POLITECNICO DI TORINO

DOCTORATE SCHOOL
Ph.D. in Metrology: Measuring science and Technique - XXVIII doctoral cycle

PhD Thesis

Lessons learned from past accidents - The integration of human and organizational factors with the technical aspect

Mehmood Ahmad

PhD Supervisors	**PhD Coordinator**
Dr. Marco Pontiggia Prof. Micaela Demichela	Prof. Franco Ferraris

December 2015

EXECUTIVE SUMMARY

It is of prime importance to ensure the safety of chemical process plants due to volatile nature of the industry and drastic consequences of the accidents. A number of parameters can affect the safety of the process plants. One of the main parameters that has the influence on the safety of operations is the Human and Organizational Factors (HOF) as suggested by numbers of existing studies. Therefore, in order to enhance the safety of operations it is required to improve the HOF. These factors can be improved by an integrated approach as proposed in this work, instead looking at these factors in an isolation. A number of existing risk assessment approaches have been analysed in this work and their compliance requirements to the relevant International Standards with respect to the HOF.

A new quantitative methodology “Method for Error Deduction and Incident Analysis (MEDIA)” has been developed in this work. During the development of this methodology, practicality; consistency; integration with other risk assessment techniques and efficient use of information were explicitly ensured. The MEDIA can help to integrate the HOF around the technical aspect and can prioritize the follow up actions based on risk. The quantification of this methodology is based on results of the accident analysis, that has been carried out in this work. The accidents of 25 years (1988-2012) in the Seveso establishments and that were reported to the European Commission’s Major Accident Reporting System (eMARS) have been studied.

The results from the accident analysis have further used in order to learn lessons and to propose future recommendations. These recommendations are mainly aimed at further integration of the HOF and to improve the overall safety of chemical process plants. More specifically, these recommendations are addressed to the use of organizational checklist during the Hazard Identification (HAZID) study; improvement of existing eMARS reporting structure and the legal obligation towards the EU Member States to report their accidents to the European Commission.

Acknowledgements

I would like to express my cordial gratitude to Dr. Marco Pontiggia for his valuable contribution to this work and help to overcome the obstacles during the course of this work. I also extend special thanks to Prof. Micaela Demichela for her precious assistance and guidance to refine this work. I was fortune enough to work with these people and to learn from their immense knowledge.

I wish to thanks Prof. Maria Chiara Leva (Trinity College Dublin), who has helped with the human factors quantification aspect and to adapt this work according to the aspirations.

I am also grateful to various people for their contribution to this work: Prof. Oliver Sträter (Universität Kassel) for reviewing work related to the CAHR application; Ms. Maureen Heraty Wood (European Commission Joint Research Centre - Major Accident Hazards Bureau) for providing the data in regard to the total number of EU Seveso establishments; Prof. Simon Wilson (Trinity College Dublin) for reviewing the statistical aspects of this work; Mr. Giovanni Uguccioni (D'Appolonia S.p.A.) for his support to acquire the necessary set of skills and Mr. Paolo Paci (D'Appolonia S.p.A.) for his support to this project.

I also like to thanks Prof. Aleksandar Jovanovic (Steinbeis Advanced Risk Technologies GmbH) for letting me to perform my secondment with them.

I deeply acknowledge the European Commission for their funding to carry out this work. This work is part of the InnHF project which is financed by the European Commission under the EU FP7 Marie Curie Actions Initial Training Networks - FP7-PEOPLE-2011-ITN: Project ID 289837.

I am also grateful to all the colleagues in the D'Appolonia S.p.A. for their support during my stay there.

Last but not least, I would like to thank my family for their encouragement. For my parents, who have always encouraged and supported me throughout my decisions and endeavours. To all friends with whom I have shared ups and downs fairly well.

Table of Contents

List of abbreviations

PSA	Probabilistic Safety Analysis
HOF	Human and Organizational Factors
HAZOP	Hazard and Operability
QRA	Quantitative Risk Assessment
SIL	Safety Integrity Level
SIF	Safety Instrumented Function
SIS	Safety Instrumented System
PSV	Pressure Safety Valve
BDV	Blow Down Valve
LOPA	Layer of Protection Analysis
HEP	Human Error Probability
PSF	Performance Shaping Factors
HF	Human Factors
OF	Organizational Factors
NHEP	Nominal Human Error Probability
FEED	Front End Engineering Design
ALARP	As Low As Reasonably Practical
LOC	Loss of Containment
P&IDs	Piping and Instrumentation Diagrams
ESDV	Emergency Shut-down Valve
C&E	Cause and Effect
MOON	“M” out of “N”
PFD	Probability of Failure of Demand
HMI	Human Machine Interface
SCM	Swiss Cheese Model

1 Introduction

The Human and Organizational Factors (HOF) are associated to almost 30% of the Loss of Containment (LOC) events during normal and maintenance operations (OGP, 2010). Meanwhile, (Nivolianitou et al., 2006) have concluded after performing an accident analysis that around 40% of all the accidents have an immediate cause related to the human factors.

There are number of existing methods that can assess the HOF. However, a possible integration of HOF can help to manage the HOF in an efficient way. Among others, (Bellamy and Geyer, 2007) have proposed to model the human factors integrated with the technical aspect and to provide a risk-based human factors assessment. Furthermore, it was also observed that the human factor engineering and conventional risk assessment engineering move in parallel during the lifetime of a project and hence induce issues due to their complex interface and transfer of information among them.

In order to provide a possible integration, existing risk assessment approaches that are commonly used in the chemical process industry have been studied. The following main risk assessment approaches have been reviewed in this work:

- Hazard Identification (HAZID);
- Hazard and Operability (HAZOP);
- Quantitative Risk Assessment (QRA);
- Safety Integrity Level (SIL) allocation / verification;

This review step can also provide an insight into how these approaches currently consider the HOF.

However, one of the main issues faced during the human factors assessment is the human reliability data. The data required for the human factors assessment is either incomplete or had been inadequately validated (Sträter, 2000). At the same time, the human reliability data is also influenced by number of internal and external Performing Shaping Factors (PSF). The influencing effect of the PSF tend to change therefore adding more complexity into the overall human reliability data. Apart from that, most of the human reliability methods and data had been developed for the nuclear industry. So, there is a need to develop or at least to validate the existing human reliability data and to adapt them specifically according to the chemical process industry (CCPS, 2000).

This work consists of following main steps:

- Development of a structure to analyse the accidents;
- Accidents analysis;
- Quantification of Human and Organizational Factors (HOF);
- Development of a new methodology (i.e. MEDIA);
- Recommendations followed by the accident analysis.

During this work, an accident analysis has been performed of the accidents reported to the European Commission's Major Accident Reporting System (eMARS). The accident analysis can help to gather the empirical data, required to quantify a HOF assessment. The probabilistic Rasch model has been used in this work to convert the obtained data into the human reliability data. The human reliability data can also be used in any of the risk assessment methods (e.g. fault tree analysis / bow tie etc) that require the Human Error Probabilities (HEPs).

A new methodology, Method for Error Deduction and Incident Analysis (MEDIA) has been developed based on the accident analysis. The MEDIA assessment not only provides a possible integration of HOF around the technical aspect but also adapt the THERP human reliability data according to the chemical process industry. The MEDIA assessment can identify the critical sections of a plant with respect to the HOF and the technical failure criticality. This new methodology can be carried out in MS Excel, integrated with the Hazard and Operability (HAZOP) and Quantitative Risk Assessment (QRA) studies.

Meanwhile, a number of recommendations are also proposed in this work as a result of the lessons learned from the accident analysis. These recommendations can help to improve and to integrate the HOF aspects in chemical process plants. The main recommendations are related to:

- HAZID study, to consider the organizational attributes;
- European Commission's Major Accident Reporting System (eMARS), to modify the existing report structure with respect to the HOF;
- Reporting criteria for the EU Member States to report their accidents to the European Commission, to modify the existing accidents reporting criteria;
- Preliminary risk assessment studies (e.g. HAZOP), to consider the maintenance activities during the risk assessment studies.

2 Major accidents – a way to learn lessons

The past accidents can provide the information about the inadequacies that possibly led to those accidents. Therefore, by analysing the accidents / near-misses it is possible to improve the situation for the future.

In this section, few accidents from the eMARS database are presented with a purpose to provide an overview of the problem and an insight about the lessons learned.

Accident 1

This accident was occurred on 10/09/2002 in a refinery, while workers were performing the catalyst unloading operation on a reactor at a Claus unit. The Claus process is used as a desulfurizing process to recover the sulfur. Therefore, workers were working in a highly toxic atmosphere. The workers from a hired contractor performed their actions for several hours with appropriate protective devices. By the end of the day, one of the workers violated the end of work order and entered the restricted area without any protection and supervision. He suddenly fell unconscious after entering into the vessel. The other two workers followed him in order to help him and suffered the same symptoms. All three workers were fatally injured as a result of this accident.

The accident was occurred due to release of hydrogen sulphide and possibly carbon monoxide from catalyst enclosure and worker's violation not to use the breathing apparatus at the end of the work. The reason why the workers violated the end of work order and entered into the vessel without protective means is still unclear. The worker's knowledge about the possible toxic atmosphere in the vessel and the consequences from their violation can also be questioned. It is quite probable that they were not aware of possible hazardous atmosphere and consequences of their actions as they were hired by an outside contractor to carry out this task.

Lessons learned

From this accident it can be learned that worker's knowledge about possible hazardous atmosphere and consequences of potential violations should be ensured. Moreover, whenever contractors are involved into the operations, it is required to further ensure the safety of operations and their preparedness for operations.

Accident 2

This accident was occurred on 03/09/2000 in a refinery, during a periodic test phase of a system in a catalytic reforming section of the plant. A number of complex factors have been identified during this accident that had increased the gravity of this accident. The accident was occurred according to the following order as reported in the eMARS database:

- Rupture of a ¾ inch tapping (connection) on the suction pipe of a pump;
- Ignition of the cloud (as a result of about 200 Kg of released material) and creation of torch fire;
- Rupture of another 3- inch pipeline which was exposed to the fire;
- By domino effect, rupture of the collector of a cooling tower and further ignition of released substances;
- By domino effect, rupture of 8-inch head pipe of a column and ignition of the release;
- By domino effect, rupture of the column valve collector, connected to the site's flare system, and ignition of the released substances;

The ignited releases kept on burning until the material being processed in the unit was exhausted. The hydrogen and hydrogen sulphide were released and ignited as a result of this accident. After investigations, numbers of factors have been identified that had led to this accident. These factors mainly caused a strong vibration of the pump, leading to fatigue stress and consequently to the rupture of the tapping connection of the pump. Another main factor that has increased the gravity of this accidents was an anomalous delay (of about 10 min) in closing the block valve of the feeding line to the pump. The valve was controlled an automatic safety system and should have operated within normal time (of about one min). The domino effects from the initial accident could have been mitigated by in-time intervention of the safety system. This accident has caused minor injury to one person and a seven-month shutdown of the unit. The material damage amounts to about 13.72 M€ for repairs and 68.6 M€ for production loss.

As a result of this accident, number of corrective actions have been proposed, some of the proposal are as follows:

- Change of pipe type and modification of the column alignment;
- Replacement of the valves on the pump feeding line in order to reduce the shutting time;
- Implementation of a campaign to increase the operator's awareness of the importance of strict application of the procedures.

Lessons learned

From this accident it can be learned that monitoring of un-wanted vibration of units specifically for pumps is important. Meanwhile, proper type of units should be selected by the management according to any potentially critical foreseen scenarios. The reaction time of the automatic safety functions should be verified by considering the shutting time, mainly from the final element.

Furthermore, in the accident number 2 and also in some other accidents it has been observed that whenever hydrocarbons release they find an un-identified source of heat and ignite. Therefore, considering three elements of a fire triangle it is recommended to contain hydrocarbons as much as possible rather than looking to isolate the hydrocarbons and the heat source. However, in certain cases these situations are interdependent.

3 An overview of existing tools/ methods

There are number of already developed tools/ methods that are used to assess/ quantify the risk of operations coming from the hazardous activities. Similarly, a numbers of human factor methods provide estimate about the reliability of human/ operator actions. In order to provide the estimates about the human reliability/ availability it is require to rely on a human factors database. A human factor database should also provide the guidelines about the modifications of Nominal Human Error Probability (NHEP) based on certain Performance Shaping Factors (PSF).

In this section an overview is provided about the relevant methods/ techniques that are used in the process industry to assess and to quantify the risk; widely used human factor databases and some of the human reliability methods.

3.1 Review of most commonly used risk assessment techniques

There are number of techniques, that are used in chemical process industry in order to assess and to manage the risk. Some of these techniques are listed in the Table 1.

Table 1: Review of risk assessment/ management techniques

Method	Qualitative/ Quantitative	Relevant Standards/ Engineering Guidelines
Hazard Identification (HAZID)	Qualitative	(ISO 17776, 2000)
Hazard and Operability (HAZOP)	Qualitative	(IEC 31010, 2009), (CEI/IEC 61882, 2001)
Quantitative Risk Assessment (QRA)	Quantitative	(CCPS, 2000), (Purple Book, 2005), (Green and Maloney, 1997)
Safety Integrity Level (SIL) assessment	Semi-qualitative	(IEC 61511, 2003), (IEC 61508, 1997)
Layer of Protection Analysis (LOPA) (also called barrier analysis	Quantitative	(IEC 31010, 2009), (IEC 61511, 2003)

The risk of a hazardous event is usually defined by a combination of likelihood and severity of that event. However, this deification of risk can subject to changes depending upon the context in which the risk is being considered.

