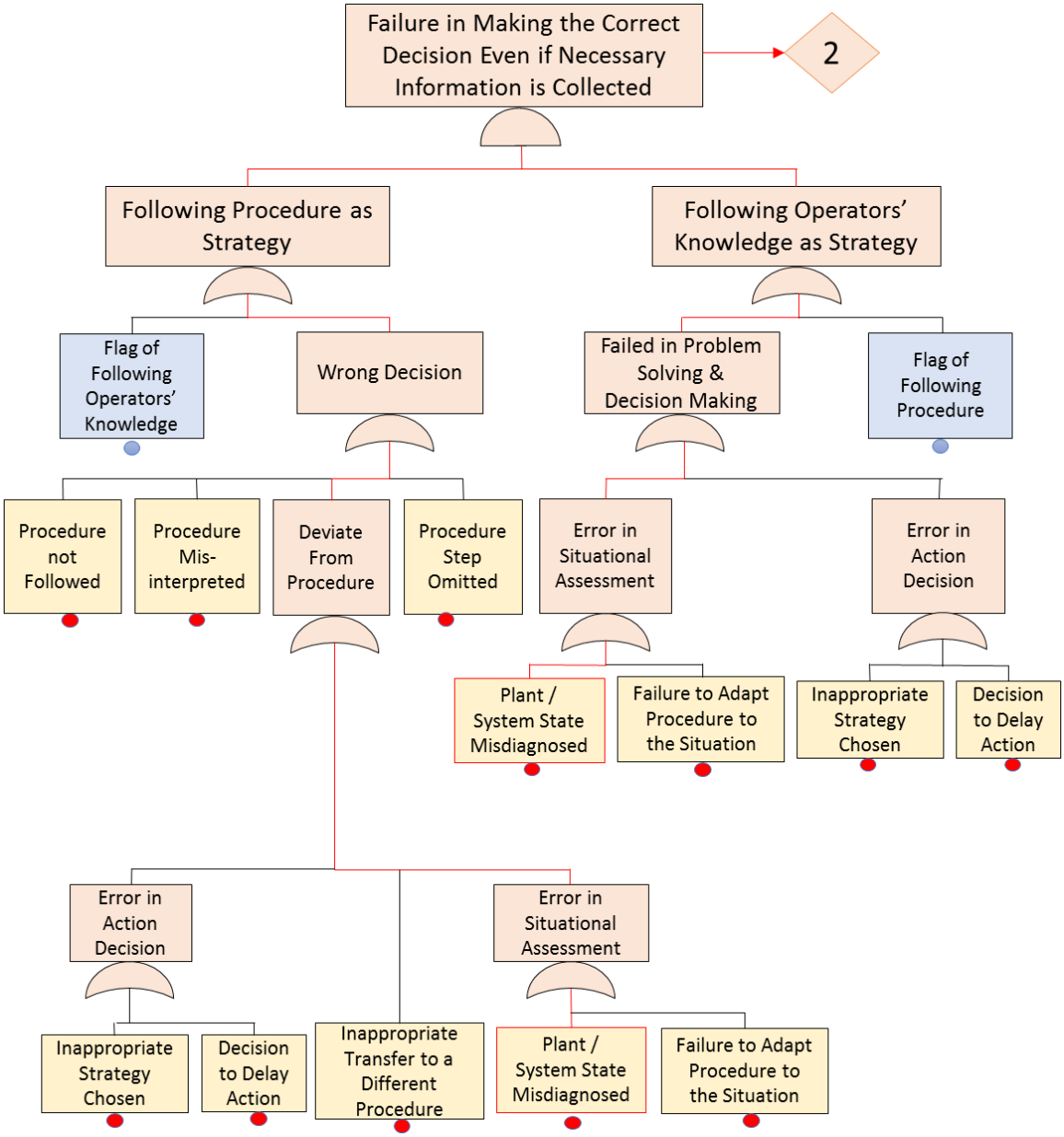


Figure 55: FT for BP E in Chevron Richmond accident Scenario - Part 2

Branch Point H is related to the action of shutting down the unit. A failure in it is in the "A" phase of IDA. A most relevant CFM for this action is related to the timing of the action, "Incorrect Timing of Action" (A1) (Figure 56 and Figure 57).

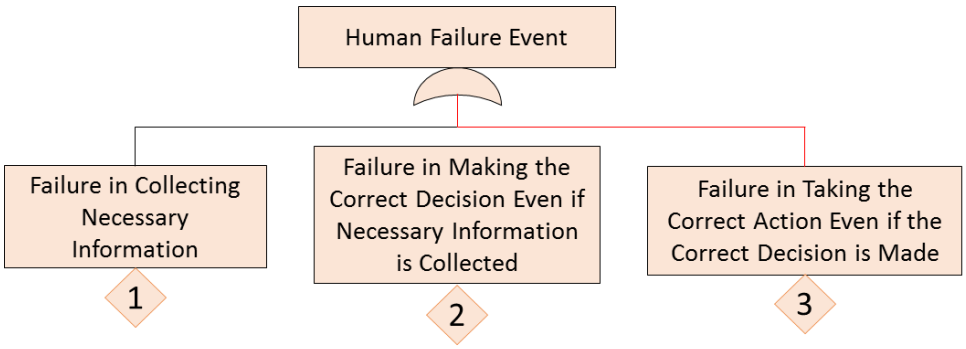


Figure 56: FT for BP H in Chevron Richmond accident Scenario - Part 1

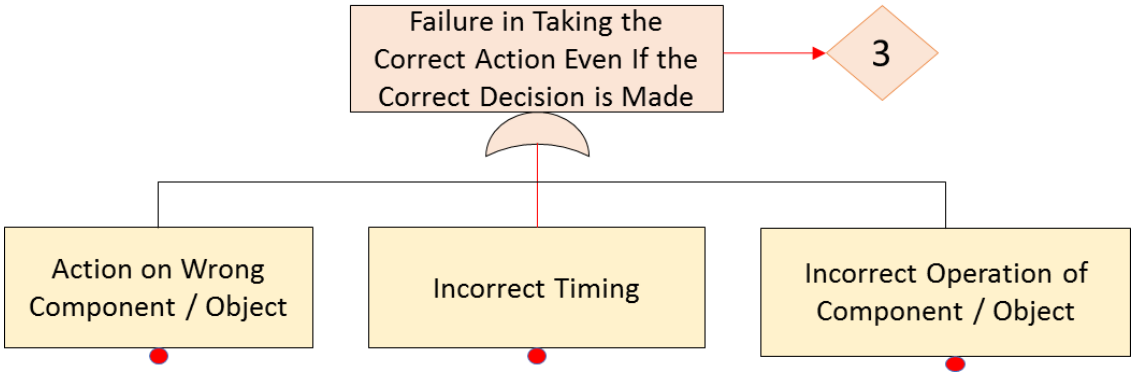


Figure 57: FT for BP H in Chevron Richmond accident Scenario - Part 2

Step 4: Identification of relevant PIFs for the CFMs and construction of BBN models

Table 17, Table 18, Table 19, Table 20 and Table 21 present the main PIFs for the CFMs of this scenario. The identification of these PIFs was made through a discussion with analysts and engineers and through extensive reading of the reports related to this accident - which have been summarized in Chapter 3.

Table 17: Main PIFs for CFM "Key Alarm/Information not Responded to" (BP D) Distillation Unit Scenario

Possible reasons for the crew not to visualize /respond to the leak	**HERO HRA Methodology corresponding PIFs**
Operator not attentive/tired	Attention
The operators are suffering from fatigue, for working too many days in a row	Fitness for Duty
Operator is not motivated or committed to the safety of the plant	Motivation/Commitment

Table 18: Main PIFs for CFM "Information Misscommunicated" (BP D) Distillation Unit Scenario

Possible reasons for the crew to have information miscommunicated	**HERO HRA Methodology corresponding PIFs**
There is no mean of communication between field operator and panel operator	Communication availabillity
The field operator fails to correctly communicate about the leak	Communication Quality

Table 19: Main PIFs for CFM "Data not Checked with Appropriated Frequency" (BP D) Distillation Unit Scenario

Possible reasons for the crew not to check the plant status with the appropriate frequency	**HERO HRA Methodology corresponding PIFs**
The procedure does not have clear instructions on how often the field operator have to check the unit status	Procedure Content
Operator is not motivated or committed to the safety of the plant	Motivation/ commitment

Table 20: Main PIFs for CFM "Plant/System State Misdiagnosed" (BP F) Distillation Unit Scenario

Possible reasons for the operators to misdiagnose the plant/system state	**HERO HRA Methodology corresponding PIFs**
The crew has no training in dealing with a leak on the pipes	Task Training
The crew has no knowledge the pipe may already be suffering corrosion	Knowledge of plant conditions
The operators do not know they all have the responsibility of deciding to shut down a unit when faced with an abnormal condition	Responsibility awareness

Tbale 20 – continuation

There is no leader in the team to conduct the assessment	Leadership
The crew has no operator specialist in this unit	Team Composition
The procedures don't instruct what should be done when there a leak in the pipes	Procedure content
The crew is divided between keeping the unit operating and shutting it down for safety	Competing goals
To identify the damage the pipe suffered to be presenting a leak is cognitive complex	Inherent Cognitive Complexity
The crew realizes they have to assess the situation quickly, since there is already hydrocarbon leaking	Stress due to perceived situation urgency
The crew get stressed because of the seriousness of the situation	Stress due to perceived situation severity
The crew get stressed because both decisions are difficult to make - to shut down the unit or to try to fix it while still running.	Stress due to decision

Table 21: Main PIFs for CFM "Incorrect Timing of Action" (BP H) - Distillation Unit Scenario

Possible reasons for the operators to not shut down the unit in time	**HERO HRA Methodology corresponding PIFs**
The crew has a communication problem on the decision about shutting down the unit, which delays the action	Communication Quality
The crew is also working on another unit	Extra work load
The panel interface is not clear	HMI input

Step 5: Model integration and analysis of HFE Scenarios, Development of Narratives, and Identification of Dependencies

By integrating the FTs to the CRT BPs, we have the CFM cut-sets for each of the outcomes of the CRT:

F01: A1

F02: D1

F03: I1+I6+I8

The narratives of each of these scenarios can be written as the following:

- The crew visualize and respond to the leak, correctly assess the situation but fail to shutting down the unit in time (A1 CFM)
- The crew visualize and respond to the leak but do not assess the situation correctly, and decide to fix the leak while the unit is still operating (D1 CFM)
- The field operator fail to visualize the leak (I1 CFM)
- The field operator fail to communicate the panel operator about the leak (I6)
- The field operator does not check the plant status with the appropriate frequency (I8)

In the actual case of the Chevron Richmond accident, the operators managed to visualize the leak. Yet, they failed to correctly assess the situation, which led to the scenario F02 because of the CFM D1

5.3 HERO HRA METHODOLOGY: HYDROTREATING UNIT SCENARIO

This scenario refers to a leak in a pipe of a Naphta Hydrotreating Unit, whose main function is to remove sulphur and nitrogen from naphta that is a product from the Distillation unit and Coker units. The main products are hydrotreated naphta, Sulphur and nitrogen. Equations 6 to 13 presents the mains reactions happening in the naphta hydrotreating unit.