3.1.1 Hazard Identification (HAZID)

The Hazard Identification (HAZID) is a technique for the identification of all significant hazards associated with a particular activity under consideration (ISO 17776, 2000). According to the International Standard (ISO 17776, 2000), a hazard is something with a potential to cause harm, this may include:

- Ill health or injury;
- Damage to property;
- Products;
- Production losses or increase liabilities.

In the risk management process, a hazard can be prevented from being released by using barriers or counter-measures. The barriers could be in the following forms (ISO 17776, 2000):

- Physical;
- Isolations;
- Separations;
- Protective devices;
- Procedures;
- Alarm systems;
- Training;
- Drills.

The International Standard also provide checklists to identify the potential hazards for offshore installations. These checklists can also be applied to onshore activities and can also be modify depending upon company’s operations. The following aspects related to hazard identifications and risk assessment with relevant check lists are included in the International Standard:

- Seismic and topographical surveys;
- Drilling and well completions;
- Field development;

- Operations;
- Decommissioning and disposal;
- Logistics.

The Table 2 shows the checklists from the International Standard that can be used for the hazards and risk assessment considerations with the proposed risk reduction measures. However, different set of checklists are proposed according to the project progress phases. The new HAZID checklists are proposed in this work, that are explained in detail in the section 5.2.

The HAZID assessment is usually performed during early phases of a project and therefore is very important to identify the potential deviations and to suggest recommendations to bring the residual risk to an acceptable level. The output from the HAZID is also generally considered during the HAZOP studies for enhanced analysis. The HAZID procedures follows a guided brainstorming using checklists in a HAZID team led by a third party chairman.

During the HAZID when a potential hazard is identified to be credible in a given plant's situation then specific cause and consequences of that hazard are also identified. The adequacy of barriers (preventive or recovery) is considered in order to assign hazard a "likelihood level". The following aspects are usually considered during the HAZID in order to assign a "severity level":

- Health
- Safety
- Environment
- Company's reputation

Usually, a probability and consequence matrix is used to rank the risk associated with the identified hazards/ deviation based on likelihood and gravity of that scenario. This is required in order to make a decision on the results of risk assessment and to establish a screening criteria. The Figure 1 illustrates a 5×4 risk matrix, on which it can be defined if the risk is acceptable or not. However, risk ranking criteria can vary from one company to the other.

If associated potential risk from inherent hazards is high or in intolerable region, then further recommendation should be agreed and proposed in order to achieve the residual risk within the tolerable region according to the pre-established criteria.

As highlighted by the International Standard, care should be taken in order to screen out the low probability and high consequences events. Since, a low probability can suggest a low probable occurrences of the events leading to a possibility of overlooking them.

The matrix proposed by the International Standard as shown in the Figure 1 has suggested to use the following main elements in order to rank the consequences of the events:

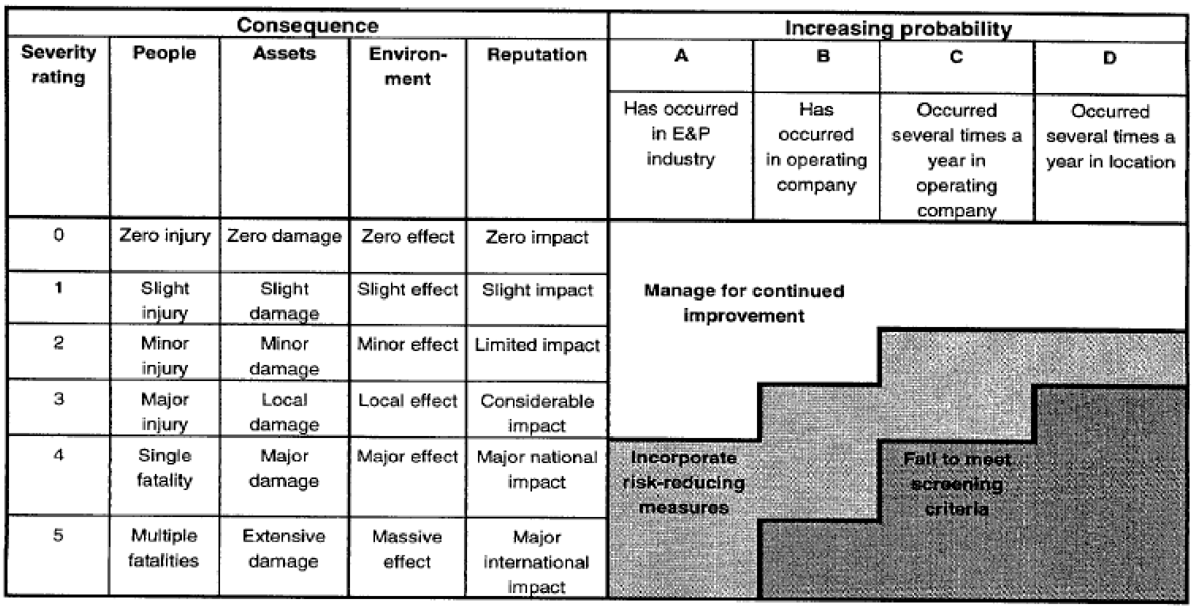
- People
- Assets
- Environment
- Reputation

Table 2: Examples of hazards identification and risk assessment considerations during the prospect evaluation and feasibility assessment phase of field development activities, Adapted from (ISO 17776, 2000), p. 35.

Activity: Field development	Description: This activity includes all tasks involved in the planning, design, procurement, construction, installations and commissioning of offshore installation used for the exploitation of oil and gas resources.	
Hazard identification and risk assessment step	Examples of aspects to be considered and activities undertaken	Comments
Identify hazards	• Consider broad hazards occurring throughout life cycle; • Identify main hazards and effects arising from wells, produced fluids and processing, structure, export facilities, utilities and manning arrangements, environment, logistic support arrangements etc; • Identify possible hazards associated with the construction and installation of the facility.	Particular attention should be given to hazards that could arise due to the use new technology or the extension of existing technology outside its previous range.
Hazards and risk assessment	• Experience from previous or similar projects; • Codes and standards, including company guidelines; • PHA; • Environmental risk assessment.	Major hazards and risks should be highlighted to allow risk management decision-making. Rough environment risk assessment concentrates on possible impact of development without consideration of frequency of occurrence.

Screening criteria	• Company maximum tolerable risk levels for personnel, environment and assets; • National and international regulations for health, safety and environment; • Special local constraints due to factors such as sensitivity of ecology, seismic activity.	At this stage the screening criteria is relatively broad.
Risk-reducing measures	• Inherently safety options to be selected whenever practicable; • Need for and extent of offshore processing; • Minimize hazardous inventory on the installation; • Minimize offshore manning without jeopardizing HSE considerations or production regularity; • Consider phased field development or long-term well testing to obtain better appreciation of risks; • Consider new technology where clear benefits are apparent; Give adequate considerations to minimize offshore inspection and maintenance tasks and evaluate alternative maintenance philosophies.	
Functional requirements	• High-level criteria regarding overall performance of installation; • High-level functional requirements for health, safety and environment protection systems to be established	

The risk in the ALARP region is acceptable if cost of further treatment is grossly disproportionate to the benefits gained (IEC 31010, 2009). In other words, the risk in ALARP region is acceptable if it is not feasible to bring down the risk economically or operationally.



Consequence					Increasing probability			
Severity rating	People	Assets	Environ-ment	Reputation	A	B	C	D
					Has occurred in E&P industry	Has occurred in operating company	Occurred several times a year in operating company	Occurred several times a year in location
0	Zero injury	Zero damage	Zero effect	Zero impact				
1	Slight injury	Slight damage	Slight effect	Slight impact	Manage for continued improvement			
2	Minor injury	Minor damage	Minor effect	Limited impact				
3	Major injury	Local damage	Local effect	Considerable impact				
4	Single fatality	Major damage	Major effect	Major national impact	Incorporate risk-reducing measures		Fail to meet screening criteria	
5	Multiple fatalities	Extensive damage	Massive effect	Major international impact				

Figure 1: Example of a risk matrix and consequences that may be considered, adapted from Standard (ISO 17776, 2000)

However, there are number of techniques that can be taken as hazard identification and these techniques are used in different stages of a project development as listed in the (Mannan, 2012) “Lees” p. 209”. Although, techniques quoted for one stage may also be applicable for another stage.

3.1.2 Hazard and Operability (HAZOP)

The hazard and operability (HAZOP) study is a structured and systematic analysis of a defined system with an objective to identify the potential hazards and operability problems (CEI/IEC 61882, 2001). In chemical process industry, among other relevant documents the Piping and Instrumentation Diagrams (P&IDs) are used to review a proposed design. This methodology relies on “guidewords” in contrary to checklists as in a HAZID study. The relevant guidewords are selected against each of the parameters and applied to all nodes in a plant.

In order to ease the guided brainstorming and to understand the complex continuous operations. A plant is usually divided into “nodes” depending upon the characteristics of materials and also the nature of operations. A "node" is a system, sub-system or portion of a system which can be analysed by itself, together with the relevant connections to the interfaces.

The HAZOP study is performed by a multidisciplinary team led by a third party HAZOP chairman to ensure the impartiality of HAZOP study. The Table 3 illustrates the basic guidewords with their generic meaning that can be used during a HAZOP study.

Table 3: Basic guidewords and their generic meaning, adapted from (CEI/IEC 61882, 2001)

Guidewords	Meaning
No or not	Complete negation of the design intent
More	Quantitative increase
Less	Quantitative decrease
As well as	Qualitative modification/increase
Part of	Qualitative modification/decrease
Reverse	Logical opposite of the design intent
Other than	Complete substitution
Guidewords relating to clock time and sequence	
Early	Relative to the clock time
Late	Relative to the clock time
Before	Relating to order or sequence
After	Relating to order or sequence

The Table 4 illustrates the typically used guidewords and deviations against different parameters during a HAZOP study. Each relevant deviation and hazards should be analysed identifying the primary potential causes (e.g. malfunction of a process control system, blockages, operational error, faulty maintenance activities, failure of power supply, cooling water, instrument air or other utilities, etc).

For each realistic cause that are identified, the consequences associated to the deviation are analysed without considering the existing safeguards, assessing whether identified causes can lead to a hazard (where the term "hazard" is intended from a safety or operational point of view: such as fire, explosion, release of flammable or toxic material, off-spec. products, loss of production, etc). Then the team considers what mitigating features actually exist (e.g. relief valves, shutdown systems, alarms, etc) and whether they could be considered sufficient or not, depending upon the severity of the expected outcomes.

When existing safeguards/ controls appear to be insufficient. In this case recommendations/

actions have to be proposed to control the hazard. The recommendations/ actions could be in the form of design modifications, extra safeguards or to review the operations procedures.

The output from HAZOP studies can also be used in further studies (e.g. QRA) to identify the credible process deviation events and where possible quantify the risk for those deviations and rank them according to company's risk ranking criteria.

However, depending upon the scope of a HAZOP and team members. The operator error are also considered intuitively during the HAZOP study. After that, depending upon the input from team members, the relevant deviation scenarios can be qualitatively ranked if causes (i.e operator error) are believed to be credible.

Table 4: Typical parameters, guidewords and deviations for continuous processes

Parameters	Guidewords	Deviations
Flow	No/ Less	No flow/ less flow
	More	High flow
	Reverse	Reverse flow
Temperature	More	High temperature
	Less	Low temperature
Pressure	More	High pressure
	Less	Low pressure
Level	More	High level
	Less/ None	Low level/ no level
State/ Composition	More	Additional Phase
	Less	Loss of phase
	Reverse	Change of state
	Other than	Off-spec composition / contaminants / corrosive concentration

A HAZOP can also be used in conjunction with other dependability analysis methods such as Failure Modes and Effects Analysis (FMEA) and Fault Tree Analysis (FTA) (CEI/IEC 61882, 2001), p. 13. Such combinations can be used in situations when:

- The HAZOP analysis clearly indicates that the performance of a particular item or equipment is critical and needs to be examined in a considerable depth. Then the HAZOP can be complimented by a FMEA of that particular item/ process;

- Having examine a single element/ deviating by the HAZOP it can be decided to assess the multiple deviations by FTA or to use the FTA to quantify the likelihood of a failure event (i.e. top event).

Whilst, HAZOP studies can provide extremely important indication about the potential process deviations. However, HAZOP also have limitations to explain complex situations in which there could be an interaction of multiple elements/ processes (CEI/IEC 61882, 2001). Therefore, it is essential to use the HAZOP in conjunction with other relevant studies. There is also a need to include the human error explicitly and affect of the overall safety management system on the results of a HAZOP.

3.1.3 Quantitative Risk Assessment (QRA)

A QRA is a tool for determining the risk of the use, handling, transport and storage of dangerous substances (Purple Book, 2005). The results from a QRA study are provided in the form of a safety report to demonstrate if calculated risk from an establishment is in the acceptable zone. The procedures to determine whether a safety report has to be made are provided in the "Seveso Directive" (EC, 2012) and are also mentioned in the (Purple Book, 2005).

Overall, the aim of a QRA study is to quantify the overall risk related to a specific plant, installation or facility with respect to people, health and safety. During a QRA, major accidental hazards arising from loss of containment events, which could lead to possible flammable gas dispersion, fire and/ or ignition or toxic exposures are analysed. Normally, following steps are taken in a QRA study:

- Hazard and incident identification;
- Frequency assessment;
- Consequence assessment;
- Risk assessment.

Further detail of aforementioned steps with relevant reference to be followed are provided in the (CCPS, 2000) and in (Purple Book, 2005).

During hazard and incident identification, major hazards are identified mostly coming from the Loss of Containment (LOC) events. Since, release of hydrocarbons (e.g. toxic or flammable) can easily lead to a hazardous situation. A complete set of LOC events consists of generic LOC, external-impact LOC, loading and unloading LOC and specific LOC (Purple Book, 2005). However, only those LOC should be considered which contribute to the individual or societal risk.

The following three major accidental events are usually identified and analysed within a QRA study:

- Process deviation Events;
- Loss of Containment (LOC) events;
- External events.

The process deviation events are those events occurring as a consequences of a process malfunction or an operator error. For example, failure of a Pressure Safety Valve (PSV) on an overpressure vessel or the operator's intervention associated with an overpressure vessel (e.g. responding to an alarm). The process deviation events can be identified based on the HAZOP report as mentioned earlier. While, LOC events consider an unexpected rupture (e.g. random rupture caused by corrosion, constructing errors, welding failures and blockage etc) of a piping/ equipment leading to release of a fluid (e.g. hydrocarbons etc). In case of particular facilities (e.g. offshore installation) some external events (e.g. ship interaction, dropped object and aircraft interaction) are also considered by adding an extra failure frequency, accounting for these particular interaction.

During QRA studies, process/ facility is divided into isolatable sections will the help of P&IDs, preferably by locating the isolation elements (e.g. ESVs etc) as an engineering practice. If the identification of isolation elements is not possible, the process streams will be divided based on homogenous representative streams, based on operative conditions (e.g. pressure, temperature, flow rate) and composition.

In order to estimate the frequency of previously identified events, Fault Tree Analysis (FTA) and historical failure data are used for process deviations and random rupture events, respectively. The Event Tree Analysis (ETA) is used to identify the final outcome of the accidental scenarios (i.e. process deviation, loss of containment and external events). The final outcome depends upon the characteristics of the events (e.g. type of release, nature of substance etc) and immediate surroundings (e.g. presence of ignition source, meteorological conditions, congestion and confinement etc).

The consequences of the identified scenarios are modelled using commercial tools by providing information about the characteristics of a release. The consequences are modelled in terms of distances reached by radiations or the hazardous concentrations.

In a QRA, risk assessment is usually performed qualitatively by using risk matrix approach as also shown in the Figure 1.The quantitative results can be obtained by using the estimated frequencies and obtained consequences, that can provide the vulnerability to the personnel exposed to the potential accidents based on physical accidents effects and the duration of the exposure. The calculation of the risk to individuals is performed on the basics of risk indices. The risk indices are usually single number estimates, which may be used to compare one risk with another or used in an absolute sense compared to a specific target, (Green and Maloney, 1997). The following main risk indices are used in a QRA to estimate the risk:

- Location Specific Individual Risk (LSIR);
- Individual Risk Per Annum (IRPA);
- Fatal Accident Rate (FAR);
- Societal risk.

3.1.4 Safety Integrity Level (SIL)

The Safety Integrity Level (SIL) assessment defines the level of integrity required by a Safety Instrumented Function (SIF) to prevent/ mitigate the hazardous events. The safety integrity levels are the discrete levels (i.e. 1OO4) for specifying the safety integrity requirements of the safety instrumented functions to be allocated to the safety instrumented systems (IEC 61511, 2003), p. 28. The Table 5 and Table 6 show the integrity levels for on-demand and continuous operations, respectively. The level 4 provides the highest level of safety integrity, while the level 1 provides the least safety integrity.

During the SIL verification, probability that a loop fails on demand, (probability of failure on demand, PFD) is assessed by the application of architectural constraints as given in the International Standard (IEC 61511, 2003). It is necessary to check if the assigned SIL level is satisfied for a given loop.

The Safety Instrumented System (SIS) is an instrumented system used to implement one or more safety instrumented functions. A SIS constitutes of initiators (device/ sensor or combination of devices/ sensors that indicates whether a process or equipment item is operating outside the operating range), logic solver (an element of SIS that performs the transformation between the input and output information) and the final element (device or combination of devices that manipulate a process variable).

Table 5: Safety integrity levels: probability of failure on demand

Safety integrity level (SIL)	Target average probability of failure on demand	Target risk reduction
4	$\geq 10^{-5}$ to $< 10^{-4}$	>10000 to ≤ 100000
3	$\geq 10^{-4}$ to $< 10^{-3}$	>1000 to ≤ 10000
2	$\geq 10^{-3}$ to $< 10^{-2}$	>100 to ≤ 1000
1	$\geq 10^{-2}$ to $< 10^{-1}$	>10 to ≤ 100

The Safety Instrumented Function (SIF) is a specific control/ mitigation performed by the SIS to achieve the specific risk reduction. It is also defined in the International Standard that when human action is a part of SIS, the availability and reliability of the operator actions must be specified and included in the SIS calculations (IEC 61511, 2003).

Table 6: Safety integrity levels: frequency of dangerous failures of the SIF (continuous mode of operations)

Safety integrity level (SIL)	Target frequency of dangerous failures to perform the safety instrumented function (per hour)
4	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-6}$ to $< 10^{-5}$

A detail list of activities during the SIS life cycle is presented in the Appendix I. The further detail about the procedure to determine the safety integrity level with guidelines can be found in the International Standard (IEC 61511, 2003).

In this scope of work, SIL allocation and SIL verification are discussed among all the activities during the life cycle of a SIS.

SIL allocation

The SIL allocation procedure is composed of following main steps, however these steps can vary mainly depending upon company's internal procedures and practices:

- Tolerable risk definition: the tolerable risk level must be defined in order to calibrate the allocation method by using ALARP approach;
- SIL allocation team: SIL allocation is performed by a team in which process, instrumentation and HSE specialists are involved;
- SIF identification: The SIF to be analysed are identified from C&E matrices and P&ID. Every SIF is characterized by a “design intent” (the hazard that the SIF has to prevent or mitigate), a “demand scenario” (conditions, deviations that determine the SIF intervention) and “consequences” (consequences of scenario arisen from the failure of SIF);
- SIL classification (unrevealed failure): Failure on demand of SIF is classified. The main SIL allocation methods are the “risk graph” (qualitative method), LOPA (semi-quantitative method) and “fault tree” (quantitative method);
- Revealed failure classification: This classification is performed to evaluate the loop robustness against any possible spurious interventions. This classification uses the economic criteria in which “cost of robustness” (the cost to make the system robust against spurious intervention), “cost of spurious trip” (cost associated to the trip of the system) and the “rate” (estimated spurious intervention frequency) are compared.

Generally, SIS loops have many final elements. In this case during the SIL allocation phase (independent of assessment methods) it is important to prioritize the final elements (final elements critical for process safety). This prioritization can be achieved by evaluating the consequences of failure on demand of the whole SIS loop compared to consequences of failure on demand of each of the final elements of SIS.

SIL verification

During the SIL verification, each SIS loop is analysed to ensure that the calculated SIL level satisfies the safety integrity level requirements assessed during the SIL classification.

Each loop is analysed considering the system’s architecture, relevant reliability data and test intervals for the elements making up the safety function. On the basis of this information, the overall PFD (Probability of Failure on Demand) is calculated by Fault Tree Analysis, and compared with the target SIL specifications. The SIL verification study is performed in conformance with the (IEC 61511, 2003) and (IEC 61508, 1997).

The human actions could be in the form of maintenance (i.e. proof test) of the SIS in the operational phase and also sometimes operator/ human could also be a part of the SIS. In a SIS, operator's interface is by which information is communicated between a human operator (s) and a SIS. For example, indicating lights, push-buttons, horns, alarms etc require a human intervention. The operator interface is sometimes referred to as the Human-Machine Interface (HMI), (IEC 61511, 2003). However, fault avoidance procedures can also be established in an organization for the maintenance of the SIS, giving the criticality of the SIS to ensure the safety of operations.

The International Standard (IEC 61511, 2003) also provides the steps to be taken mostly by the end-users to conform SIS to the International Standards, clauses 5 through 19. While, clause 5 shows the management steps to be taken to ensure that functional safety objectives have been met. Moreover, Standard also highlight that the "*persons, departments or organizations involved in the safety life-cycle activities shall be competent to carry out the activities for which they ate accountable*". The minimum criteria to assess the competency of a person, department, organization or other units involved in the safety life-cycle activities are as follows:

- Engineering knowledge, training and experience appropriate to the process application;
- Engineering knowledge, training and experience appropriate to the applicable technology used (e.g. electrical, electronic or programmable electronics);
- Engineering knowledge, training and experience appropriate to the sensors and final elements;
- Safety engineering knowledge (e.g. process safety analysis);
- Knowledge of the legal and safety regulatory requirements;
- Adequate management and leaderships skills appropriate to their role in safety-life cycle activities;
- Understating of the potential consequences of an event;
- The safety integrity level of the safety instrumented functions;
- The novelty and complexity of the application and the technology.

The common cause failures are also need to be considered during the SIL verification. The International Standard provides following list of common cause failures that should be considered (IEC 61511, 2003):

- Plugging of instrumentation connections and impulse lead lines;
- Corrosion and erosion;

- Hardware failure due to the environment causes;
- Software failure;
- Power supplies and power sources;
- Human error.

Therefore, human factors/ errors are one of the common cause failures that could influence the performance of a SIF and can lead to a hazardous situation as it has also been seen during the past accident analysis. Meanwhile, human capabilities and limitations should also be considered during the design and engineering of a SIS related to maintenance tasks performed by the operator. The International Standard says that "*The design of all human-machine interface shall follow good human factors practices and shall accommodate the likely level of training and awareness that operator should receive"* (IEC 61511, 2003), p. 45. Therefore, during the design and engineering of a SIS it should be ensured that the relevant training and procedures for operator are also in place. These aspects can be assessed during the SIL verification, however lack of existing knowledge about this field pose an enormous challenge to materialize these aspects practically.

3.1.5 Layer of Protection Analysis (LOPA)

During a LOPA, it is determined if there are sufficient measures to prevent or mitigate a risk. However, the main use of the LOPA is to provide the specification of Independent Protection Layers (IPLs) and SIL (SIL levels) for the Safety Instrumented Systems (SIS) as described in the Standard (IEC 61511, 2003) and is also mentioned in the Standard (IEC 31010, 2009). The LOPA can also be used to allocate risk reduction resources effectively by analyzing the risk reduction provided by the IPLs (IEC 31010, 2009). Therefore, a LOPA can help to identify the most critical layers to spend further resources and time. The Figure 2 depicts typical layers that are used in the process industry to reduce the risk.

The different types and number of layer can be applied against different scenarios depending upon the likelihood of an events and severity of relevant consequences. However, more layers can possibility add more complexity into the operations and difficult to maintain them during the operational stage of a project. Therefore, use of layers should carefully be selected against only credible scenarios.

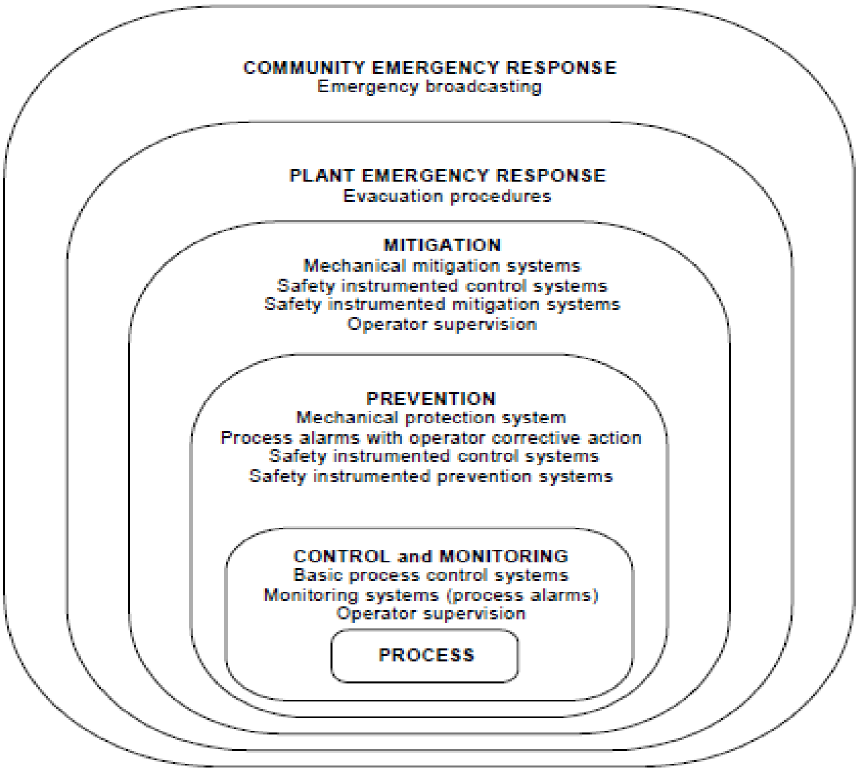

COMMUNITY EMERGENCY RESPONSE
Emergency broadcasting
PLANT EMERGENCY RESPONSE
Evacuation procedures
MITIGATION
Mechanical mitigation systems
Safety instrumented control systems
Safety instrumented mitigation systems
Operator supervision
PREVENTION
Mechanical protection system
Process alarms with operator corrective action
Safety instrumented control systems
Safety instrumented prevention systems
CONTROL and MONITORING
Basic process control systems
Monitoring systems (process alarms)
Operator supervision
PROCESS

Figure 2. Risk reduction method, adapted from (IEC 61511, 2003), p. 10.