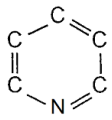
$$C-C-C-C-SH+H_2 \rightarrow C-C-C-C+H_2S \quad (6)$$

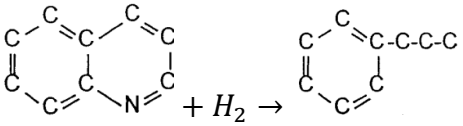
$$C-C-S-C-C+2H_2 \rightarrow 2C-C+H_2S \quad (7)$$

$$C-C-S-S-C-C+3H_2 \rightarrow 2C-C+H_2S \quad (8)$$


$+ 2H_2 \rightarrow C-C-C-C\left(and\ \text{C-C(C)-C}\right)+H_2S$ (9)

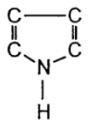

$+ 4H_2 \rightarrow C-C-C-C\left(and\ \text{C-C(C)-C}\right)+H_2S$ (10)


$+ 5H_2 \rightarrow C-C-C-C-C\left(and\ \text{C-C-C(C)-C}\right)+NH_3$ (11)



$$+ H_2 \rightarrow$$

$$+ NH_3 \quad (12)$$



$$+ 4H_2 \rightarrow C - C - C - C \left(and \right.$$

$$\left. \right) + NH_3 \quad (13)$$

This scenario was based in the QRA of the unit, and identified with severe consequences. However, this example aims to illustrate not only how to apply HRA to this scenario, but also to demonstrate the possibility of conjugating the HRA in a traditional QRA.

Indeed, as stated in Chapter 1, QRA is one of the main tools for risk management in the petroleum industry. Most of the standards and guidelines on QRA do not prescribe HRA nor provide guidelines on how HRA can be applied in a QRA, e.g. CETESB standard P 4.261 (CETESB, 2014), which provides the guidelines for QRA performed in Brazil. Moreover, this example also demonstrates how different level of knowledges on the factors, which, influence the human action, may strongly influence the individual risk results.

5.3.1 HRA scenario

Step 1: Scenario Development/Familiarization

The scenario consists of a rupture of the pipe exiting the recycle compressor suction drum V-06, as can be seen in Figure 58. This stream is rich in hydrogen and contains traces of naphta and hydrogen sulphide.

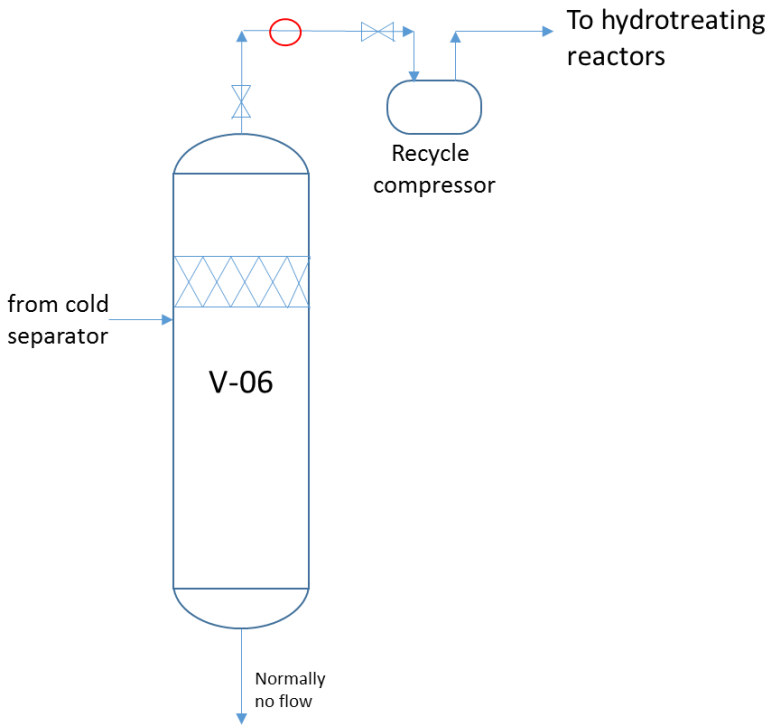


Figure 58: Hydrotreating Unit scenario leak location

The area around this drum, in the field, is equipped with an indicator of hydrogen presence – if there is a leak in this section, the indicator will activate an alarm, and the operator will then have to close the valves to isolate this pipe section and prevent more hydrogen to leak. This response is covered in the procedures. In case of failure of this alarm, other cues can be used by the crew to identify the leak, such as changes in pressure. However, the H2 presence alarm would be the cue that would lead the crew to an immediate response, not requiring an assessment of the situation, since there is a procedure indicating what to do in the case the alarm goes off. Therefore, as the only successful action in this scenario, we considered responding to the alarm, following procedure, and, finally, successfully closing the valves, thus isolating the leak.

Step 2: Development of Crew Response Tree

Table 22 and Table 23 present the answers for the CRT construction questions and for the description of the BPs. The CRT for this scenario is presented in Figure 59.

Table 22: Flowchart questions and answers for Hydrotreating Unit scenario

No.	Question	Answer
1	Is the specific function designed to be initiated automatically?	No. Go to Question 2.
2	Are there available instruments to indicate relevant process conditions to the operators?	Yes. There is a H2 indicator
3	Are there other other cues the operators can use to assess the situation?	No.
4	Are there procedures instructing the manual activation of the safety function?	Yes.
5	Are there other resources the operators could use to manually activate the safety function?	No.
6	Are there additional equipment and manual actions that could be used to provide the specific safety function?	No.

Table 23: Description of Branch Points of Hydrotreating Unit scenario

BP	Description	Application on CRT
A	NA	NA
B	NA	NA
C	The key instrument is the level indicator alarm	Success path: H2 presence alarm goes off Failure path: H2 presence alarm fails
D	Operators can respond to the alarms or not	Success path: Operators respond to the alarm Failure path: operators fail to respond to the alarm
E	The procedure indicates that the response for this alarm is to close the valves	Success path: Operators follow procedure Failure path: operators don’t follow procedure
F	NA	NA
G	Safety function is not impaired by equipment (hardware / system) failure.	This BP is ignored because of the low probability of this event. Therefore this BP is not created
H	After correctly assessing the situation, the operators can successfully close the valves	Success path: Operators successfully close the valves. Failure path: Operators fail to close the valve.

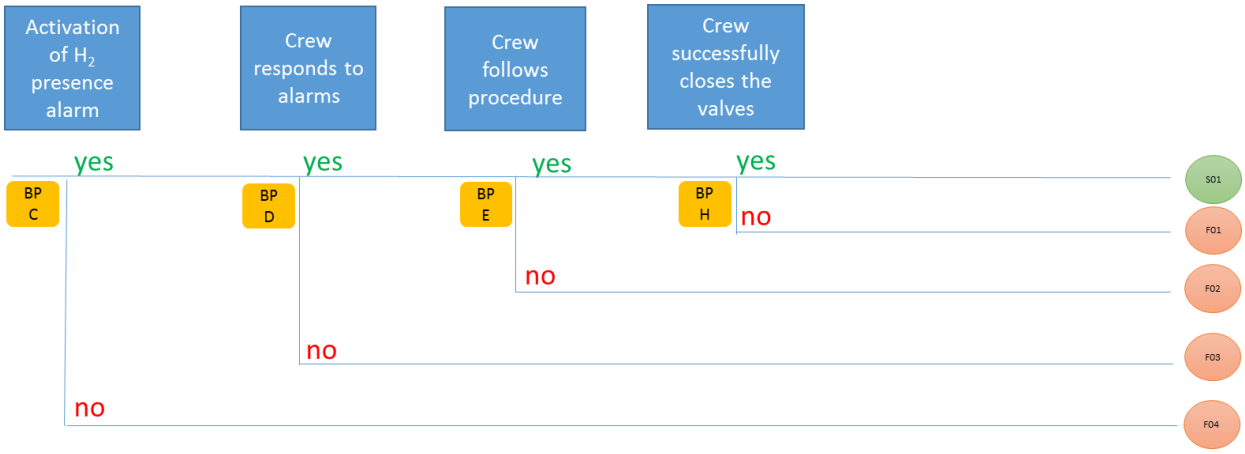


Figure 59: CRT for Hydrotreating Unit scenario

Step 3: Identification of Crew Failure Modes for CRT Branches and Development of Fault Trees

BP D is related to responding to the H_2 presence alarm, in which a failure is represented by the CFM "key alarm/plant information not responded to" (I1).

Given that the crew noticed the alarm and decided to respond to it, they may follow the procedures, which indicate that the valves isolating this pipe section must be closed, or may not follow the procedures (BP E). The CFM indicating a failure in this action is "procedure not followed" (D5)**.**

BP H refers to a failure in closing the valves, even after taking the correct decision (following procedure) to do it. A major reason for failure in closing the valves in this case is failing to so on time, represented by the CFM "incorrect timing of action" (A1)

The FTs leading to these CFMs is presented in Appendix B.

Step 4: Identification of relevant PIFs for the CFMs and construction of BBN models

The possible reasons that could lead the operator to the CFMs were identified through discussions with operators and engineers, and are presented in Table 24, Table 25 and Table 26.

Table 24: Main PIFs for CFM "Key Alarm not Responded to" (BP D) Hydrotreating unit scenario

Possible reasons for the operators not to respond to the alarms	**HERO HRA Methodology corresponding PIFs**
Too many alarms at the environment at the same time	Passive Information Load
Inadequate panel interface	HMI Output
Operator not attentive/tired	Attention
Operators working also on another unit	Extra work load
Too much ambient noise	Workplace Adequacy
Operator absent at the moment	Motivation/Commitment
Operator believes the H_2 indicator may be incorrect	Confidence in Instruments

Table 25: Main PIFs for CFM "Procedure not followed" (BP E) Hydrotreating unit scenario

Possible reasons for the operators not to follow procedures	**HERO HRA Methodology corresponding PIFs**
The crew is mislead for believing this pipe section is in perfect state	Knowledge of plant conditions
The procedure is not clear about the crew response to the alarms	Procedure content
Operator believes the H_2 indicator may be incorrect	Confidence in Instruments

Table 26: Main PIFs for CFM "Incorrect timing of action" (BP H) Hydrotreating unit scenario

Possible reasons for the operators to perform action in incorrect timing	**HERO HRA Methodology corresponding PIFs**
It is not clear which operator should do it	Responsibility Awareness
Operators working also on another unit or other section of this unit	Extra Work Load

Step 5: Model integration and analysis of HFE Scenarios, Development of Narratives, and Identification of Dependencies

When we integrate the FTs (Appendix B) to the respective BPs in the CRT (Figure 59), it is possible to obtain the CFM cut-sets for the HFE scenario of interest. The HFEs scenarios can be identified as one of the outcomes in the CRT (F01, F02, F03, F04). For each of the outcomes, the CFM cut-sets are:

F01: A1

F02: D5

F03: I1

All of these HFEs scenarios contribute to the final HFE, namely: failure to close the valves isolating the leak. The narratives, therefore, can be written as:

- The crew respond to the H_2 presence alarm and follow procedure that indicate to close the valves, but fail to close the valves in correct timing (A1 CFM)
- The crew respond to the H_2 presence alarm, but do not follow procedure (D5 Cfm)
- The crew do not respond to H_2 presence alarm (I1 CFM).

In short, it is noticeable that these CFMs were enhanced by the factors listed in Table 24, Table 25 and Table 26.

5.3.2 Quantitative Risk Analysis

For a hydrotreating unit scenario, the HRA was linked to a quantitative risk analysis to 1) suggest a possibility on how to use HRA in a traditional QRA and 2) to illustrate how the human performance can have a considerable effect on the final risk of a scenario. The QRA was performed following CETESB standards (CETESB, 2014), which are the ones followed for QRAs in Brazil. The QRA in question was made of a consequence analysis, a frequency analysis, and the risk calculation. The human actions, in this scenario, will affect the frequency of the event. This will be further explained Subsection 5.3.2.2.

Since there are no data to quantify the BBN generated by the CFMs and the PIFs of HERO HRA Methodology, the frequency analysis made use of the data provided by the Phoenix methodology. The available data, however, are still limited. We decided then to make use of the joint conditional probabilities of the CFMs given two PIFs states – degraded and nominal, which are available in Nsima (2013). The results cover then two extreme situations: one in which the PIFs are all nominal, which is the best-case scenario, and one in which the PIFs are all degraded, which is the worst-case scenario. Moreover, such probabilities consider not only the relevant PIFs identified in the section above, but all PIFs. It should be noticed that, rather than providing a quantitative example of HRA, our aim is to illustrate how HRA can be put together into a QRA as well as the effect human performance can have on the risk

of a scenario. The following subsections describe the consequence analysis, the frequency analysis with the HRA, and, finally the risk analysis.