As mentioned in the International Standard (IEC 61511, 2003), p. 47, that information required for a LOPA is usually collected and developed during a HAZOP study. Therefore, LOPA can easily be applied followed by a HAZOP study as a correspondence can be seen in the Table 7.

Table 7: HAZOP data for LOPA, adapted from (IEC 61511, 2003), p. 47

LOPA required information	HAZOP developed information
Impact event	Consequences
Severity level	Consequences severity
Initiating cause	Cause
Initiating likelihood	Cause frequency
Protection layers	Existing safeguards
Required additional mitigation	Recommended new safeguards

While, during a LOPA credits based on PFD_{avg} can be claimed for different layers. Therefore, a LOPA can provide an estimate if the existing layers are enough and also the integrity of SIF, if any.

Table 8: Typical protection layers PFDs, adapted from (IEC 61511, 2003), p. 49

Protection layer	PFD_{avg}
Control loop	$1{,}00\times10^{-1}$
Human performance (trained, no stress)	$1{,}00\times10^{-2}$ to $1{,}00\times10^{-4}$
Human performance (under stress)	$5{,}00\times10^{-1}$ to $1{,}00\times10^{0}$
Operator response to alarms	$1{,}00\times10^{-1}$
Vessel pressure rating above maximum challenge from internal and external pressure sources	$1{,}00\times10^{-4}$ or better, if vessel integrity is maintained

In order to claim the credits from the human/ operator layer, it is also important to consider the PSF that can affect the reliability of the human/ operator. The Human Error Probability (HEP) (in this case PFD) and effect of PSF to modify the HEPs have been obtained in this work and are highlighted in the section 6.

It has identified that LOPA have certain advantages as compared to the conventional QRA mainly because LOPA can consider wider range of issues as followed (Gowland, 2006):

Initiating events such as:

- Human error;
- Procedural failures;

and barrier performance such as

- Operator response;
- Management systems;

Therefore, a concept similar to LOPA can provide an easy estimate about the severity of an event and distribution of safety layers according to the severity. Hence, LOPA can be beneficial to distribute the available resources (i.e. safety layers) according to the failure criticality.

3.2 Review of existing human and organizational factors databases/ methods

It has been reported by (Alvarenga et al., 2014), that Human Reliability Analysis (HRA) in general lacks a human reliability database. The similar aspects are also highlighted by the (Sträter and Bubb, 1999). While, (Mannan, 2012) has pointed out that large number of human error data points are collected from the nuclear industry. Since, scope of this work is the chemical process industry, therefore it is important to analyse the human factors database and subsequently human reliability methods specifically for the chemical process industry.

A number of human reliability databases are already available which can provide numerical estimates of Human Error Probabilities (HEP) and associated Performance Shaping Factors (PSF). Furthermore, some of these databases are also complemented with an associated methodology to perform the human factor assessment. Meanwhile, there are number of Human Factor (HF) methods that are qualitative, therefore these methods not require any database. The Human Reliability Assessment (HRA) involves the use of qualitative and quantitative methods to assess the human contribution to the risk, (Bell and Holroyd, 2009). In a report by HSE (Health and Safety Executive), a review of 72 potential HRA methods can be found, out of which 17 methods have been identified that are potentially useful for major hazards directorates (Bell and Holroyd, 2009). These methods are also listed in the Table 9.

The further detail about the safety methods, databases or models can be found in (Everdij and Blom, 2013). The (Bell and Holroyd, 2009) have highlighted, that 2nd generation methods are generally considered to be under development but they can provide some further insight into human reliability issues and challenges.

However, the Table 10 lists the selected human reliability methods which will be discuss in detail in this scope of work. Some of the concepts from these methods that can be applicable are used during the development of new methodology (i.e. MEDIA) in this work. These human reliability methods have been selected after concluding a preliminary literature review and based on amount of information required to quantify the human factors assessment. It can be seen from the Table 10 that majority of methods developed in chemical process industry are qualitative compare to the nuclear industry. The qualitative methods can lessen the required information for assessment compare to quantitative methods but at the same time qualitative methods have the tendency to add more uncertainty due to subjective interpretation of assessment and results.

Table 9: List of HRA tools, adapted from (Bell and Holroyd, 2009), p. 6.

		Tool	Domain
Publicly available	1st generation	Techniques for Human Error Rate Prediction (THERP)	Nuclear with wider application
		Accident Initiation and Progression Analysis (ASEP)	Nuclear
		Human Error Assessment and Reduction Techniques (HEART)	Generic
		Simplified Plant Analysis Risk Human Reliability Assessment (SPAR-H)	Nuclear with wider application
	2nd gen.	A Technique for Human Error Analysis (ATHEANA)	Nuclear with wider application
		Cognitive Reliability and Error Analysis Method (CREAM)	Nuclear with wider application
	Expert judgment	Absolute Probability Judgment (APJ)	Generic
		Paired Comparison (PC)	Generic
		Success likelihood index methodology, multi-attribute utility decomposition (SLIM-MAUD)	Nuclear with wider application
Not Publicly available	1st gen.	Human Reliability Management System (HRMS)	Nuclear
		Justified Human Error Data Information (JHEDI)	Nuclear
		INTENT	Nuclear
	2nd gen.	Connectionism Assessment of Human Reliability (CAHR)	Generic
		Commission Errors Search and Assessment (CESA)	Nuclear
		Conclusion from occurrences by descriptions of actions (CODA)	Nuclear
		Method d’Evaluation de la Realisation des Missions Operateur pour la Surete (MERMOS)	Nuclear
	3rd gen.	Nuclear Actions Reliability Assessment (NARA)	Nuclear

Since, it was observed that establishments generally lack the information that is required to perform in-detail human factors analysis especially when a project is in the design phase. Therefore, emphasis is given to those methods that have a potential to generate human factors estimates balancing against the required information for the assessment. However, whenever enough information and resources are available it is recommended to carry out in-detail human factors assessment including cognitive, PSFs and HMI aspects etc.

Table 10: Review of the human factors database/methods

Methods	Domain	Qualitative/ Quantitative	References
Tecnica Emiprica Stima Errori Operatori (TESEO)	Chemical	Quantitative	(Bello and Colombari, 1980)
Predictive Human Error Analysis (PHEA)	Chemical	Qualitative	(Embrey, 1992) cited in (Baber and Stanton, 1996)
System for Predictive Error Analysis and Reduction (SPEAR)	Chemical	Qualitative	(CCPS, 1994) cited in (Mannan, 2012) and (Stanton et al., 2005)
Techniques for Human Error Rate Prediction (THERP)	Nuclear	Quantitative	(Swain and Guttmann, 1983)
Human Error Analysis and Reduction Technique (HEART)	Nuclear	Quantitative	(Williams, 1986)
Standardized Plant Analysis Risk-Human Reliability Analysis (SPAR-H)	Nuclear	Quantitative	(Gertman et al., 2005)
Cognitive Reliability and Error Analysis Method (CREAM)	Nuclear	Quantitative	(Hollnagel, 1993)
Connectionism Assessment of Human Reliability (CAHR)	Nuclear	Quantitative	(Sträter, 2000)

3.2.1 Tecnica Emiprica Stima Errori Operatori (TESEO)

The Tecnica Emiprica Stima Errori Operatori (TESEO) was developed mainly for the control room operator to quantify the reliability based on five parameters. This model describes a plant control-room operator’s failure probability as a multiplicative function of following parameters, (Bello and Colombari, 1980):

- The type of activity to be carried out (K_1);
- The time available to carry out this activity (K_2);
- The human operator's characteristics (K_3);
- The operator emotional state (K_4);
- The environmental ergonomics characteristic (K_5);

The Table 11 shows the proposed HEPs for control room operator in this method for each of the five aforementioned parameters. However, full scale validation of this data has not yet obtained but some modest estimation have been made as mentioned by (Bello and Colombari, 1980). Furthermore, this work also highlighted the possible approached to quantify the unreliability of an operator as follows:

- Data from experience of operations in real plants (field data);
- Data from plant simulators;
- Data from laboratory studies;
- Data collected by interviewing "experts".

The (Bello and Colombari, 1980) have argued that field data can provide the more reliable estimates compare to rest of the alternatives. However, there are numbers of challenges that have to be faced to collect data from operational experience. In the scope of present work, data has been collected from past accidents (i.e. closet to the field data) in order to provide estimates for the human reliability.

Table 11: Failure probability of control room operator, adapted from (Bello and Colombari, 1980).

Activity's topologic factors		Temporary stress factor for routine activities	
Type of activity	K_1	Time available	K_2
Simple, routine	0,001	2	10
Requiring attention, routine	0,01	10	1
Not routine	0,1	20	0,5
Operator's typological factors			
Operator's topologic factor	K_3	State of anxiety	K_4
Carefully selected, expert, well trained	0,5	Situation of grave emergency	3
Average knowledge and	1	Situation of potential	2

training		emergency	
Little knowledge, poorly trained	3	Normal situation	1
Environmental, ergonomics factors			
Ergonomics factors	K_5		
Excellent microclimate, excellent interface with plant	0,7		
Good microclimate, good interface with the plant	1		
Discrete microclimate, discrete interface with plant	3		
Discrete microclimate, poor interface with plant	7		
Worst microclimate, poor interface with plant	10		

In the TESEO method the Human Unreliability (HU) or probability of an error is estimated by using equation the Eq. 1.

$$\mathrm{HU} = \mathrm{K}_1 \cdot \mathrm{K}_2 \cdot \mathrm{K}_3 \cdot \mathrm{K}_4 \cdot \mathrm{K}_5 \qquad \text{Eq. 1}$$

Whenever, the product gives a value above unity, it is assumed that HU = 1 i.e. the operator’s probability of carrying out the activity successfully are considered to be nil.

However, theoretical background of this method has been questioned and not considered to be accurate by some reviewers as mentioned in the (Bell and Holroyd, 2009).

3.2.2 Predictive Human Error Analysis (PHEA)

The Predictive Human Error Analysis (PHEA) method adapted the error classification against the behavioural taxonomy. According to (Embrey, 1992), the PHEA is a method by which specific errors associated with tasks are identified. In this method a checklist provides the information about the error classification as also shown in the Table 12. The validation of this error classification has been performed by Murgatroyd and Tait (1987), who have found that

PHEA error classification related to the equipment calibration tasks account for about 98% of accidents over a 5-years period and is reported in the (Mannan, 2012).

Table 12: PHEA error classification, adapted from (Embrey, 1992)

Planning Errors: P1: Incorrect plan executed P2: Correct but incomplete plan executed P3: Correct plan executed too soon / too late P4: Correct plan executed in wrong order
Operation Errors: O1: Operation too long/ short O2: Operation mistimed O3: Operation in wrong direction O4: Operation too li ttle/ too much O5: Misalign O6: Right operation on wrong object O7: Wrong operation on right object O8: Operation mistimed O9: Operaion incomplete
Checking Errors: C1: Check omitted C2: Check incomplete C3: Right action on wrong object C4: Wrong check on right object C5: Check mistimed
Retrieval Errors: R1: Information not obtained R2: Wrong information obtained R3: Information retrieval incomplete

Communication Errors: T1: Information not communicated T2: Wrong information communicated T3: information communication incomplete
Selection Errors: S1: Selection omitted S2: Wrong selection made

Furthermore, an application of PHEA method is also presented by the (Embrey, 1992) with potential error reduction recommendations (i.e. Procedure, training, equipment etc). This error classification can help an analyst to identify the potentially critical errors relevant to an action and take precautionary measure, if required.

The PHEA method has five principle stages as reported in the (Baber and Stanton, 1996) and illustrated in the Figure 3. The screening of errors (i.e. whether an error is relevant) is also performed in the error identification stage. Therefore, only those error classes are considered for further analysis which are relevant.