5.3.2.1 Consequence Analysis

The scenario consists of a leak of a stream consisting of mainly hydrogen, with traces of naphta and hydrogen sulphide. Since the hydrogen is the main component, it was adopted as the representative substance in the simulation.

A leak of hydrogen can have the following consequences:

- Jet fire, if there is immediate ignition
- Cloud fire, if there is no immediate ignition and there is a late ignition
- Explosion, if there are conditions for explosion (confinement of the cloud) and late ignition

For the consequence analysis, the following values were used:

- Closing time of the blocking valves: a remote-controlled blocking system was considered, i.e., a system where the detection of the leakage is fully automatic. The detection results in a signal in the control room. The operator validates the signal and closes the blocking valves using a switch in the control room. In this system, according to the Purple Book of TNO (TNO, 2005), the closing time of the blocking valves is ten minutes.
- The simulation was performed for day and night periods. The meteorological conditions considered were the ones from the SUAPE region in Pernambuco, Brazil, a technological complex that comprises petrochemical companies and oil refinery.
- The vulnerability contours considered are the ones used in QRAs in Brazil, following the CETESB standard. Table 27 shows the values considered for cloud fire and explosion.

Table 27: Vulnerability contours adopted for Cloud Fire and Explosion

Consequence	**Contour**	**Vulnerability**
Cloud Fire	Lower Flamability Limit	100%
Overpressure (explosion)	>0,3bar	75%
	Between 0,1 and 0,3 bar	25%

For thermic radiation (pool fire and jet fire), CETESB indicates that 35kW/m^2 corresponds to 100% probability of fatality. For a radiation lower than this value, the Probit equation must be used:

$$\Pr = a + b.\ln(I^n.t)$$

with a= -36.38; b=2.56, n=4/3 and the time of exposure t = 20s (CETESB, 2014).

The process parameters were based on a real Hydrotreating unit (Table 28)

Table 28: Process conditions

Parameter	**Value**
Temperature (^{o}C)	55
Pressure (atm)	25
Vessel volume (m^3)	10
Pipeline dimeter (inch)	12
Pipeline length (m)	100

The simulations were performed in the software EFFECTS, v8.1.8, and the results are presented in Table 29.

Table 29: Consequence Analysis results

Consequence	**Contour**	**Vulnerability**	**Distance (m)**	
			Day	**Night**
Cloud Fire	**LFL**	**100%**	868.92	1208.21
Explosion	**0.3bar**	**75%**	406.69	388.91
	0.1bar	**25%**	162.16	153.93
Jet fire	**9.85kW/m^2**	**1%**	148.80	164.00
	19.5kW/m^2	**50%**	138.67	153.23
	35kW/m^2	**100%**	132.34	146.27

5.3.2.2 Frequency Analysis with HRA

The frequency analysis of the scenario is the second step of the QRA. In regular QRA, with no consideration of HRA, the frequency analysis entails the identification of the frequency of the initial event and the probabilities of each of the consequences. In this scenario, thus, we have to identify the frequency of a rupture of the pipe, which is the initial

event, and the frequencies of having a jet fire, cloud fire and explosion – which depends on the probabilities of having early and late ignition and conditions for explosion.

The frequency of the pipe rupture can be found in generic reliability databases, such as OREDA (Offshore Reliability Data), EiREDA (European Industry Reliability Data Bank), Concawe database (Environmental Science for the European Refining Industry), TNO Purple Book. For this study we adopted the TNO Purple Book (TNO, 2005) database, which provides a yearly frequency of Loss of Containment (LOCs) through pipes, given as function of the pipes length and of the pipe diameter. The LOCs for pipes cover all types of process pipes and inter-unit pipelines above ground of an establishment. For the pipe analyzed in this scenario, which has a diameter larger than 150mm, TNO Purple Book defines that the frequency of a full-bore rupture is $1x10^{-7}$ $m^{-1}y^{-1}$. For a 100m pipe, the frequency of the initial event f_{ie} is then $1x10^{-5}$ y^{-1}.

The event tree of this scenario, not considering the HRA, can be seen in Figure 60. The source for the probabilities for immediate ignition (iip), late ignition (lip) and condition for explosion (cep) is CETESB (2014). For late ignition, we considered few ignition sources in the area.

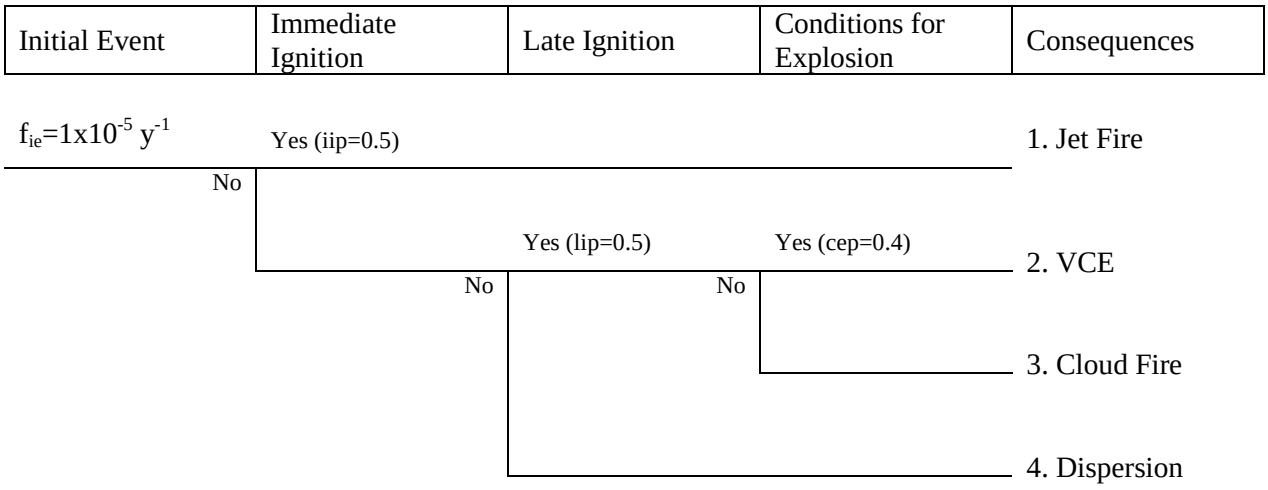


Figure 60: Event tree for Hydrotreating Unit Scenario with no consideration of HRA

The frequency of a jet fire is then $f_{ie} \times iip$; of having a Vapor Cloud Explosion is $f_{ie} \times (1 - iip) \times lip \times cep$ and a cloud fire is $f_{ie} \times (1 - iip) \times lip \times (1 - cep)$. These frequencies are shown in Table 30.

Table 30: Frequencies for Hydrotreating Unit Scenario with no consideration of HRA

Consequence	**Frequency (year^{-1})**
Jet Fire	$5x10^{-6}$
Vapor Cloud Explosion	$1x10^{-6}$
Cloud Fire	$1.5x10^{-6}$

Note that the event tree of Figure 60 and its resulting frequencies are obtained with a traditional QRA, with no consideration of human actions. It thus considers that, when there is a rupture of the pipe, the possible outcomes are a jet fire, an explosion, a cloud fire, or the dispersion of the cloud. However, another possible outcome is that the operators would notice the pipe rupture and act on it, closing the valves before a large amount of gas leaks. The human actions, in this case, will then serve as a barrier – they can prevent the formation of the cloud and avoid a cloud fire and a vapor cloud explosion (considering that the amount of gas leaked before the crew actions will be small enough to disperse with no cloud fire or explosion).

Given that for the jet fire to occur, only an immediate ignition source is needed, we consider that in this case the operators could not prevent its occurrence (they can, however, shorten its duration, when closing the valves). The cloud fire and explosion will, therefore, happen if the crew *fail* to act on achieving the safety function – which is closing the valves to stop the hydrogen to leak. This can thus be added to the event tree (Figure 61).

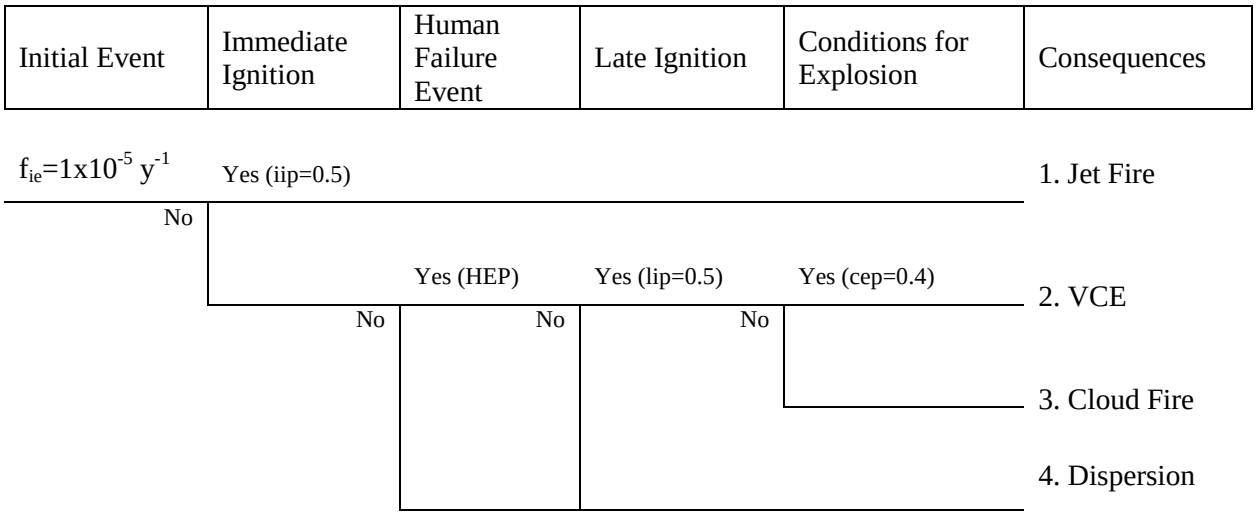


Figure 61 Event tree for Hydrotreating Unit Scenario with consideration of HRA

Considering the crew actions, the frequency of having a VCE is now $f_{ie} \times (1 - iip) \times HEP \times lip \times cep$ and a cloud fire is $f_{ie} \times (1 - iip) \times HEP \times lip \times (1 - cep)$.

Going back to the CRT of this scenario, presented in Figure 59, the crew will fail if they: do not respond to the alarm (I1 CFM) OR do not follow procedure (D5 CFM) OR fail to act in the correct timing (A1 CFM). I1, D5 and A1 are the cut-sets for this Human Failure Event.

The Human Error Probability is then given by:

$$HEP = P(I1) + P(D5) + P(A1) \quad (14)$$

However, we do not have the data to calculate the probabilities of these CFMs given its relevant PIFs. Ekanem (2013) provides joint conditional probabilities for Phoenix CFMs given three states of the PIFs: degraded, midway and nominal. These probabilities consider all PIFs and not only the ones relevant to this scenario; and they are based on Phoenix CFMs and PIFs rather than HERO HRA Methodology set of CFMs and PIFs. Yet, in order to illustrate this example, we will use the joint conditional probabilities for the CFMs provides by Ekanem (2013) given two states of the PIFs: degraded and nominal. Therefore, we consider two scenarios: a best-case scenario, in which all PIFs are nominals, i.e., all factors affect the human actions by enhancing it; and a worst-case scenario, in which all PIFs are degraded, i.e., all factors affect the operators by increasing their probability of error.

Moreover, since Phoenix does not have the CFM "procedure not followed", we will instead use the probability of its CFM "Failure to adapt procedure to the situation". Table 31 presents the probabilities for these CFMs.