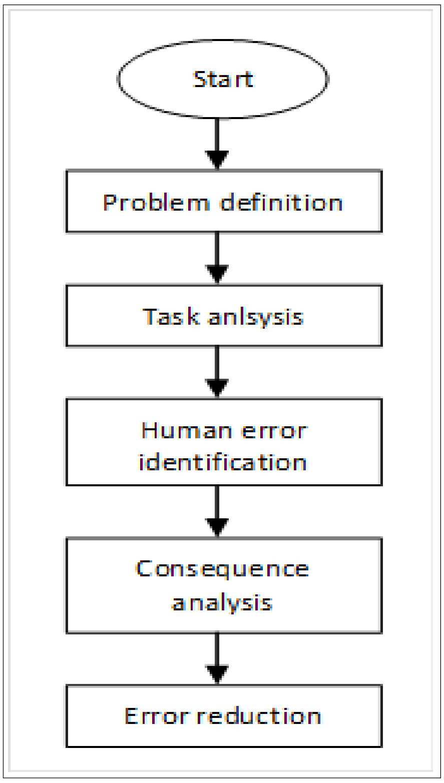


Figure 3. PHEA Flowchart, adapted from (Baber and Stanton, 1996).

3.2.3 System for Predictive Error Analysis and Reduction (SPEAR)

The System for Predictive Error Analysis and Reduction (SPEAR) was developed by the Centre for Chemical Process Safety for use in the American chemical process industry as reported in the (Stanton et al., 2005). The SPEAR method also considers the action classes similar to the PHEA, and consists of following main steps (Mannan, 2012):

- Task analysis;
- Performance shaping factors;
- Consequence analysis;

- Error reduction analysis.

Using a subjective judgment, the analyst classifies each step of an action into one the following classes used in the SPEAR taxonomy:

- Action;
- Retrieval;
- Check;
- Selection;
- Transmission.

Hence, after the identification of the action type. The available information and analyst's domain expertise can be used to determine if the relevant errors are credible or not. The next step is to determine if recovery is possible or not and consequence associated with the error. In the SPEAR method, consequence are not only determined from failure to perform the task but also of consequences of any side-effect that may occur if the tasks is not executed properly (Mannan, 2012).

However, as SPEAR is a structured approach to the human error identification by considering the PSF. This method becomes labours and time consuming for complex and large systems, (Stanton et al., 2005). At the same time, this method also lacks the cognitive component of the error.

3.2.4 Techniques for Human Error Rate Prediction (THERP)

The Techniques for Human Error Rate Prediction (THERP) was reported by the (Swain and Guttmann, 1983) was the first systemic human reliability method especially for the Nuclear Power Plants (NPP). The THERP handbook presents methods, models and estimated HEPs to assist an analyst to make qualitative and qualitative assessment of human reliability.

The key tasks to complete the quantification process are described by the (Kirwan, 1996) and are reported in the (Bell and Holroyd, 2009):

- Decomposition of tasks into elements;
- Assignments of nominal HEP to each element;
- Determination of effect of PSF on each element;
- Calculation of effect of dependence between tasks;
- Modelling in an HRA event tree;
- Quantification of total task HEP;

During the first step, a task is break down into its constitute elements according to the THERP taxonomy. The assignments of the nominal HEPs is carried out according to Chapter 20 of the THERP handbook. The Table 13 illustrates the THERP tables that can be used to assign the nominal HEP against the selected taxonomy. However, problems can arise when task elements don't appear to be representative from any of the tables as argued by the (Kirwan, 1996). The effect of the PSFs on the HEPs are considered by using multiplier to the nominal HEPs. This aspect of determining the effect of the PSFs on the nominal HEPs is relatively less structured in THERP as also highlighted by the (Kirwan, 1996). This aspect of determining the effect of PSFs is highly subjective as based on the analyst and this aspect might require some further improvement.

The THERP provides five levels of dependency, which have very high inter-relation. A failure to model dependency can have dramatic effects on the overall HEP. The last two steps of developing a HRA event tress and quantification of total HEP are relatively straightforward tasks. In order to develop a HRA event tree elements of a task are divided into failure and successful outcome of the tasks and a tree is developed according to decomposition of task. The Figure 4 represents an event tree for a series and parallel system and also relevant calculations for probability of success /failure of task. A validation study of THERP model has been provided by (Kirwan et al., 1997) and recently another attempt was made by (Shirley et al., 2015)

As highlighted by Swain and Guttmann themselves that real HEP is difficult to predict due to its variability. Each person/ operator has a tendency of variability and this variability also exists among the different persons/ operators. There are number of internal and external Performance Shaping Factors (PSFs) which indicate the behaviour/ response of a person/ operator. However, despite this variability it is possible to predict the reliability of a person/ operator with a varying degree of uncertainty. This uncertainty will be smaller while predicting behaviour of a person/ operator for routine tasks and will be higher while predicting the behaviour for abnormal activities.

In the THERP database, HEPs are provided using the lognormal distributions and single points are the median points of distribution. The range of error factors is considered to include the 90% of the HEPs in distribution. However, if this range is questionable then analyst can use another range by providing relevant justifications.

The THERP handbook also justify the selection of lognormal distribution to provides HEPs. Since, it is believed that performance of skilled persons tends to bunch up towards the low HEPs on a distribution of HEPs and response time is main parameters that determined the performance of a skilled person. Due to lack of sufficient data to propose an exact distribution, Swain and Guttmann argued that lognormal distribution can provide the best fit as shown in the Figure 5. However, it is also hypothesised that a "SD (Standard Deviation) = 0.42" would provide a best fit for the NPP operations. But, for tasks performed under high stress the entire distribution will be shifted to the right and may be skewed to the left rather than the right. This phenomenon ensures the factual condition that under high stress majority of actions tend to fail.

Table 13: THERP tables for HEPs adapted from (Swain and Guttmann, 1983)

Screening	Diagnosis (Table 20.1) Rule-based actions (Table 20.2)
Diagnosis	Nominal diagnosis (Table 20.3) Post event CR staffing (Table 20.4)
Error of omission	Written materials mandated Preparation (Table 20.5) Administrative control (Table 20.6) Procedural items (Table 20.7) No written materials Administrative control (Table 20.6) Oral instruction items (Table 20.8)
Error of commission	Displays Displays selection (Table 20.9) Read/ record quantitative (Table 20.10) Check-read quantitative (Table 20.11) Control & MOV selection & use (Table 20.12) Locally operated Valves Valve selection (Table 20.13) Stuck valve detection (Table 20.14)
PSFs	Tagging levels (Table 20.15) Stress/ experiences (Table 20.16)

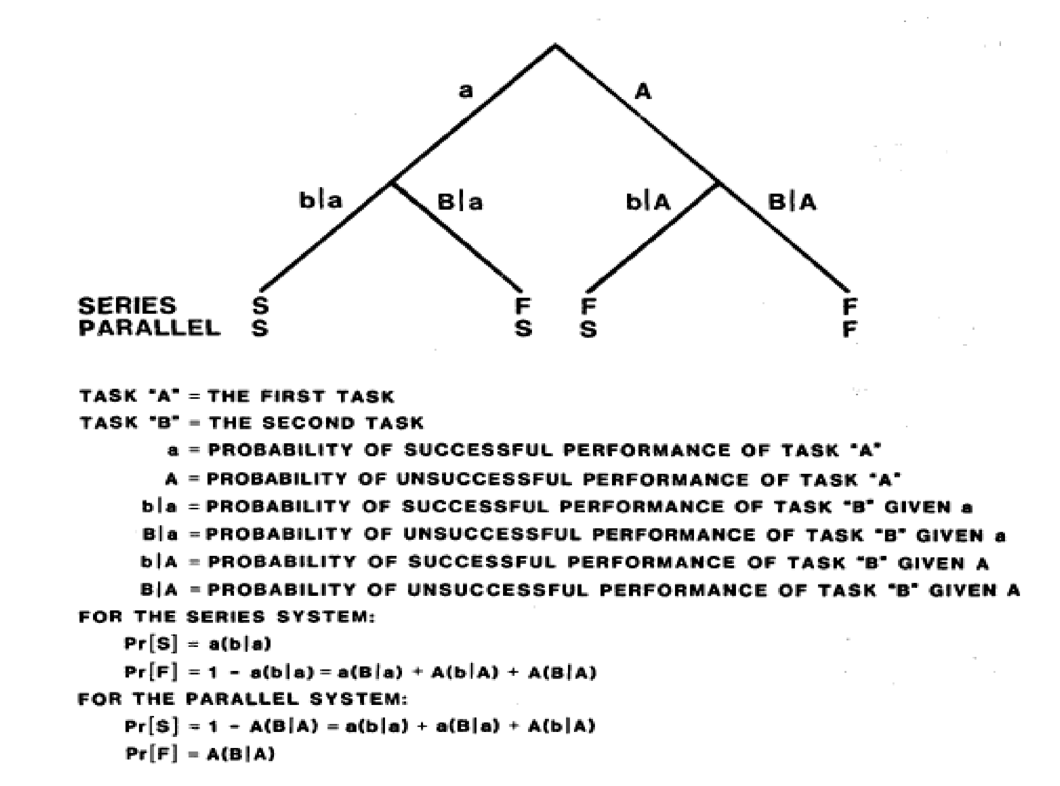
	Dependence (Table 20.17, 20.18, 20.19) Other PSFs
Uncertainty bounds	Estimated UCBs (Table 20.20) Conditional HEPs and UCBs (Table 20.21)
Recovery factors	Errors by checker (Table 20.22) Annunciated cues (Table 20.23, 20.24) Control room scanning (Table 20.25, 20.26) Basic walk-around inspection (Table 20.27)

As can be seen from the Figure 5, HEP distribution also consider the uncertainty bounds (UCBs). These uncertainty bounds of HEPs account for both the imperfect knowledge and also the stochastic variability. The ratio of the upper to the lower bounds is the range ratio. The error factor (EF) corresponding to the HEPs is calculated by following equation, Eq. 2.

$$\text{Error factor} = \sqrt{\frac{\text{Upper uncertainty bound}}{\text{Lower uncertainty bound}}} \qquad \text{Eq. 2}$$

Furthermore, THERP also proposes to use large EFs when HEPs < 0.001 to reflect the greater uncertainty associated with the infrequent occurring of the events. While, HEPs in range of 10^{-3} - 10^{-2} generally apply to routine tasks involving rule-based behaviour.

The THERP also provides general guidelines to assign the UCBs according to HEPs and relevant conditions as also shown in the Table 14 for the experienced personnel. It can be seen that higher EF values are proposed when HEPs are low, in order to account for the uncertainty due to infrequent events. Similarly, the EFs are also increased with the increase of stress level of the operator.



TASK "A" = THE FIRST TASK
TASK "B" = THE SECOND TASK
a = PROBABILITY OF SUCCESSFUL PERFORMANCE OF TASK "A"
A = PROBABILITY OF UNSUCCESSFUL PERFORMANCE OF TASK "A"
b|a = PROBABILITY OF SUCCESSFUL PERFORMANCE OF TASK "B" GIVEN a
B|a = PROBABILITY OF UNSUCCESSFUL PERFORMANCE OF TASK "B" GIVEN a
b|A = PROBABILITY OF SUCCESSFUL PERFORMANCE OF TASK "B" GIVEN A
B|A = PROBABILITY OF UNSUCCESSFUL PERFORMANCE OF TASK "B" GIVEN A

FOR THE SERIES SYSTEM:

$Pr[S] = a(b|a)$

$Pr[F] = 1 - a(b|a) = a(B|a) + A(b|A) + A(B|A)$

FOR THE PARALLEL SYSTEM:

$Pr[S] = 1 - A(B|A) = a(b|a) + a(B|a) + A(b|A)$

$Pr[F] = A(B|A)$

Figure 4. HRA event tree for series and parallel systems, adapted from (Swain and Guttmann, 1983)

Given the fact that the exact values of these EFs are difficult to obtain, these EF can provide a comparative indication about the uncertainly among different actions types and operating conditions.

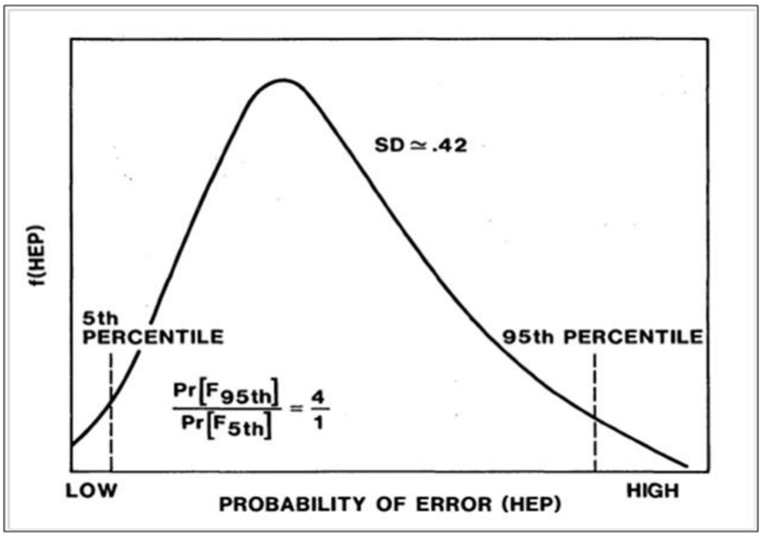


Figure 5. Hypothesized lognormal probability density function of THERP HEPs, adapted from (Swain and Guttmann, 1983)

During calculations, the simplest way to incorporate these UCBs is to use the most conservative estimates of the spread between the upper and lower bounds.