Table 31: Joint Conditional probabilities of CFMs given PIFs (EKANEM, 2013)

CFM	PIFs states	
	Degraded	Nominal
Key alarm not responded to	1.65E-04	4.24E-06
Failure to adapt procedure to the situation	1.81E-02	4.68E-04
Incorrect timing of action	1.72E-02	2.85E-04

Given Equation 14, thus, we have $HEP_{degraded} = 3.55E^{-2}$ and $HEP_{nominal} = 7.57E^{-4}$.

The frequency of the consequences considering the possibility of the crew acting on the leak are presented in Table 32. These frequencies, combined with the consequence analysis results, were used to calculate the individual risk of this scenario, presented in next subsection.

Table 32: Frequencies for Hydrotreating Unit Scenario with consideration of HRA - for worst and best case scenario

Consequence	**Frequency (year^{-1})**	
	Worst case scenario (Degraded PIFs)	**Best Case Scenario (Nominal PIFs)**
Jet Fire	$5x10^{-6}$	$5x10^{-6}$
Vapor Cloud Explosion	$3.55x10^{-8}$	$7.57x10^{-10}$
Cloud Fire	$5.32x10^{-8}$	$1.14x10^{-9}$

5.3.2.3 Risk Analysis

In order to analyze the effect the HRA can have on the final risk, we used Individual Risk, which represents the frequency of an individual dying due an accidental scenario. Details on the calculation of individual risk can be seen in TNO Purple Book (TNO, 2005). The Risk Analysis was performed using the software RiskCurves v7.7.9. The individual risk was calculated for the two scenarios of Table 33– worst- and best-case scenario. Thus, the distances for vulnerabilities presented in Table 29 remain the same, and the frequencies changed from one scenario to another.

Figure 62 and Figure 63 present the individual risk for the worst-case scenario (degraded PIFs) and for the best-case scenario (nominal PIFs).

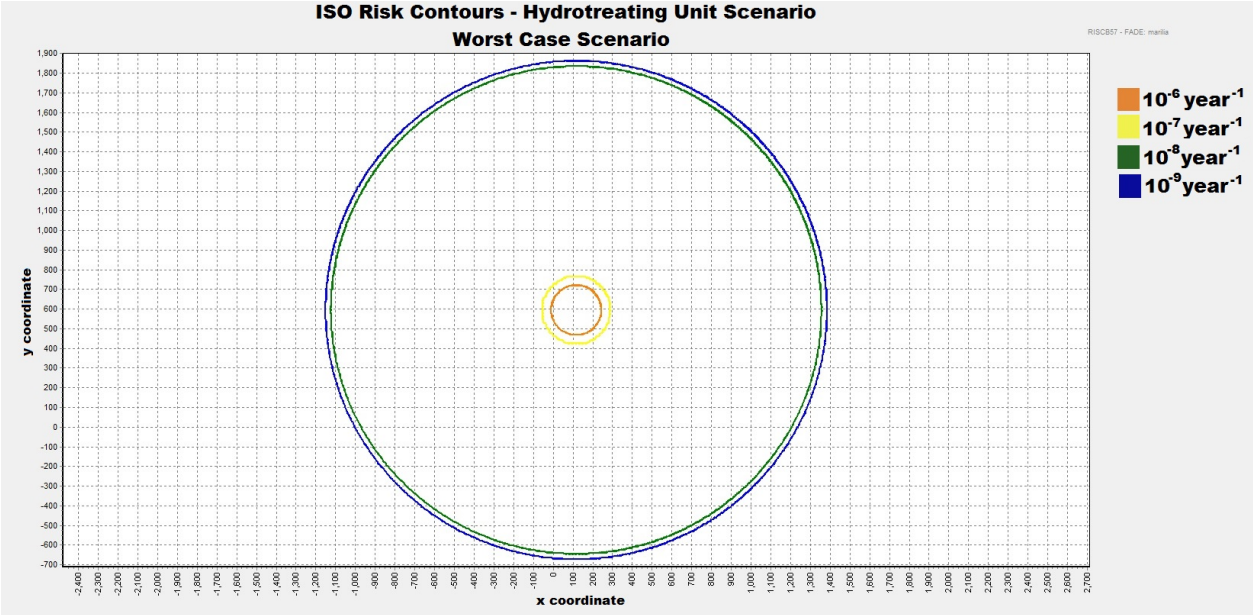


Figure 62: Individual Risk for Hydrotreating Unit Scenario considering HRA - Worst Case Scenario

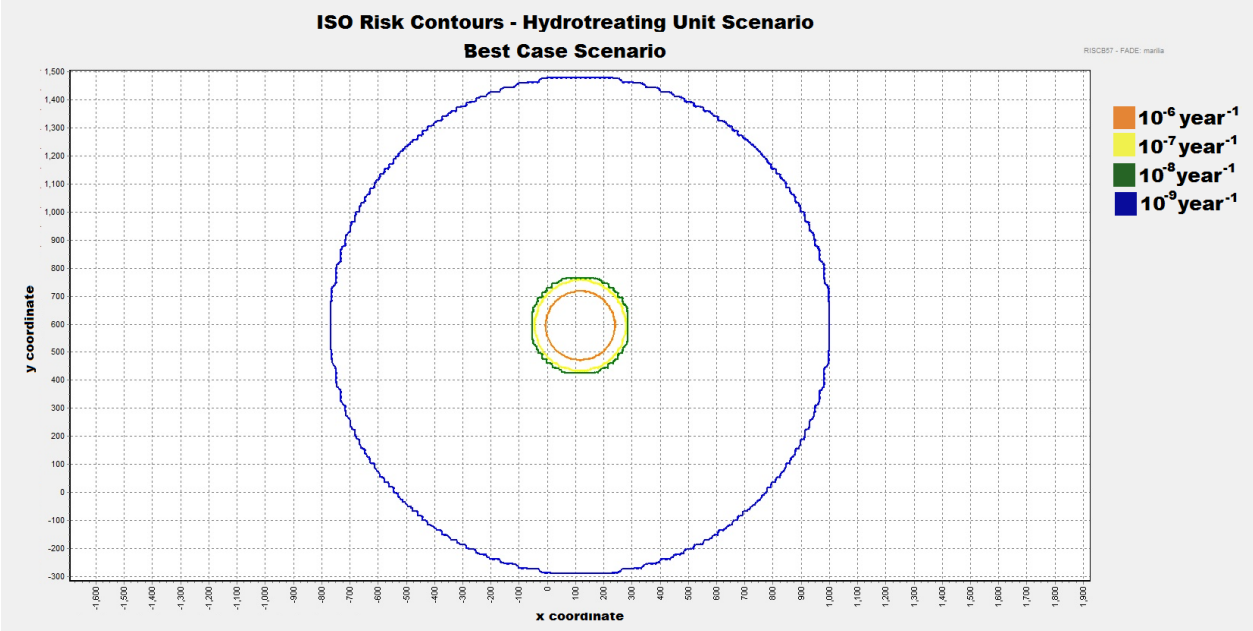


Figure 63: Individual Risk for Hydrotreating Unit Scenario considering HRA - Best Case Scenario

Table 33: Radius for Individual Risk of Hydrotreating Unit Scenario considering HRA

Individual Risk ($year^{-1}$)	Radius (m)	
	Worst Case Scenario	Best Case Scenario
10^{-9}	1274.15	889.2
10^{-8}	1238.5	169.85
10^{-7}	178.3	164.1
10^{-6}	126	63

As expected, the best-case scenario presents radius for individual risks considerably smaller than the worst-case scenario.

CETESB standard stablishes the following risk regions:

- Tolerable: $RI < 1 \times 10^{-6} year^{-1}$
- ALARP[16]: $1 \times 10^{-6} year^{-1} \leq RI \leq 1 \times 10^{-5} year^{-1}$
- Intolerable: $RI > 1 \times 10^{-5} year^{-1}$

The risk that may occur in this scenario would fall into the ALARP zone since it may reach 10^{-6} $year^{-1}$. When this risk level is inside the installation, CETESB indicates that it would be a residual risk that must be managed with a Risk Management Program. If it reaches zones out of the installations, however, the industry must implement measures that would reduce such risk. Depending on the location of the leak in the installation, having the best- or worst- HRA case scenario could mean managing the risk or having to present changes in the process in order to reduce the consequences or the frequencies of the accident.

In this sense, having the PIFs in a nominal or degraded level can have a big considerable difference on the risk. If the factors that influence the operators' actions are appropriate, there is a higher probability of the operators to successfully deal with a situation, to respond correctly and in time, and to prevent a serious accident. Adequate actions include following available procedures, an appropriate work load, a good Human Machine Interface, attentiveness from operators, and others. When there is enough data to populate the BBN, we can then quantitatively identify the factors that would have a larger influence on the operators' actions in a specific scenario; the industry can then take risk-based decisions to have a safer environment.

[16] As Low As Reasonably Practicable - measures must be taken to reduce the risk

In addition, the example we examined and provided presents an effective way to conjugate HRA to a traditional QRA as it is applied today in oil refineries and petrochemical plant operations. This case study showed a scenario in which the operators' actions would function as a barrier, reducing the risk and being able to prevent an accident. Yet, it is important to note that the operators' actions can also worsen an accident, or even initiate one. The BP Texas City Refinery accident, presented in Chapter 3 is an example of that: the operators started the unit with a valve closed, and with the tower level higher than it should be. The Chevron Richmond Refinery accident, on the other hand, presents a scenario where the crew worsened the accident since they decided for an aggressive strategy to deal with the leak and thus contributed to transform a small leak into a rupture.

The HERO HRA Methodology in short, is capable of modeling all these types of operators' interactions with an accident, and it can be conjugated to a traditional QRA with no efforts, as shown through this example.

CHAPTER 6 – HRA FOR OIL AND GAS: FINAL CONSIDERATIONS

As was mentioned in Chapter 1 of this thesis, both petroleum refining installations and petrochemical plants pose safety problems. This cannot be changed since toxic and flammable fluids are part of everyday work in such installations. A large part of accidents that occur within these installations, however, could be prevented: human error, as has been argued throughout the chapters of this thesis, has been responsible for a significant number of accidents. This thesis aimed to advance our knowledge on how human error can be prevented in the specific context of oil refineries and petrochemical plants.

HRA has been essential in developing effective forms to reduce the possibility of accidents causes by human behavior. In this sense, in the last decades, it was crucial in making it possible for the human contribution to risk to be assessed. Several HRA methods have been developed since the first one, which dates back to 1952. Nonetheless, HRA was first developed for nuclear plants, being a new concept when it comes to the two contexts abovementioned. The lack of a methodology developed specially for Oil and Gas can be considered to be a consequence of the scarcity of studies on human error and HRA applied to the field; it is also the reason for the lack of practical tasks related to them in the analyses on the risks of a facility.

In this thesis, I thus put our efforts toward creating a new HRA methodology designed specifically for oil refineries and petrochemical plants. In order to do so, I considered elements that are easily relatable to operations that are part of such installations with the purpose of accurately reflecting the specificities of this industry. It was also important for the new methodology to have a strong qualitative and quantitative basis, so it could overcome the well-known deficiencies of most existing HRA methodologies. Hence, the new methodology - HERO HRA Methodology - was built on the foundations laid out by the Phoenix Methodology, which combines the benefits of the existing and emerging HRA methods.

Phoenix was, however, developed for nuclear plants operations, as has been the case for the majority of the HRA methodologies. Yet, I decided to take advantage of the strengths of Phoenix while adapting its elements, its definitions and its terms to the oil refineries and petrochemical plants operation scenarios. This made it possible to develop a model-based method specifically for this sector. The HERO HRA Methodology is thus extremely relatable to oil refinery operations: it reflects the possible interactions between the crew and the plant,

the possible errors the operators can make, and the factors that influence the crew to follow a path that would bring the plant back to safety/maintain the plan in safety, or a path that would lead to an accident such as an explosion, a fire, a toxic cloud.

Given that having a solid qualitative analysis when performing an HRA is of great relevance, as pointed out by Taylor (2014), this thesis explored the qualitative aspects of HERO HRA Methodology. This thesis thus focused on HERO structure, with three layers, and its elements: the crew response tree, the crew failure modes, and the performance influencing factors. I presented a flowchart that could represent all interactions between the crew and the plant in order to build a solid CRT. I also introduced a set of CFMs, which aims to represent any error the crew could make, and I developed on how these CFMs apply to a refinery context. In addition, I presented a set of PIFs, and demonstrated, with examples from oil refinery operations, their importance and applicability in an oil refinery operation context.

To develop the elements abovementioned, I made use of detailed past oil refinery accidents reports, of visitations of a refinery control room and meetings with its operators and supervisors; I also interviewed HRA specialists. These helped us develop our step-by-step guide on how to apply HERO HRA Methodology. I then illustrated these steps by making use of three examples: a potential scenario within the Hydrogen Generation Unit, a scenario based on the Chevron Richmond refinery accident in 2012, and a potential scenario with the Hydrotreating Unit.

The following sections will explain the final considerations of this thesis. I will first explain in Section 6.1 the main research contributions. In Section 6.2 I will outline the main challenges I faced in developing the new methodology. These will include the expected ones as well as the ones that occurred along the way. I will also explain how they have been overcome in creating a solid robust methodology. Finally, I will provide potential ideas for future work.

It is important to notice that the motivation for working with Risk Analysis and Reliability is always to guarantee an operation can be performed in safety; in this sense, I expect that the development of HERO HRA Methodology and this thesis overall can help improving the safety within petroleum industries and allow for stronger risk-informed decisions. HERO is a methodology ready to use, and can be applied to scenarios of interest in order to identify how operators can fail and why.

6.1 RESEARCH CONTRIBUTIONS

This research main contribution is the development of an HRA methodology specific for oil refineries and petrochemical plants operations; being the first methodology built in this direction. To develop this methodology, however, I followed some steps that have become research contributions as well. These are outlined below:

- The analysis of four past accidents in oil refineries, selected by their importance in terms of consequences and by the availability of detailed reports of the crew actions. Such analysis demonstrates that human error was strongly present in these accidents and may serve as reference for future studies in the area.
- Besides making use of existing HRA methodologies, this thesis also draws on interviews with HRA specialists about the applicability on CFMs and PIFs in oil refinery operations. This brought a greater integration between qualitative studies, existing methodologies, and practical feedback from those that are part of everyday operations in oil and gas facilities.
- A flowchart for the construction of the CRT, which represents the interactions between the crew and an oil refinery or petrochemical plant.
- I also provide a set of CFMs that is specific to the operators working in an oil refinery and petrochemical plants, with definitions easily relatable to oil refinery operations.
- In addition, I propose a set of PIFs that reflects the conditions of the work in an oil refinery. These three elements can be used in future studies both for the development of other methodologies as for qualitative studies in the area.
- Finally, the creation of an enhanced Phoenix's set of FTs, which was done by improving its overall structure to include the CFMs proposed for use in this methodology.

6.2 CHALLENGES

Although some challenges were anticipated, the process of developing this new methodology proved to be more challenging than expected. The main ones relied specially on the following:

- The scarcity of accidents' investigation reports that detail the operators' actions during the accident. Even though the Chemical Safety Board (CSB) of the U.S. elaborates public investigation on large accidents – which is the reason the accident analysis

focused on accidents that happened in the United States – it only provides three reports on accidents with a not-more-than-enough level of details. The Environmental Protection Agency (EPA) provided one more, which completed the four accidents analyzed in the thesis. Having access to a larger number of reports would have allowed us to detail more crew actions and influencing factors during past accidents, and this would have allowed us to have even more solid sets of CFMs and PIFs;

- The difficulties in finding available specialists on HRA and oil refinery operations. This challenge was expected given than HRA applied to oil refinery operations have not been widely explored until the present moment. I contacted 23 experts from different countries, such as Sweden, Norway, the United States, Brazil, and Italy. Some of them, despite being experts on HRA, declared themselves as having not sufficient expertise with regard to HRA applied to oil refineries and petrochemicals. Hence, I gathered the opinions and feedback of eight of them. These are highly trained specialists and extremely experimented in the issue, having between five and forty years of experience;
- The difficulty in having access to operators and engineers of refineries control room. Two oil refining companies were contacted, one in the United States and one in Brazil, to provide access to operators and engineers for formal interviews, and some barriers in the way made it impossible to happen. However, it was possible to have informal conversations with them, which enlightened possible crew actions and influencing factors.

Having a larger number of investigation reports, more specialists for interview, and formal access to control room operators would have allowed expanding this work. Nonetheless, I strongly believe that these challenges were overcome in this thesis. The use of the available reports combined with the interviews, the visitations of a control room, and informal conversation with operators, and a comparison between NPP and oil refineries control room/operations made it possible to develop a strong basis for the methodology.

6.3 FUTURE WORKS

I expect that HERO HRA Methodology will be used in oil refineries and petrochemical plants. For future work on the methodology itself, I believe that it can be further improved by:

- Validating the set of CFMs and PIFs with refinery and petrochemical operators;
- Enhancing the set of CFMs and PIFs with analysis of a larger number of past accidents;
- Applying the methodology to a larger number of scenarios, in order to reassure that the CFMs and PIFs set cover all failure modes and influencing factors that can happen in oil refineries and petrochemical plants;
- Having experienced risk analysts to apply the methodology within accidental scenarios in order to reassure the definitions of the CFMs and PIFs are easily relatable;
- Analyzing other possible ways to conjugate HRA into a QRA;
- Having data from oil refineries and petrochemical plants operation for populating the BBN and thus allow for quantification of HFEs using specific data.

REREFENCES

ARDAKANI, M.; ZARE, M,; MAHDAVI, S.; GHEZAVATI, M.; FALLAH, M,; HALVANI, G.; GHANIZADEH, S.; BAGHERAAT, A. Relation between job stress dimensions and job satisfaction in workers of a refinery control room. **Journal of Community Health Research**. 2013

BELL, J.; HOLROYD, J. Review of human reliability assessment methods. **HSE Books** - RR679 Research Report. 2009

BORING, R. Adapting Human Reliability Analysis from nuclear power to oil and gas applications. **Safety and Reliability of Complex Engineered Systems** – Podofillini et al. (Eds)© Taylor & Francis Group, London, ISBN 978-1-138-02879-1. 2015

BORING, R. Fifty years of THERP and Human Reliability Analysis. **Proceedings of Probabilistic Safety Assessment and Management (PSAM 11).** June 2012

BORING, R. Human Reliability Analysis in cognitive engineering. **Frontiers of Engineering: Reports on Leading-Edge Engineering from the 2008 Symposium.** National Academy of Engineering. 2009

BORING, R.; OIE, K. Defining Human Failure Events for Petroleum Risk Analysis. **Probabilistic Safety Assessment and Management PSAM 12**. Honolulu, Howaiii, June 2014

BRANSBY, J.; JENKISON, J. Alarm management in the chemical and power industries-a survey for the HSE). **IEE Colloquium on Stemming the Alarm Flood** (Digest No: 1997/136). 1997

CHANG, Y.; MOSLEH, A (a). Cognitive modeling and dynamic probabilistic simulation of operating crew response to complex system accidents - part 1. Overview of IDAC model. **Reliability Engineering and System Safety**. 2006

CHANG, Y.; MOSLEH, A (c). Cognitive modeling and dynamic probabilistic simulation of operating crew response to complex system accidents - part 3. IDAC operator response model. **Reliability Engineering and System Safety**. 2006

CHANG, Y.; MOSLEH, A (d). Cognitive modeling and dynamic probabilistic simulation of operating crew response to complex system accidents - part 4. IDAC Causal

model of operator problem-solving response. **Reliability Engineering and System Safety**. 2006

CHANG, Y.; MOSLEH, A (e). Cognitive modeling and dynamic probabilistic simulation of operating crew response to complex system accidents - part 5. Dynamic probabilistic simulation of the IDAC model. **Reliability Engineering and System Safety**. 2006

CHANG, Y.; MOSLEH, A. (b) Cognitive modeling and dynamic probabilistic simulation of operating crew response to complex system accidents - part 2. IDAC Performance influencing factors model. **Reliability Engineering and System Safety**. 2006

COMPANHIA AMBIENTAL DO ESTADO DE SÃO PAULO -CETESB. Risco de Acidente de Origem Tecnológica - Método para decisão e termos de referência. **Norma Técnica P4.261.** 2ed. 2014

CSB - U.S. Chemical Safety and Hazard Investigation Board. Final Report - Chevron Richmond Refinery. Pipe Rupture and Fire. **REPORT NO. 2012-03-I-CA**. January 2015

CSB - U.S. Chemical Safety and Hazard Investigation Board. Investigation Report – Refinery Explosion and Fire. **Report No. 2005-04-I-TX**. March 2007

CSB (a) - U.S. Chemical Safety and Hazard Investigation Board. Investigation Report – Catastrophic Rupture of Heat Exchanger. **Report 2010-08-I-WA**. May 2014

CSB (b) - U.S. Chemical Safety and Hazard Investigation Board. Regulatory Report – Chevron Richmond Refinery. Pipe Rupture and Fire. **REPORT NO. 2012-03-I-CA**. October 2014

EKANEM, N. & MOSLEH, A. (a) Phoenix – A Model-Based Human Reliability Analysis Methodology: Qualitative Analysis Overview. **Proceedings to Probabilistic Safety Assessment and Management PSAM12.** Honolulu, Hawaii, 2014

EKANEM, N.; MOSLEH, A. Human failure event dependency modeling and quantification: A Bayesian network approach. **In Proc. 2013 European Safety and Reliability (ESREL) Int. Conf**., Amsterdam, Netherlands, 2013.

EKANEM, N.; MOSLEH, A.; SHEN, S. Phoenix – A model-based Human Reliability Analysis methodology: Qualitative Analysis Procedure. **Reliability Engineering and System Safety** v 145, p 301–315, 2016

EKANEN, N. J. **A Model-Based Human Reliability Analysis Methodology (Phoenix Method).** Ph.D. dissertation, University of Maryland at College Park, 2013

EKANEN, N.; MOSLEH, A. (b) Phoenix – A Model-Based Human Reliability Analysis Methodology: Quantitative Analysis Procedure and Data Base. **Proceedings to Probabilistic Safety Assessment and Management PSAM12**. Honolulu, Hawaii, 2014

EPA - U.S. Environmental Protection Agency. EPA **Chemical Accident Investigation Report - Tosco Avon Refinery - Martinez**, California. Washington, 1998

FELICE, F.; PETRILLO, A.; CARLOMUSTO, A.; RAMONDO, A. Human Reliability Analysis: a review of the state of the art. **International Journal of Research in Management & Technology**. 2012

FORESTER, J.; DANG, V.; BYE, A.; LOIS, E.; MASSAIU, S.; BROBERG, H.; BRAARUD, P.; BORING, R.; MANNISTO, I.; LIAO, H.; JULIUS, J.; PARRY, G.; NELSON, P. The International HRA Empirical Study – Final Report – Lessons Learned from Comparing HRA Methods Predictions to HAMMLAB Simulator Data", **NUREG-2127 (HWR-373)**, OECD Halden Reactor Project. 2013

FORESTER, J.; KOLACZKOWSKI, A.; LOIS, E.; KELLY, D. Evaluation of Analysis Methods Against Good Practices. Final Report. **NUREG-1842**. U.S. Nuclear Regulatory Commission Office of Nuclear Regulatory. 2006

GALIZIA, A.; DUVAL, C.; SERDET, E.; WEBER, P.; SIMON, P; IUNG, B. Advanced investigation of HRA methods for probabilistic assessment of human barriers efficiency in complex systems for a given organisational and environmental context. **International Topical Meeting on Probabilistic Safety Assessment and Analysis**, PSA 2015, Apr 2015

GERTMAN, D.; BLACKMAN, H.; MARBLE, J.; BYERS, J.; SMITH, C. The SPAR-H human reliability analysis method. Tech. rep. **NUREG/CR-6883**. Washington, DC: US Nuclear Regulatory Commission; 2005.