The THERP is a well-used method in practice not only in NPP but also in chemical process industry. However, there are some aspects that are highlighted by the (Bell and Holroyd, 2009) among others, that need to be improved:

- THERP does not offer enough guidance on modelling scenarios and the impact of PSFs performance;
- THERP level of detail can be excessive for some assessment. As this is certainly the case at lease for chemical process industry.

It was observed on certain occasions that companies are unable to provide detailed information about their operation, especially when a project is still in the design phase. In this case, assessment based on THERP model has to be based on certain assumptions, that can add more uncertainty to the analysis.

Table 14: General guidelines for estimating uncertainty bounds for HEPs, adapted from (Swain and Guttmann, 1983)

Task and HEP guidelines	Error factor
A: Step by step procedures, routine, optimal stress level	
Estimated HEP < 0.001	10
Estimated HEP 0.001 to 0.01	3
Estimated HEP > 0.01	5
B: Step by step procedures, non-routine, moderate stress level	
Estimated HEP < 0.001	10
Estimated HEP > 0.001	5
C: Dynamic interplay between operator and system indication, routine, optimal stress level	
Estimated HEP < 0.001	10
Estimated HEP > 0.001	5
D: Dynamic interplay between operator and system indication, non-routine, moderate stress level	10
E: Task under high stress, e.g. large LOCA; conditions in which the status of shaping factors is not perfectly clear; conditions in which the initial operator responses have proved to be inadequate and sever time pressure is felt.	5

Apart from that, THERP was developed mainly for nuclear power plants. A study is also required which can indicate its validation / adjustments for chemical process industry based on the operational experience obtained within the chemical process industry.

3.2.5 Human Error Analysis and Reduction Technique (HEART)

In the HEART, as described by the (Williams, 1986), the HEP of a task is treated as a function of type of task and relevant Error Producing Conditions (EPCs) also called PSFs as mentioned in the (Mannan, 2012). The HEART method is relatively simple and quick to estimate the human reliability as compare to the THERP.

The main steps of HEART are as follows, as mentioned in (Bell and Holroyd, 2009):

- The basic human reliability is dependent upon the generic nature of the tasks to be performed;
- In "perfect" conditions, this level of reliability will tend to be achieved consistently with a given nominal likelihood within probabilistic limits;
- Given that these perfect conditions do not exist in all circumstances, the human reliability predicted may degrade as a function of the extent to which identified Error Producing Conditions (EPCs) might apply.

In the HEART method, there are 9 generic task types, each with an associated nominal human error probability and 38 error producing conditions that may affect the task reliability. The nominal human error probability can be modified by a multiplier defined for each of the error producing conditions. The Table 15 illustrates the HEART generic tasks and associated NHEPs as proposed by (Williams, 1986). The probability percentiles are calculated by assuming the log normal distribution for the HEPs.

In the HERAT method, HEP is calculated from the NHEP by considering the effect of the EPCs. The effect of the EPCs is calculated by estimating two terms as shown in Eq. 3 also called assessed impact of EPCs. The multipliers against 38 EPC are also identified in the HEART. The assessed proportion of effect is an estimation of the impact of each EPC on the task and this effect value varies between 0 to 1.

The HERAT assesses the impact as follows in the Eq. 3:

$$\text{Assessed impact} = \big((\text{Mutiplier - 1}) \ \cdot \text{Assessed proportion of effect}\big) + 1 \qquad \text{Eq. 3}$$

Whereas:

Assessed proportion of effect ≈ 0 - 1

Table 15: Classification of generic HEART tasks and associated unreliability estimates adapted from (Williams, 1986) cited in (Mannan, 2012)

Generic task	Proposed NHEP (5th-95th percentile boundaries)
A: Totally unfamiliar, performed at speed with no real idea of likely consequences	0,55 (0,035 – 0,97)
B: Shift or restore system to a new or original state on a single attempt without supervision or procedures	0,26 (0,14 – 0,42)
C: Complex task requiring high level of comprehensive and skill	0,16 (0,12 – 0,28)
D: Fairly simple task performed rapidly or given scant attention	0,09 (0,06 – 0,13)
E: Routine, highly practiced, rapid task involving relatively low level of skill	0,02 (0,007 -0,045)
F: Restore or shift a system to original or new state following procedures, with some checking	0,003 (0,0008 – 0,007)
G: Completely familiar, well-designed , highly practiced, routine task occurring several times per hour, performed to highest possible standards by highly motivated, highly trained and experienced person, totally aware of implications of failure, which time to correct potential errors, but without the benefit of significant job aids	0,0004 (0,00008 – 0,009)
H: Respond correctly to system command even when there is an augmented or automated supervisory system providing accurate interpretation of system stage	0,00002 (0,000006 – 0,00009)
M: Miscellaneous task for which no description can be found (Nominal 5th – 95th percentile data spread were chosen on the basis of experience suggesting log normality).	0,03 (0,008 – 0,11)

While, the HEP can be calculated by multiplication of nominal HEP and assessed impact of each of identified EPCs as also highlighted by the Eq. 4.

$$\mathrm{HEP} = \mathrm{Nominla\ HEP}\ \times \mathrm{Assess\ impact\ 1}\ \times \mathrm{Asssessed\ impact\ 2}\ \times \mathrm{etc} \qquad \text{Eq. 4}$$

In order to check the variability of the assessed impact, calculations are performed against the assessed proportion for EPCs using Eq. 3. A linear relation has been obtained for all the EPCs for their assessed proportion scale (i.e. 0 to 1). So, it can be concluded that in HEART method, the assessed impact of EPCs varies linearly against the assessed proportion values. This is also a theoretical explanation of Eq. 3. If the assessed proportion of a EPC is zero, in this case the value of the assessed impact become one and the total HEP becomes equal to the NHEP. While, in cases when assessed proportion has any values except zero, then assessed impact also increase with a possible maximum value equal to the EPC's multiplier value.

Although, a simple linear relation between EPCs and their impact on the NEHP is proposed by HEART but considering lack of general data for quantification. This type of estimations can be justifiable since it can provide some initial estimates about the HEPs.

The HEART has been designed as a practical and easy to use method. It was one of the principal techniques used in the quantitative risk assessment as indicated by the (Mannan, 2012). The HEART can also be used in number of domains like nuclear, chemical, aviation, rail and medical as also indicated by (Bell and Holroyd, 2009).

The main criticism which received by HEART is that the EPCs data has not been fully released and validated. Furthermore, assessed proportion of EPCs defined solely based on expert's judgment, so it can be highly subjective and sensitive towards the HEP calculations. The relevant checklists to assess the EPCs can help to mitigate this uncertainty by providing the same ground to assessment procedures that are carried out by different analysts.

3.2.6 Standardized Plant Analysis Risk-Human Reliability Analysis (SPAR-H)

The SPAR-H method was developed for the US Nuclear Regulatory Commission by Idaho National Laboratory and is reported by the (Gertman et al., 2005). During the SPAR-H method following main steps should be followed as identified by the (Gertman et al., 2005):

- Decompose probability into contribution from diagnose failures and actions failures;
- Accounts for the context associated with human failure events (HFEs) by using performance shaping factors and dependency assignment;
- Assign appropriate values of PSFs to pre-defined the base case of HEPs;
- Use of beta distribution for uncertainty analysis;
- Use the proposed worksheets to ensure the analyst's consistency.

In the SPAR-H method, two main types of actions are identified:

- Action
- Diagnostic

The examples of action task include operating equipment, performing line-ups, starting equipment, conducting calibration and other activities performed during the course of the following plant procedures or work orders. While, diagnostic tasks consider the reliance on knowledge and experience to understand existing conditions. The base rate (i.e. HEP) for action and diagnostic activity types are defined as 1× 10^{-3} and 1× $10^{-2,}$ respectively.

In the SPAR-H method, following eight types of PSFs are identified, which were considered to have an influence on the human reliability:

- Available time;
- Stress and stressors;
- Experience and training;
- Complexity;
- Ergonomics (including human-machine interface);
- Procedures;
- Fitness for duty;
- Work processes.

When applying the basic SPAR-H model, three out of eight PSFs are evaluated: time available, stress /stressors and complexity while rest of five PSFs are rated nominally because they are related to the event, plant or personal-specific. The Appendix II lists the SPAR-H PSFs levels and the associated multipliers along with recommended multiplier from HEART, CREAM, ASEP and THERP models. But, this comparison cannot be an absolute because multipliers' final effect on the nominal HEP is determined by relevant equations in each of the method, that varies among methods. However, it can provide a relevant idea about the effect of PSFs when apply one of the method. Since, evaluation steps and relevant criteria varies among methods. Therefore, it is highly recommended to use just one method in whole plant or a facility.

The SPAR-H also accounts for the +ve influence of the PSFs on human reliability as defined by its influencing levels. This model can be used retrospective as well as in prospective manner.

In order to account for the effect of PSFs on human reliability, a different approach has been used in SPAR-H method compared to its predecessors. In most of the previous methods, multiplicative models have been used to modify the nominal human error probability. Although, practically multiplicative models can provide the similar results like THERP and HEART models but strictly in mathematical terms the direct application (i.e. HEP = NHEP

×PSF) of multiplicative models is only approximately correct as argued in the (OECD, 1998). The following main reasons have been identified for multiplicative models:

- In Multiplicative models, a scalar (i.e. PSF value) is to multiply a probability and the value of HEP cannot be greater than 1. If PSFs values are greater than 1 then multiplicative models can provide a HEP greater than 1 for higher values of NHEPs and PSFs.

Therefore, Given the aforementioned challenge, the SPAR-H method propose a new model to determine the HEP as also anticipated by the (OECD, 1998) and is also shown in the Eq. 5, in special cases when PSFs have -ve impact on the HEP (Gertman et al., 2005).

$$\mathrm{HEP} = \frac{\mathrm{NHEP} \cdot \mathrm{PSF}_{\mathrm{Composite}}}{\mathrm{NHEP} \cdot \left(\mathrm{PSF}_{\mathrm{Composite}} - 1\right) + 1} \qquad \text{Eq. 5}$$

Whereas:

PSF_{Composite} is obtained by product of analysts rating of all PSFs contained in the SPAR-H worksheet.

The SPAR-H model provides some further insight into the human factors assessment and to understand the effect of the PSFs on the human reliability. At the same time, this model is also a simple model that can be adopted easily, (Bell and Holroyd, 2009). However, on the other hand, the degree of resolution of the PSFs may be inadequate for a detailed analysis.

In the SPAR-H method, the PSFs definitions, levels and PSF's multipliers are questionable as also pointed out by the (Laumann and Rasmussen, 2015), who have tried to adjust the SPAR-H PSFs levels for the chemical process industry application based on expert's opinion.

3.2.7 Cognitive Reliability and Error Analysis Method (CREAM)

The Cognitive Reliability and Error Analysis Method (CREAM) has been developed by the (Hollnagel, 1993) and was reviewed by the (Bell and Holroyd, 2009). The CREAM model uses an advanced cognitive concepts developed primarily for the nuclear plants. In this model a distinction is made among competence and control that is based upon Hollnagel's COCOM (Contextual control) model:

- Competence includes a person's skills and knowledge;

- Control is reviewed as running along a continuum from a position where the individual has little/ no control to where they have complete control.

In the CREAM model, genotypes (i.e. causes to errors) and phenotypes (i.e. consequences of operator's actions) concepts have been used. The three main genotypes are identified in the CREAM as follows:

- Direct or indirect cause to behaviour (e.g. emotional state and personality);
- Causes related to man-machine interaction and interface;
- Causes that are typical of an organization (e.g. temperature, nose etc).

In this method, the context of human action is defined by following nine Common Performance Conditions (CPCs):

- Adequacy of organization:
- Working conditions;
- Adequacy of man-machine interface and operational support;
- Availability of procedures/ plans;
- Number of simultaneous goals;
- Available time;
- Time of day;
- Adequacy of training and experience;
- Quality of crew collaboration.

The CREAM method can be used both retrospectively to analyse errors and prospectively to predict the potential errors. However, the CREAM model does not provides any remedial measures to remove or to mitigate the human erroneous actions (Stanton et al., 2005).

3.2.8 Connectionism Assessment of Human Reliability (CAHR)

The Connectionism Assessment of Human Reliability (CAHR) has been developed at the Technical University of Munich and the Gesellschaft fur Anlagen-und Reaktorsicherheit (GRS) between 1992 and 1997 (Sträter, 2000) also is also cited in (Bell and Holroyd, 2009). The CAHR model is a database system developed after learning from past experience of German nuclear power plants and then comparing the obtained values with the THERP HEPs using the probabilistic models. During the development of the CAHR, it has been seen that probabilistic model based on Rasch provides the maximum agreement with the THERP values (Sträter, 2000).

The underlying philosophy of this tool is as is reported in the (Bell and Holroyd, 2009):

- The focus of this tool is the working system and not just the human/ operator;
- Human error caused by the interaction of several situational factors;
- CAHR uses a fixed structure but not a fixed taxonomy;
- A strict differentiation between observable information and causes is maintained.

In the Connectionism Assessment of Human Reliability (CAHR) model, the term connectionism was used because it models the cognition aspects on the basics of artificial intelligence. Therefore, it refers to the idea that human performance is affected by the interrelation of multiple conditions and factors as mentioned in the (Everdij and Blom, 2013). Furthermore, an application of CAHR model in the maritime accidents investigation can be found in the (Loer et al., 2011). However, some theoretical challenges are also acknowledged in this model.