GHOLI-NEJAD, N.; JAFARI, M.; GHALEHNOI, M.; MEHRABI, Y.; GHADIRI, M.; NIKBAKHT, M. Structure of human errors in tasks of operators working in the control room of an oil refinery unit. **Indian Journal of Science and Technology**. Vol. 5 No. 2. ISSN: 0974- 6846. 2012

GOULD, J.; LOVELL, S. Human Error Analysis at a Refinery**. IChemE Symposium Series no. 155** - Hazards XXI. 2009

GROTH, K. A data-informed model of performance shaping factors for use in human reliability analysis. PhD Dissertation. College Park, Maryland: University of Maryland, 2009

GROTH, K.; MOSLEH, A. A data-informed PIF hierarchy for model-based Human **Reliability Analysis, Reliability Engineering and System Safety**, v 108, p 154-174. 2012

GROTH, K.; SWILER, L. Bridging the Gap between HRA research and HRA practice: A Bayesian network version of SPAR-H**. Reliability Engineering and System Safety**. 2013

HENDRICKSON, S.; WHALEY, A.; BORING, R.; SHEN, S-H.; MOSLHE, A.; OXSTRAND, J.; FORESTER, J.; KELLY, D. A Mid-Layer Model for Human Reliability Analysis: Understanding the Cognitive Causes of Human Failure Events, in **Proc. 2010 Probabilistic Safety Assessment and Management (PSAM 10)** Int. Conf., Washington, USA, 2010.

HOLLNAGEL E. **Cognitive reliability and error analysis method (CREAM**). 1 ed. Amsterdam, the Netherlands: Elsevier; 1998.

HOLLNAGEL, E. Human Reliability Analysis in context. **Nuclear Engineering and Technology,** v 37, no. 2, 2005.

HOLLNAGEL, E. **Human reliability analysis: context and control.** Academic Press., 1993

HSE - Health and Safety Executive. **Managing human performance:** Core topic 3: Identifying human failures. 2008.

KARIUKI, S. G.; LOWE, K. Integrating human factors into process hazard analysis. **Reliability Engineering and System Safety**, n 92, p 1764–1773, 2007

KIM, M.; SEONG, P.; HOLLNAGEL, E. A probabilistic approach for determining the control mode in CREAM. **Reliability Engineering and System Safety**, n115, p 33-42. 2013

KIRWAN, B. **A guide to practical human reliability assessment**. London: Taylor & Francis, 1994.

KOFFSKEY, C.; IKUMA, L.; HARVEY, C. Performance Metrics for Evaluating Petro-Chemical Control Room Displays. **Proceedings of the Human Factors and Ergonomics Society 57th Annual Meeting**. 2013

KOLACZKOWSKI, A.; FORESTER, J.; LOIS, E. ; COOPER, S. **NUREG-1792** - Good Practices For Implementing Human Reliability Analysis, Final Report. Prepared for Division of Risk Analysis and Applications by Sandia National Laboratories. 2005

LAUMANN, K.; ØIEN, K.; Taylor, C.; Boring, R.; Rasmussen, M. Analysis of human actions as Barriers in major accidents in the petroleum industry, applicability of human reliability analysis methods (Petro-HRA). **Probabilistic Safety Assessment and Management PSAM 12**, Hawaii, 2014

MACKENZIE, C.; HOLMSTRON, D.; KASZNIAK, M. Human Factors Analysis of the BP Texas City Refinery Explosion. **Proceedings of the Human Factors and Ergonomics Society Annual Meeting**. 2007

MARTINS, M.; MATURANA, M. Application of Bayesian Belief networks to the human reliability analysis of an oil tanker operation focusing on collision accidents. **Reliability engineering and System Safety**, 2013

MERWE, K.; HOGENBOON, S.; RASMUSSEN, M.; LAUMANN, K.; GOULD, K. Human Reliability Analysis for the Petroleum Industry: Lessons learned from applying SPAR-H. **SPE Economics and Management**, 2014

MKRTCHYAN, L.; PODOFILLINI, L.; DANG, V. Bayesian belief networks for Human Reliability Analysis: a review of applications and gaps. **Reliability Engineering and System Safety,** v 129, p1-16. 2015

MOHAGHEGH, R.; KAZEMI, R.; MOSLEH, A. Incorporating organizational factors into Probabilistic Risk Assessment (PRA) of complex socio-technical systems: A hybrid technique formalization. **Reliability Engineering and System Safety,** v 94, p 1000-1018. 2009

MOHAGHEGH, Z.; KAZEMI, R.; MOSLEH, A.. "Incorporating organizational factors into Probabilistic Risk Assessment (PRA) of complex socio-technical systems: A hybrid technique formalization". **Reliability engineering and System Safety**, 94(5), pp: 1000-1018. 2009

MOSLEH, A.; CHANG, J. Cognitive modeling and dynamic probabilistic simulation of operating crew response to complex system accidents—Part 1 overview of the IDAC model. **Reliability Engineering and System Safety,** 2007.

MOSLEH, A.; CHANG, J. Model-Based Human Reliability Analysis: Prospects and Requirements. **Reliability Engineering & System Safety**, vol. 83, no. 2. 2004.

MOSLEH, A.; FORESTER, J.; BORING, R.; HENDRICKSON, S.; WHALEY, A; SHEN, S-H; KELLY, D.; CHANG, J.; DANG, V.; OXSTRAND, J.; LOIS, E. A model-based human reliability analysis framework. In: **Proceedings of the international conference on probabilistic safety assessment and management PSAM 10**. Washington, USA; June 2010.

MOSLEH, A.; SHEN, S-H; KELLY, D.; OXTRANS, J.; GROTH, K. A model-based human reliability analysis methodology. In: **Proceedings of the international conference on probabilistic safety assessment and management PSAM 11**. Helsinki, Finland; June 2012.

NICHOLSON, A. Bayesian Artificial Intelligence. **Series in Computer Science & Data Analysis**. Chapman & Hall/CRC. London. 2003

NIVOLIANITOU, Z.; KONSTANDINIDOU, M.; MICHALIS, C. Statistical analysis of major accidents in petrochemical industry notified to the major accident reporting system (MARS), **Journal of Hazardous Materials**, v 137,p 1-7, 2006

NOLAN, D. **Handbook of Fire and Explosion Protection Engineering Principles**. Ed. Elsevier. 3rd Edition. 2014

OSHA - Occupational Safety and Health Administration. **Petroleum Refinery Process Safety Management National Emphasis Program.** 2007. Available at <https://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=DIRECTIVES&p_id=3589>

OXSTRAND J.; KELLY, D.; SHEN, S-H.; MOSLEH, A.; GROTH, K. A Model-based approach to HRA: Qualitative Analysis Methodology. **Proceedings of the International Conference on Probabilistic Safety Assessment and Management (PSAM11)**. Finland, 2012

PALTRINIERI, N.; MASSAIU, S.; MATTEINI, A. Human Reliability Analysis in the Petroleum Industry: Tutorial and Examples. **Dynamic Risk Analysis in the Chemical and Petroleum Industry.** Edited by Paltrinieri and Khan. p 181-192. 2016

PODOFILLINI, L.; MKRTCHYAN, L.; DANG, V. Quantification of Bayesian Belief net Relationships for HRA from operational event analyses. . **Proceedings of the International Conference on Probabilistic Safety Assessment and Management (PSAM12)**. Honolulu, 2014

PYY, P. **Human Reliability Analysis methods for probabilistic safety assessment**. Technical Research Centre of Finland, VTT Publications. PhD Dissertation. Lappeenranta University. 2000

RAMOS, M.; DROGUETT, E. Quantitative Risk Analysis of an LNG terminal using two-step Bayesian analysis. *In: Proceedings to the European Safety and Reliability Conference ESREL 2013*. Amsterdam, 2013.

ROSEKIND, M.; GREGORY, K.; MILLER, D.; CO, E.; LEBACQZ, J. Analysis of crew fatigue factors in AIA Guantanamo Bay aviation accident, appendix E. **Aircraft Accident Report**: Uncontrolled Collision with Terrain, NTSB/AAR-94/04. Washington, 1993

SAURIN, T.; GONZALEZ, S. Assessing the compatibility of the management of standardized procedures with the complexity of a sociotechnical system: Case study of a control room in an oil refinery. **Applied Ergonomics**, 2013

SHEN, S-H.; MOSLEH, A.; KELLY, D.; BORING, R. Example Application of Model-Based HRA Approach, **Proc. of the 10th Int. Conf. on Probabilistic Safety Assessment and Management**. 2010

SHIRLEY, R.; SMIDTS, C.; LI, M.; GUPTA, A. Validating THERP: Assessing the scope of a full-scale validation of the Technique for Human Error Rate Prediction. Annals of Nuclear Energy, v 77, p 194-211. 2015

SMIDTS, C., SHEN, S-H, MOSLEH, A. The IDA cognitive model for the analysis of nuclear power plant operator responses under accident conditions. Part 1: Problem solving and decision making model. **Reliability Engineering & System Safety**, vol. 55, no. 1, pp. 51-71, 1997.

SOUZA, C.; FREITAS, C. Analysis of work-related accidents and incidents in an oil refinery in Rio de Janeiro. Cad. **Saúde Pública**, Rio de Janeiro, 19(5):1293-1303, set-out, 2003

SPURGINI, A. **Human Reliability Assessment Theory and Practice**. CRC Press. 2009

SWAIN, A. A method for performing a human factors reliability analysis. **Monograph SCR-685**, Sandia National Laboratories. Albuquerque, NM, USA. 1963

SWAIN, A. Accident Sequence Evaluation Program Human Reliability Analysis Procedure, **NUREG/CR-4772**. US Nuclear Regulatory Commission, Washington, DC. 1987

SWAIN, A. Human Reliability Analysis: need, status, trends and limitations. **Reliability Engineering and System Safety**, v 29, p 301-313. 1990

SWAIN, A.; GUTTMAN, H. Handbook of human reliability analysis with emphasis on nuclear power plant applications. Tech. rep. **NUREG/CR-1278**. Washington, DC: US Nuclear Regulatory Commission; 1983.

SWAIN, A.D. & GUTTMAN H. E. Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications. **NUREG/CR-1278**, Sandia National Laboratories, USA. 554p. 1983

TAYLOR, C. Qualitative Data Collection for Human Reliability Analysis in the Offshore Petroleum Industry. **Probabilistic Safety Assessment and Management PSAM 12,** Hawaii, 2014

TNO. **CPR18E** - Guidelines for Quantitative Risk Assessment - Purple Book. The Hague, 2005

TRUCCO, P.; CAGNO, E.; RUGGERRI, F.; GRANDE, O. A Bayesian Belief Network modeling of organizational factors in risk analysis: a case study in maritime transportation. **Reliability Engineering and System Safety**. 2008

UNDERGAARD, N. Hydrogen production by steam reforming of hydrocarbons. **Preprints of Papers - American Chemical Society, Division of Fuel Chemistry**. 2004

US NUCLEAR REGULATORY COMMISSION (USNRC). Technical Basis and Implementation Guidelines for A Technique for Human Event Analysis (ATHEANA). **NUREG- 1624**. Division of Risk Analysis and Applications. Office of Nuclear Regulatory Research, Washington DC. May 2000

VEJA, 2015 - available at http://veja.abril.com.br/noticia/economia/explosao-em-refinaria-da-petrobras-na-ba-deixa-3-feridos

VINEEM, J.; BYE, R.; GRAN, B.; KONGSVIK, T.; NYHEIM, O.; OKSTAD, E.; SELJELID, J.; VATN, J. Risk modelling of maintenance work on major process equipment on offshore petroleum installations. **Journal of Loss Prevention in the Process Industrie**s, 2012

WHALEY, A., HENDRICKSON, S., BORING, R., XING, J. Bridging human reliability analysis and psychology, Part 2: A cognitive framework to support HRA, **in Proc. 2012 Probabilistic Safety Assessment and Management (PSAM 11) Int. Conf**., Helsinki, Finland, 2012.

WHALEY, A.; XING, A.; BORING, R.; HENDRICKSON, S.; JOE, J.; LE BLANC, J.; LOIS, E. Building a psychological foundation for human reliability analysis, US Nuclear Regulatory Commission & Idaho National Engineering and Environmental Laboratory, Tech. Rep. **NUREG-2114 / INL/EXT-11-01166,** 2012.

WILLIAMS, J. HEART: A proposed method for assessing and reducing human error, **Advances in Reliability Technology Symposium** (9th), University of Bradford. 1986.

APPENDIX A

Specialist's Questionnaire

Field of expertise	
Years of experience	
In your knowledge of petrochemical/refinery control room operations, which Crew Failure Modes would be more likely to happen?	
Crew Failure Modes are generic functional modes of failure of the crew in its interactions with the plant, and can happen during information gathering, situation assessment, decision and action. Ex: failure to respond to an alarm, failure to follow a procedure, or acting on the wrong component/object	

What are the factors that could affect such operator errors (in your response please specify factors under major categories such as cognitive factors, environmental factors, organizational factors, human-system interface factors, etc.)	

Please mark the table below about CFMs on Refinery control room

CFM	**Frequency**			
	Extremely rare	**Remote**	**Probable**	**Frequent**
	Conceptually possible, but I don't see how it would happen	It's not expected to happen, although I see how it could happen	Happens occasionally. I have seen or heard about such events	happens often
Key alarm not responded to (intentional & unintentional)				
Data Not Obtained (Intentional)				
Data Discounted				
Decision to Stop Gathering Data				
Data Incorrectly Processed				
Reading Error (e.g. instrument reading error)				
Information Miscommunicated				
Wrong Data Source Attended to				
Data Not Checked with Appropriate Frequency				

Plant/System State Misdiagnosed				
Procedure Misinterpreted				
Failure to Adapt Procedures to the Situation				
Procedure Step Omitted (Intentional)				
Inappropriate Transfer to a Different Procedure				
Decision to Delay Action				
Inappropriate Strategy Chosen				
Incorrect Timing of Action				
Incorrect Operation of Component/Object				
Action on Wrong Component / Object				

Are there any failure modes you know of that are not covered by the ones in the table above? If yes, which ones?

_____
_

PIFs are the factors that influence the operators' actions. In the table below, mark as **Non Relevant (NR), Moderately Relevant (MR)** or **Highly Relevant (HR)** regarding the influence the PIF can have on an operator working on a **refinery control room**.

Group	PIF	NR	MR	HR
Human System Interface	1. Human System Interface Input			
	2. Human System Interface Output			
Procedures	3. Procedure Quality *refers to the condition of the required procedure with regard to completeness of content, ease of adherence and appropriateness in terms of ensuring adequate job completion*			
	4. Procedure Availability *refers to the situation where procedures for*			

		the task at hand are in existence and accessible			
Resources	Tools	5. Tool Availability *refers to the appropriateness and readiness of the required tools, e.g a valve, a pressure indicator*			
		6. Tool Quality *refers to the accessibility of the required tools to perform the task at hand.*			
		7. Workplace adequacy *refers to the quality of the work environment and includes aspects of workplace layout and configuration that could affect crew performance.*			
Team Effectiveness	Communication	8. Communication Quality *refers to the degree by which the information that is received corresponds to the information that was transmitted*			
		9. Communication Availability *refers to the existence and accessibility of the tools, means and mechanisms necessary for the crew to share information.*			
	Team Coordination	10. Leadership *refers to the team leader's ability to set a direction and gain the commitment of the team to change / maintain goals by building relationships and working with them to overcome obstacles to change.*			
		11. Team Cohesion *refers to the interpersonal interaction between the crew members and represents the group morale and attitude towards each other.*			
		12. Role Awareness *represents how well each crew member understands his or her responsibilities, role, and duties within the group.*			
		13. Team Composition *refers to the size, uniformity and variety of the team which provides the required knowledge, experience and skills to perform a given task*			
		14. Team Training *refers to the degree to which the crew members are trained on how to work with each other as members of the same team*			
Knowledge/ abilities	Knowledge/ experience/ skill (content)	15. Task training *refers to the adequacy of knowledge/Experience/skill , that the crew possesses for the task at hand.*			
	Knowledge/ experience/ skill (access)	16. Attention *is comprised of attention to the current task and attention to the surroundings*			
		17. Physical Abilities and Readiness *Physical Abilities includes alertness, fatigue,*			

		sensory limits, and fitness for duty			
Bias		18. Morale / Motivation / Attitude *indicates their commitment and willingness to thoroughly complete task and the amount of effort they are willing to put into a task*			
		19. Safety Culture *organizational attitude, values, and beliefs toward the employees and the safety of the public*			
		20. Confidence in Information *refers to the team's belief in the information they have in terms of accuracy, validity, credibility, etc.*			
		21. Familiarity with or Recency of Situation *refers to the perceived similarities between the current situation and the crew's past experiences, training received and general industry knowledge*			
		22. Competing or Conflicting Goals *refers to the situation where the crew has different goals and objectives that are conflicting or competing*			
Stress	Stress due to Situation Perception	23. Perceived Situation Urgency *refers to the tension / pressure induced on the team by the assessment of the speed at which an undesired outcome (e.g. system failure) is approaching*			
		24. Perceived Situation Severity *refers to the tension / pressure on the crew caused by their assessment of the magnitude of an undesired outcome (e.g. system failure) and its potential consequences.*			
		25. Stress due to Decision *refers to the tension / pressure on the crew caused by the awareness of the responsibility that comes along with that particular decision and their perception of the impact / consequences of the decision on themselves, the facility and the society in general.*			
Task Load	Cognitive Complexity	26. Inherent Cognitive Complexity *Refers to the cognitive demands induced on the crew by the inherent complex nature of the problem being solved*			
		27. Cognitive Complexity due to External Factors r*efers to the cognitive demands induced on the crew by external situational factors and conditions*			
	Execution Complexity	28. Inherent Execution Complexity *refers to the physical demands induced on the crew by the inherent complex nature of the problem being solved*			
		29. Execution Complexity due to External Factors			

		refers to the physical demands induced on the crew by external situational factors and conditions.			
		30. Extra Work Load *refers to the load induced on the crew by the extra work that has to be performed in addition to the main tasks.*			
		31. Passive Information Load *refers to the load induced on the crew by the amount of information and cues (e.g. indicators, alarms) that is presented to them by the external world*			
Time constraint		32. Time Constraint *refers to the crew's perception of the adequacy of the time available to complete the task at hand.*			

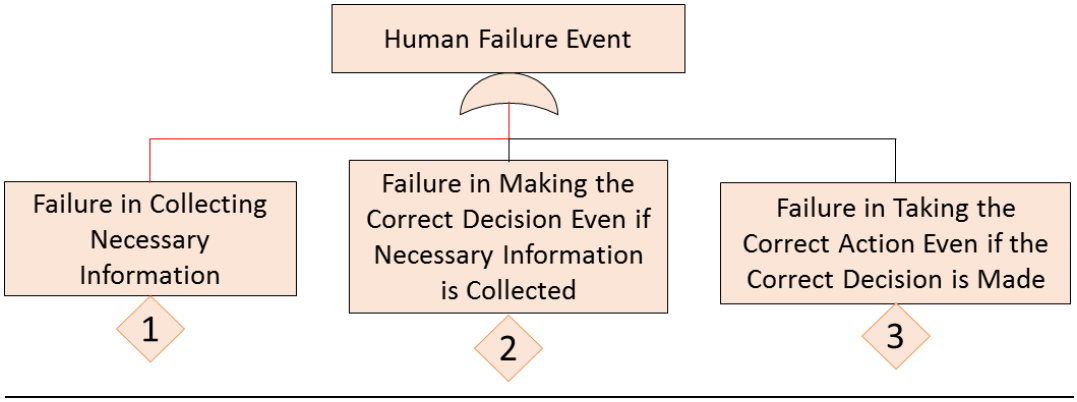
Are there any PIFs that are not covered by the ones in the table above? If yes, describe.

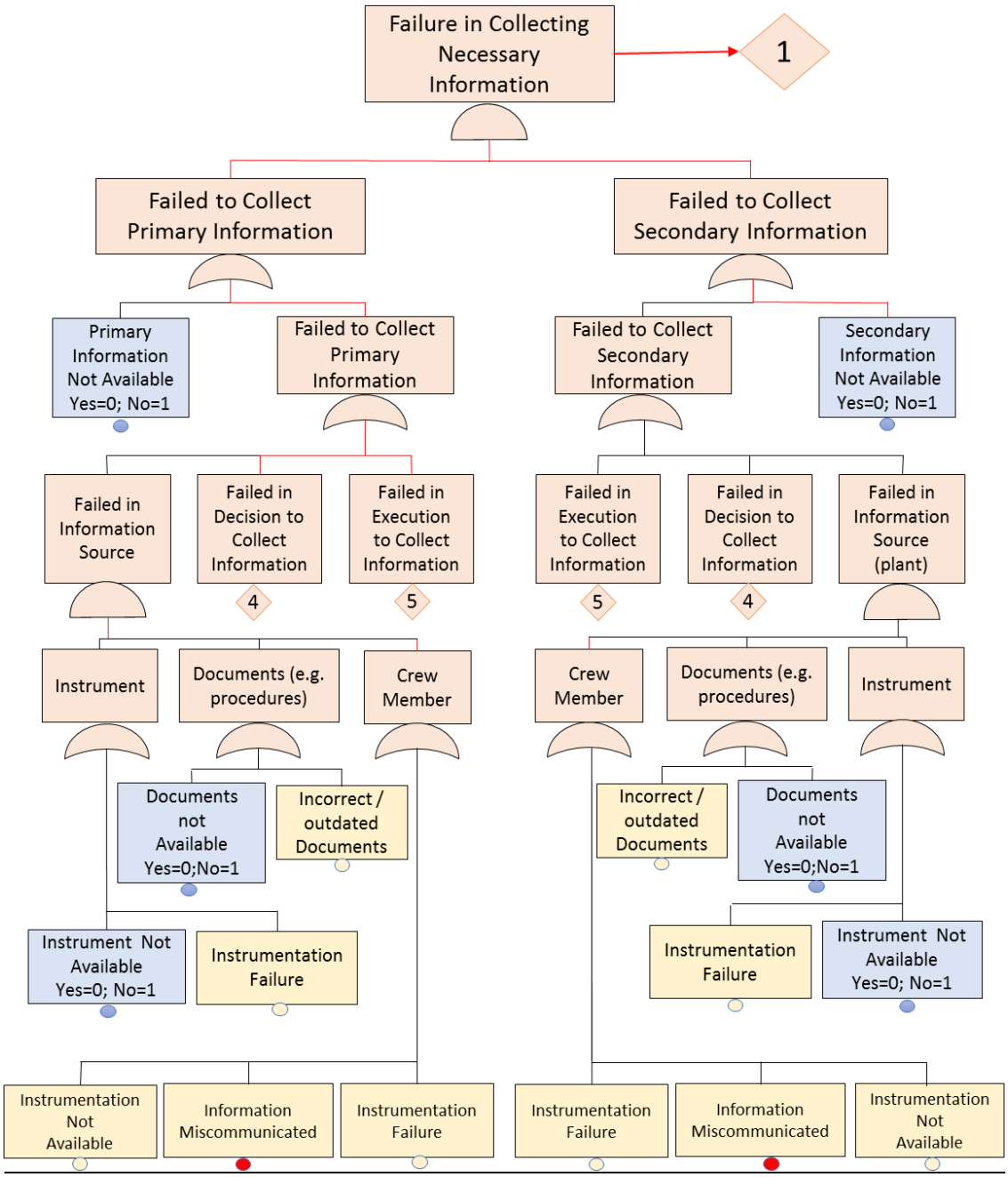
Would you describe some of the PIFs above in a more specific manner to better represent oil refineries/petrochemical plants control room? If yes, describe below.