The concepts from this model have been used in the present work and therefore are described in detail in the section 6.

3.3 Models to integrate the risk assessment techniques and HOF

As anticipated earlier, the scope of this work is to integrate the existing risk assessment techniques with the Human and Organizational Factors (HOF). The purpose of this work is not to provide a dedicated human factor tool that can account for all the PSF. Therefore, in this section some of the developed methods/ approaches will be discusses that can help to integrate the risk assessment techniques (mainly discuss in section 3.1) and the HOF.

The (Bellamy and Geyer, 2007) have highlighted that often there are difficulties in explaining and communicating about the human factors and how human factors overlap and interface with the safety management systems and wider organizational issues, in the context of risk control.

Furthermore, (Bellamy and Geyer, 2007) have analysed eight past accidents in order to understand the human factors, safety management systems and the organizational factors and have provided an integrated model. Furthermore, it was also mentioned that about 25% of the Loss of Containment (LOC) accidents with vessels could be attributed to human factors aspects which could have been prevented. In this model, (Bellamy and Geyer, 2007) have identified following main events as related to the theme of human errors during maintenance operations:

- Corrosion

Containment not maintained (repaired/ replaced)

- Exceeds containment limits

Installed incorrectly (or wrong thing installed)

Not replaced like with like

- Operator error

Wrong part (containing hazardous material) worked on

- High Pressure

Pressure relief fails to prevent excessive overpressure

- Wrong equipment/ location

Mixed up in storage/ location

Not available

right equipment in wrong place

Incorrectly installed equipment

Therefore, these issues should be addressed in the maintenance system in the plan-do-check-act cycle featured in safety management systems. Furthermore, (Bellamy and Geyer, 2007) have concluded that integration of human element around a technical theme closely linked to the risk is particularly an interesting aspect, since it enables assessment and inspection approaches to be targeted in a risk based way.

In the I-Risk approach, the management system was linked to the technical system through the base events of fault trees from the risk assessment and is reported by the (Papazoglou et al., 2003). The key components of the I-Risk methodology are the technical model, the management model and their interface. In the I-Risk methodology, the technical model consists of developing a Master Logic Diagram (MLD) defining major immediate causes of Loss of Containment (LOC) events and associated quantitative models for assessing their frequencies. While, the management model consists of the tasks, which must be carried out systematically in the primary business functions. In the I-Risk, the updated frequency of failure is provided against three management models (i.e. worst case, best case and against the current management system of specific installation).

The (Øien, 2001) has proposed another model, Organizational Risk Indicator Model (ORIM) as a tool for risk control during operations of offshore installation as a complement to the QRA-based indicators. The results comprise a qualitative organizational model, proposed organizational risk indicators and a quantification methodology for assessing the impact of the organization on the risk. It has been highlighted by the (Øien, 2001) that risk prediction has mainly covered technical failures and human errors but recently there is a focus to include the organizational aspects, explicitly. Since, the human error in certain cases is trigged by an error in the organizational aspects. The conceptual model of ORIM is illustrated in the Figure 6. In this figure, the selected organizational risk indicators can be used to modify the leak frequencies and hence the risk originated from those leak scenarios.

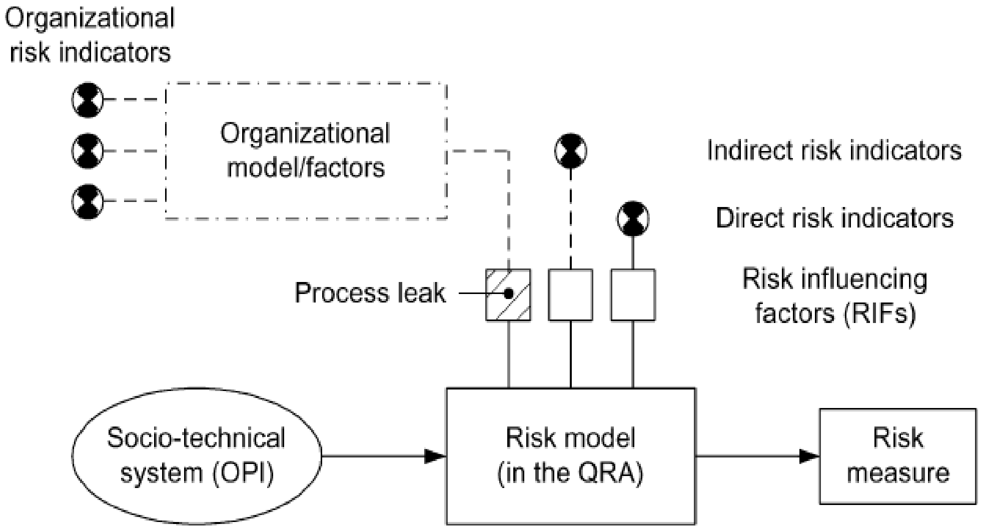

Organizational risk indicators
Organizational model/factors
Indirect risk indicators
Direct risk indicators
Process leak
Risk influencing factors (RIFs)
Socio-technical system (OPI)
Risk model (in the QRA)
Risk measure

Figure 6. Conceptual model for organizational risk indicators adapted from (Øien, 2001)

In the ORIM model, the considered organizational factors can be seen in the Table 16. The six main organizational factors are considered in the ORIM method. Furthermore, organizational risk indicators are also defined against each of the selected factors and five mutually exclusive states of the organizational factors can be defined. The organizational risk indicators can help to identify the existing state of an organizational factor.

Table 16: Organizational factors used in ORIM, adapted from (Øien, 2001)

Organizational factors
Individual factor
Training/ competence
Procedures, guidelines and instructions etc
Planning, coordination, organization and control

Design
PM-Program/inspection

The overall rating of an organizational factor is calculated by a combination of the rating of the organizational risk indicators and their weight on the organizational factor as shown by the Eq. 6.

$$r_k = \sum_{j=1}^{n_k} v_{kj} \,.\, r_{kj} \qquad \text{Eq. 6}$$

Whereas:

v_{kj} is the distribution of individual weights of different indicators. (assigned by expert judgment and assumed to remain constant over time).

v_{kj} is the rating of different indicators.

The Barriers and Operational Risk Analysis of hydrocarbon release (BORA - Release) method was developed to calculate the establishment's specific conditions of technical, human, operational and organizational influencing factors and their impact on the barrier's performance, that are established to prevent the hydrocarbon release as proposed by the (Aven et al., 2006). It was highlighted that technical, human, operational and organizational factors can influence the accident sequence. The following steps are the main steps to be carried out during the BORA-release analysis:

- Development of a basic risk model including release scenarios;
- Modelling the performance of safety barriers;
- Assignment of industry average probabilities/ frequencies and risk quantification based on these probabilities/ frequencies;
- Development of risk influencing diagrams;
- Scoring of risk influencing factors;
- Weighting of risk influencing factors;
- Adjustment of industry average probability/ frequencies;
- Recalculation of the risk in order to determine the platform specific risk related to the hydrocarbon release.

In the BORA- Release, the effect of the risk influencing factors on barriers is calculated by a combination of weighting and rating as proposed in the ORIM approach as well.

The ω-factor approach has been developed by the (Mosleh et al., 1997) to quantify the effect of sub-organizational attributes on equipment's reliability and on operator's performance in nuclear power plants. The results of this quantification has been used to determine the amount of increase in equipment failure rate and human error probability due to organizational factors. In the context of present work, some concepts from ω-factor model has been used therefore in the following section more description about this model is provided.

In the ω-factor model, it has been argued that organizational factors influence is common to all technical components and human actions as demonstrated in the Figure 7. In this model it has been argued that there could be two possible influences of the organizational factors on the technical components:

- Higher failures rate as a result of poor organization but independent from each other;
- Dependency model of organizational factors similar to common cause failure (CCF) analysis, in which failures are simultaneous.

But the first alternative has been considered to be more feasible and appropriate, therefore considered in this approach.

In this model, it is proposed that failure rates (e.g. λ) are composed of two components: inherent failures (λ_1) "the inherent portion of failure rate which is beyond the control of organization in-charge" and failures induced due to organizational influences (λ_O), as shown by the following equation:

$$\lambda_{\mathrm{Total}} = \lambda_1 + \lambda_{\mathrm{O}}$$

A parameter (ω) has been defines as follows:

$$\omega = \frac{\lambda_O}{\lambda_1}$$

Therefore:

$$\lambda_{Total} = \lambda_1 + \omega\lambda_1$$

A structural relationship of the organization is shown in the Figure 8 as has been proposed in this model. The model of a big organization can be quite complex network of nodes and links. Therefore, considering the entire organizational influence diagram at once might be complex but a type of multi-layered model can be considered as shown in Figure 8. A parameter “P” is calculated, which is degree that the worker’s performance is adversely affected by organizational factors. In similar way, the human error probability can be written as:

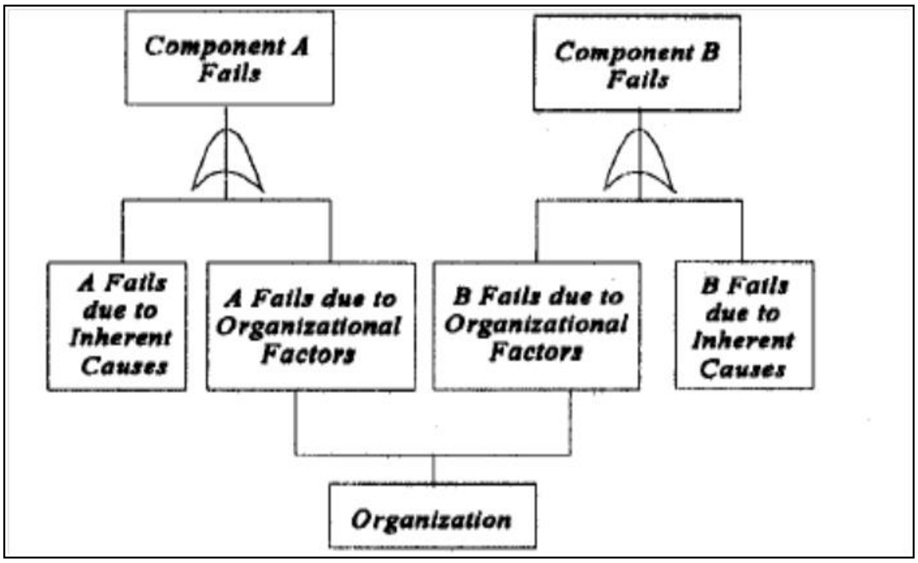
$$h_{\text{Total}} = h_1 + h_O \qquad \text{Eq. 7}$$

Whereas:

h1 is based on individual PSF

h2 is due to organizational PSF

Since, most HRA models use PSF to quantify the human error probabilities so a link of human reliability through Eq. 7 can be justifiable.



Component A Fails
Component B Fails
A Fails due to Inherent Causes
A Fails due to Organizational Factors
B Fails due to Organizational Factors
B Fails due to Inherent Causes
Organization

Figure 7: Representation of dependency due to organizational factors, adapted from (Mosleh et al., 1997)

In another model proposed by the (Schönbeck et al., 2010), a new approach to adjust the design values of safety integrity levels by considering the operational effect of the HOF has been demonstrated. The HOF affect can adversely impact the design risk reduction expressed as safety integrity levels. In this work, (Schönbeck et al., 2010) has identified following eight safety influencing factors with a potential to influence the performance of safety instrumented functions:

- Maintenance management;

- Procedures;
- Error-enforcing conditions;
- Housekeeping;
- Goal compatibility;
- Communication;
- Organization;
- Training.

In the subsequent steps, the relative weights of these safety influencing factors has to be identified. It has been proposed that weights can be obtained from past accidents but given the low ratio of the past accidents, the data from the dangerous detected failures can also be used. In this case, a relative weight can be assigned for each of the safety influencing factors and then these weights have to be normalized.

Therefore, by providing weights and rating to these factors, operational SIL can be obtained from design SIL from the Eq. 8.

$$\mathrm{SIL_{Operational}} = \left(\theta \sum_{i=1}^{8} \mathrm{RiWi} - 1\right) \log \mathrm{PFD_{design}} \qquad \text{Eq. 8}$$

Whereas:

θ is the proportion of the design SIL that can be explained by HOFs ($0 \leq \theta \leq 1$)

R_i is the rating for the safety influencing factor ith ($0 \leq Ri \leq 1$ for all i)

w_i the weight factor for the safety influencing factor ith ($0 \leq wi \leq 1$ for all i)

PFD_{design} is the average probability of failure on demand according to the design.

A similar equation can also be used for operations in high demand mode or continuous mode and where PFD is given in dangerous failures per hour. Therefore, by using this kind of model, a difference between design and the operational SIL (ΔSIL) can be obtained. However, some of the previous identified challenges are also observed here: how influencing affect (i.e. weights) of various safety influencing factors can be obtained and if possible how to validate them.

Meanwhile, (CCPS, 2000) p. 642, has highlighted the following areas of further improvement with respect to the human factors in quantitative risk assessment:

- Continued improvements in models for incorporating human factors into a chemical process' quantitative risk assessment study;
- Better understanding of the impact of company and plant culture, management systems, maintenance practices, and other such factors on the reliability of process plant equipment (i.e. PSFs).