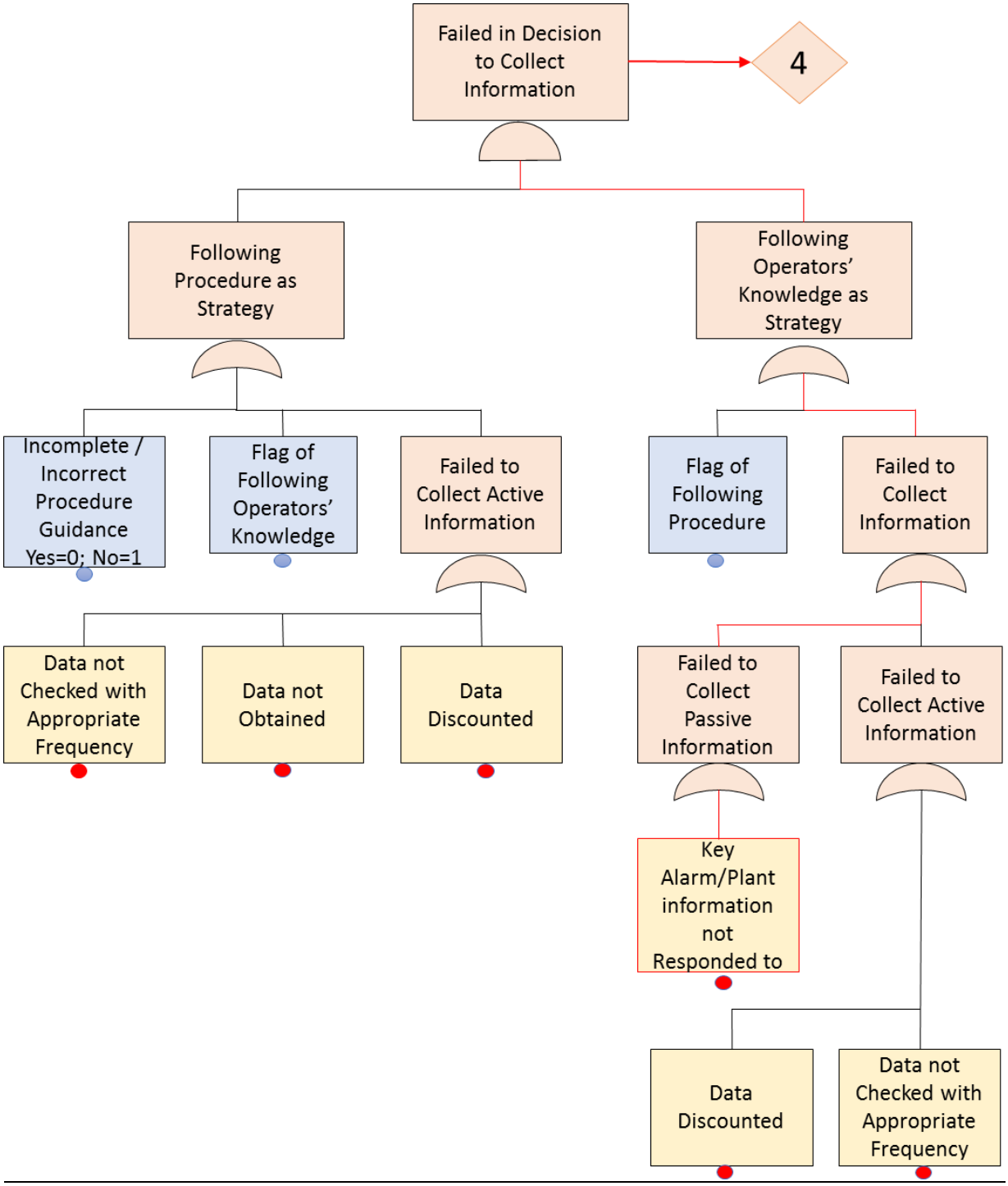
APPENDIX B

Fault Trees for Hydrotreating Unit Scenario (section 5.3)

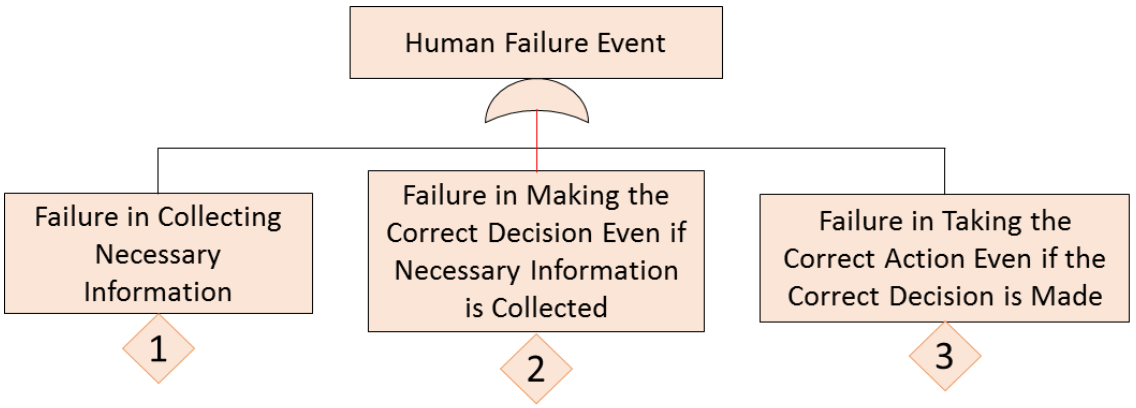
Branch Point D

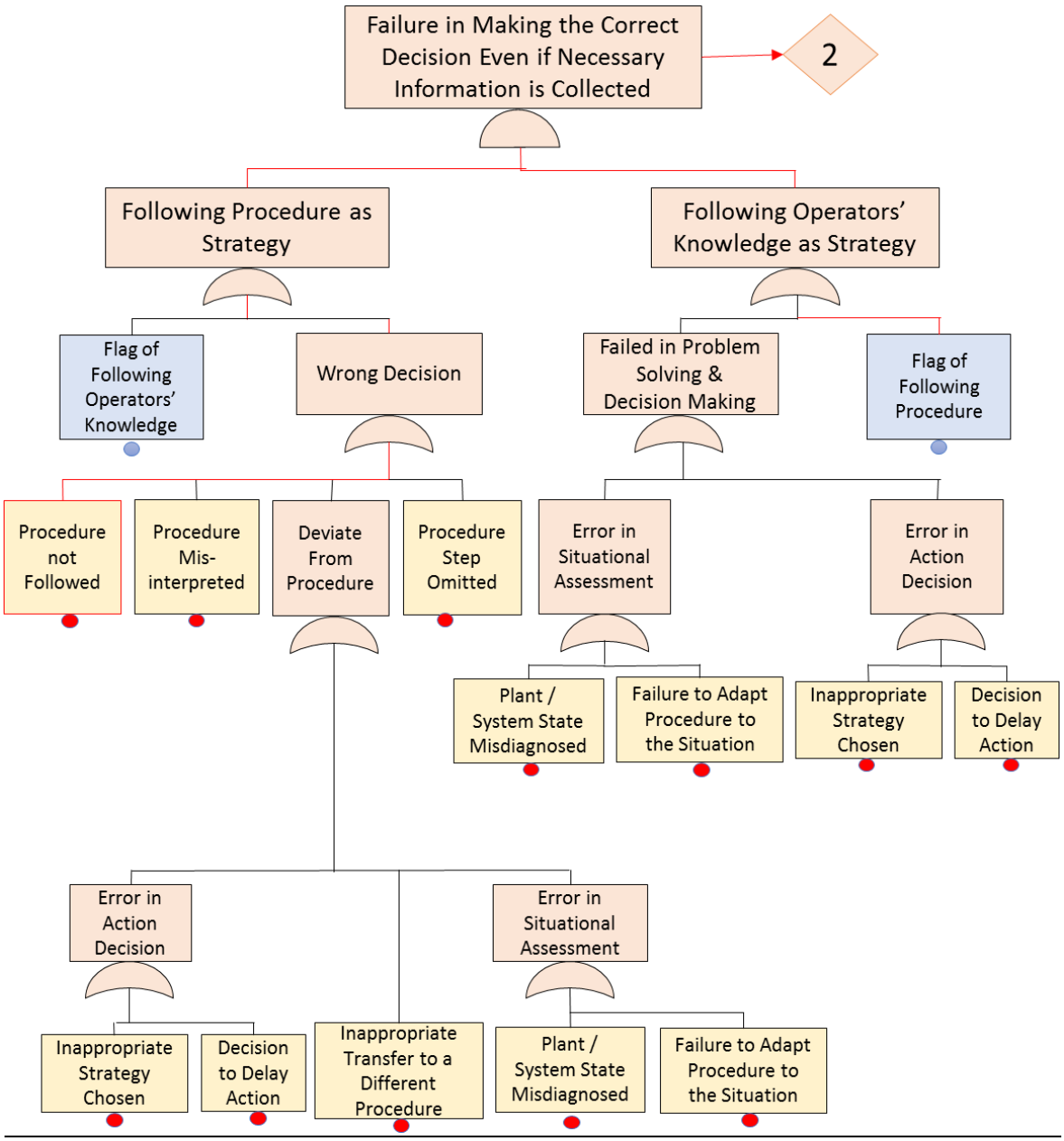



Failure in Collecting Necessary Information
1
Failed to Collect Primary Information
Failed to Collect Secondary Information
Primary Information Not Available Yes=0; No=1
Failed to Collect Primary Information
Failed to Collect Secondary Information
Secondary Information Not Available Yes=0; No=1
Failed in Information Source
Failed in Decision to Collect Information
Failed in Execution to Collect Information
Failed in Execution to Collect Information
Failed in Decision to Collect Information
Failed in Information Source (plant)
4
5
5
4
Instrument
Documents (e.g. procedures)
Crew Member
Crew Member
Documents (e.g. procedures)
Instrument
Documents not Available Yes=0;No=1
Incorrect / outdated Documents
Incorrect / outdated Documents
Documents not Available Yes=0;No=1
Instrument Not Available Yes=0; No=1
Instrumentation Failure
Instrumentation Failure
Instrument Not Available Yes=0; No=1
Instrumentation Not Available
Information Miscommunicated
Instrumentation Failure
Instrumentation Failure
Information Miscommunicated
Instrumentation Not Available


Failed in Decision to Collect Information
4
Following Procedure as Strategy
Following Operators' Knowledge as Strategy
Incomplete / Incorrect Procedure Guidance Yes=0; No=1
Flag of Following Operators' Knowledge
Failed to Collect Active Information
Flag of Following Procedure
Failed to Collect Information
Data not Checked with Appropriate Frequency
Data not Obtained
Data Discounted
Failed to Collect Passive Information
Failed to Collect Active Information
Key Alarm/Plant information not Responded to
Data Discounted
Data not Checked with Appropriate Frequency

Branch Point E




Failure in Making the Correct Decision Even if Necessary Information is Collected
2
Following Procedure as Strategy
Following Operators' Knowledge as Strategy
Flag of Following Operators' Knowledge
Wrong Decision
Failed in Problem Solving & Decision Making
Flag of Following Procedure
Procedure not Followed
Procedure Mis-interpreted
Deviate From Procedure
Procedure Step Omitted
Error in Situational Assessment
Error in Action Decision
Plant / System State Misdiagnosed
Failure to Adapt Procedure to the Situation
Inappropriate Strategy Chosen
Decision to Delay Action
Error in Action Decision
Error in Situational Assessment
Inappropriate Strategy Chosen
Decision to Delay Action
Inappropriate Transfer to a Different Procedure
Plant / System State Misdiagnosed
Failure to Adapt Procedure to the Situation

Branch Point F