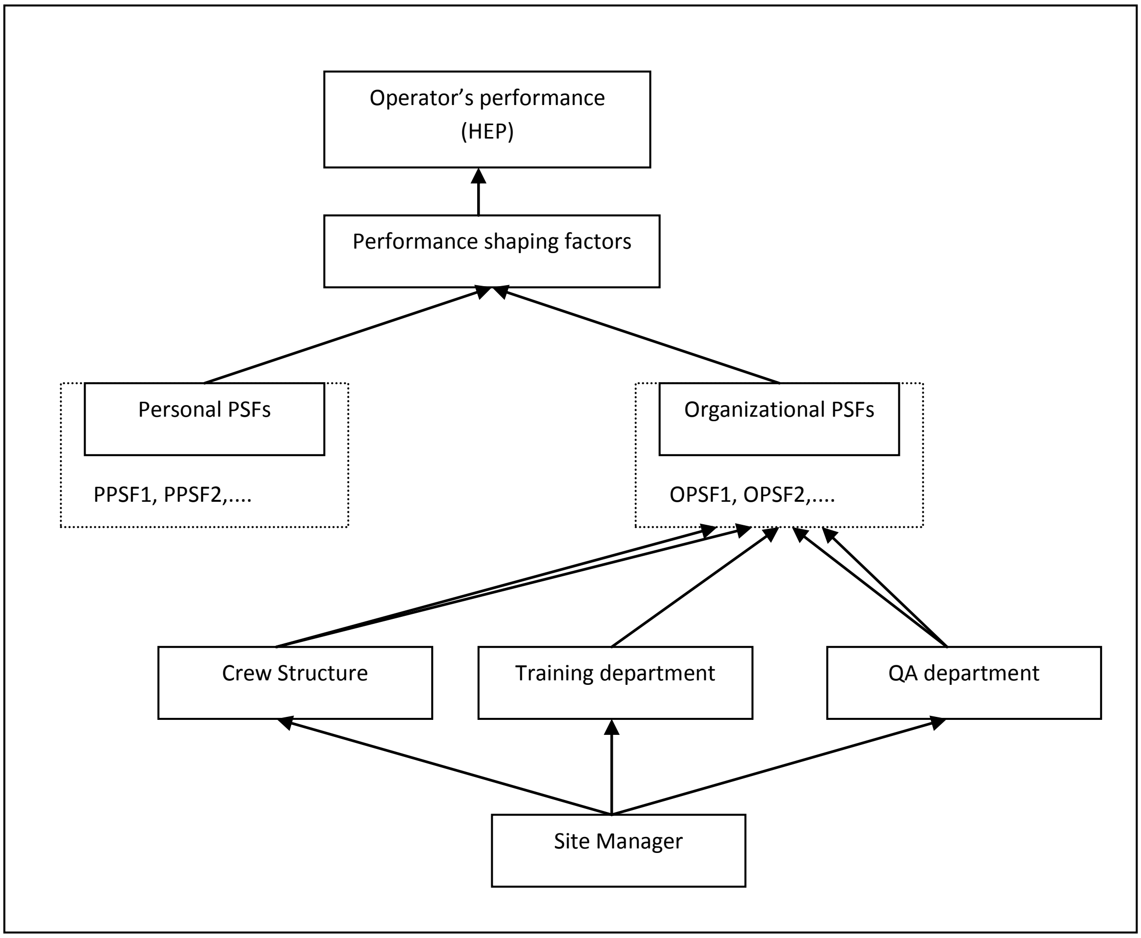


Figure 8. Evaluating PSF through organizational factors, adapted from (Mosleh et al., 1997)

However, similar approaches can also be used for the human factor models, where the reliability of an operator changes with respect to the management systems or the organizational factors.

Therefore, in the light of base models for both conventional risk assessment and human factors quantification. In this scope of work, it has been decided to use the data from past accidents to quantify the effect of the organizational factors on the human reliability. The International Standard (IEC 31010, 2009), has also mentioned to use the historical data from past accidents and to predict the probability of occurrence of failure in the future.

There are numbers of available databases to record past accidents for chemical process industry. These databases have been analyses to quantify the human and organizational factors assessment and to learn lessons.

4 Analysis of past accidents

The Following main databases have been found which can be used to acquire the useful data, required for the quantification of human and organizational factors as detailed in Table 17. The website of Norges teknisk-naturvitenskapelige universitet (NTNU, 2014) provides the useful information about the available accident databases.

Table 17: List of some of the existing accident databases

Accident databases	Sources
European Major Accident Reporting System (eMARS)	Maintained by Major Accident Hazards Bureau (MAHB) under EU Seveso II/III Directive.
Failure and Accident Technical System (FACTS)	Maintained by unified Industrial and Harbour Fire Department – Rotterdam, Netherlands.
Analyse, Recherche et Informations sur les Accidents (ARIA)	Maintained by French Ministry of Ecology, bureau for analysis of industrial risks and pollutions.
Process Safety Incident Database (PSID)	Maintained by Canter for Chemical Process Safety (CCPS).
Natural and Environmental Disaster Information Exchange System (NEDIES)	Maintained by the European Commission's Joint Research Centre.
World Offshore Accident Database (WOAD)	Maintained by Det Norske Veritas (DNV GL).
Accident statistics for fixed offshore unit on the UK Continental Shelf (1980 - 2005)	Prepared by (DNV, 2007a).
Accident statistics for floating offshore units on the UK Continental Shelf (1980 - 2005)	Prepared by (DNV, 2007b).
Ship/ platform collision Incident database (1975 - 2001)	Prepared by (Robson, 2003).

The eMARS database has been maintained by the Major Accident Hazards Bureau (MAHB) and collects the accidents occurred mainly in the EU Member States under Seveso II Directive or now Seveso III Directive (EC, 2012). The FACTS database contains information about the accidents involving hazardous materials which caused or could have caused severe damage or danger. The FACTS database was initiated by TNO but now is maintained by unified Industrial and Harbour Fire Department - Netherlands.

The PSID database is managed by CCPS to collect, track and share important information, process safety incidents and experience among project participants.

The NEDIES database has been started and maintained by European Commission's joint Research Centre with the aim to update the information about the occurrence of natural disasters and their management.

The WOAD database can provide an access to accident database for diverse offshore facility. The WOAD database also provides accident causes, location, social and economic impacts that can be valuable for the risk management initiatives.

The HSE has also collected data about past accidents mostly related to offshore facilities as also shown in the Table 17.

Therefore, given the information of all aforementioned databases, it has been decided to use the eMARS for further analysis due to following main reasons:

- EMARS is developed in the context of the EU Seveso Directive, therefore it is mandatory for the EU Member States to report their major accidents to the European Commission;
- EMARS identify and record the causal factors to accidents;
- EMARS provides a free access to their database and has already been used by other researchers to learn lessons from accidents.

4.1 Accidents reported to eMARS

The data from the European Commission's Major Accident Reporting System (eMARS) has been analysed from past accidents occurred from 1988 to 2012 (i.e. 25 years). The purpose of eMARS is to facilitate the exchange of lessons learned from accidents and near misses involving dangerous substances to improve the chemical accident prevention and mitigation of potential consequences (Emars, n.d.). It is obligatory for the European Union (EU) Member States to report the major accidents to eMARS, if threshold of an event meets the criteria established in annex VI of the Seveso III Directive (EC, 2012). The reporting of a major industrial accident by competent authorities was also a requirement under predecessor Directives (i.e. Seveso I &II Directives). The criteria to notify an accident is based on discharge amount of a dangerous substance. The Annex I of the Directive provides information about the amount of dangerous substances to qualify an establishment as lower or upper-tier establishments. The notifying criteria is also based on the consequences as a result of the accident. The detail about the notifying criteria can be found in the Appendix III of this document.

However, accidents or “near misses” which do not meet the quantitative criteria defined in the Directive but the Member States regard them as of particular technical interest should also be notified to the European Commission (EC, 2012).

The number of interesting results had already been obtained from the analysis of past accidents reported to eMARS by previous researchers. For example, (Nivolianitou et al., 2006) have highlighted after analysing accidents from 1985 to 2001reported to the eMARS that about 40% of the major accidents have their cause either exclusively (19%) or partially (21%) related to human factors. While equipment failure was the cause to about 44% of the accidents. The rest of the accidents have their causes either related to natural phenomenon, combination of natural phenomenon and equipment or unclear.

The (Kirchsteiger, 1999) has also concluded similar aspects that human error contributed to number of past accidents after reviewing the accidents reported to eMARS.

A report published by the European Commission’s Joint Research Centre (Sales et al., 2007) has highlighted that analysis of past accidents in the process industries is a useful method for identifying common aspects regarding the causes that triggered such accidents. In this report, a trend in the evolution of the accidents is also presented. Furthermore, it was demonstrated that evolution of safety in process industries is cyclic, probably related to variations in risk perception or awareness. This could be due to an increased awareness after following an accident. Another report by the European Commission’s Joint Research Centre (JRC) has concluded after studying past accidents and contribution of corrosion to equipment failure that corrosion failures originated mainly in the pipework as compare to the storage tanks or rest of the units (Wood et al., 2013).

4.1.1 EMARS reporting structure

In the eMARS database, a classification has been provided among the following industrial types as can also be shown in the Table 18. In this scope of work only those industrial types are considered which are usually considered under the umbrella of the chemical process industry. These considered industrial types are highlighted in bold font in this table. The selection of these industrial types is considered due to relevancy of operations among them and also to obtain enough data to conclude lessons learned.

Table 18: Industrial types considered in the eMARS database

Industrial types
Agriculture
Building & works of engineering construction
Ceramics (bricks, pottery, glass, cement etc)
Chemical Installations – ammonia
Chemical Installations – carbon oxide
Chemical Installations – chlorine
Chemical Installations – fluorine or hydrogen fluoride
Chemical Installations – hydrogen
Chemical Installations – industrial gases
Chemical Installations – inorganic gases
Chemical Installations – nitrogen oxides
Chemical Installations – other fine chemicals
Chemical Installations – sulphur oxide, oleum
Electronics & electrical engineering
Fuel storage (including heating, retail sale, etc)
General chemicals manufacture (not included above)
General engineering, manufacture and assembly
Handling and transportation centres (ports, airports, lorry parks, marshalling yards etc)
Leisure activities
LPG production, bottling and bulk distribution
Manufacture of cements, lime and plaster
Manufacture of food products and beverages
Manufacture of glass
Medical, research, education (including hospitals, universities,...)

Mining activities (tailing & physicochemical process)

Not known / not applicable

Petrochemical /Oil Refineries

Plastic and rubber manufacture

Power supply and distribution

Processing of ferrous metals (foundries, smelting, etc).

Processing of metals

Processing of metals using electrolytic or chemical process

Processing of non-ferrous metals (foundries, smelting etc)

Production and manufacture of pulp and paper

Production and storage of explosives

Production and storage of fireworks

Production and storage of pesticides, biocides, fungicides

Production of basic organic chemicals

Production of pharmaceuticals

Shipbuilding, ship breaking, ship repair

Textiles manufacturing and treatment

Waste treatment, disposal

Water and sewage (collection, supply and treatment)

Wholesale, retail storage and distribution (excluding LPG)

Wood treatment and furniture

In the eMARS accident reporting system following main aspects are considered relevant to an accident:

- Reason of reporting
- Accident involving
  - Domino effect
  - Natech events
  - Transboundary effects
  - Contractor

- Release major occurrences / initiating events
- Fire major occurrences / initiating events
- Explosion major occurrences / initiating events
- Site description
- Substances involved
- Causes of accident
  - Organizational
  - Plant / equipment
  - Human
  - External
- Consequences
  - Human
  - Environment
  - Cost
  - Disruption
- Emergency response
- Theme of lessons learned
- Attachment section (if any)

A detailed specimen of the eMARS reporting structure is also presented in the Appendix IV, which can highlight the options chooses by the European Commission to be presented during the reporting system. The data from the analysis of past accidents has been collected from these accident's reports.

4.2 Existing accident models

In order to analyse the accidents systematically; coherently and structured, it is required to use an accident model. The (Al-shanini et al., 2014) have described accident modelling as a "methodology used to related the cause and effects of events that lead to an accident". In this scope of work, the characteristics of used accident model should be as follows:

- Applicable with the amount of information provided in the eMARS reporting system;
- The structure of data acquisition (i.e. with the help of accident model) should also be coherent with the proposed model. The structure should also be applicable

prospectively to quantify the human and organizational factors (HOFs).

Therefore, it is required to perform a background search about the available accident methods/ models that can be used to perform the accident analysis and consequently choose the most appropriate model.

A typical safety pyramid for chemical process plants is shown in the Figure 9 in which the incidents/ un-safe behaviours move to the top of the pyramid (CCPS, 2011). There are multiple layers/ barriers with an intention to prevent/ mitigate the consequences of an incident. The failure of these layers lead to an accident with higher magnitude or severity. Another way to explain the Figure 9 is that incidents at the top of the pyramid reflect those situations where failure to the multiple layers of protection have already occurred while the bottom of the pyramid reflects failures or challenges to the safety layers as also mentioned by the (CCPS, 2011).

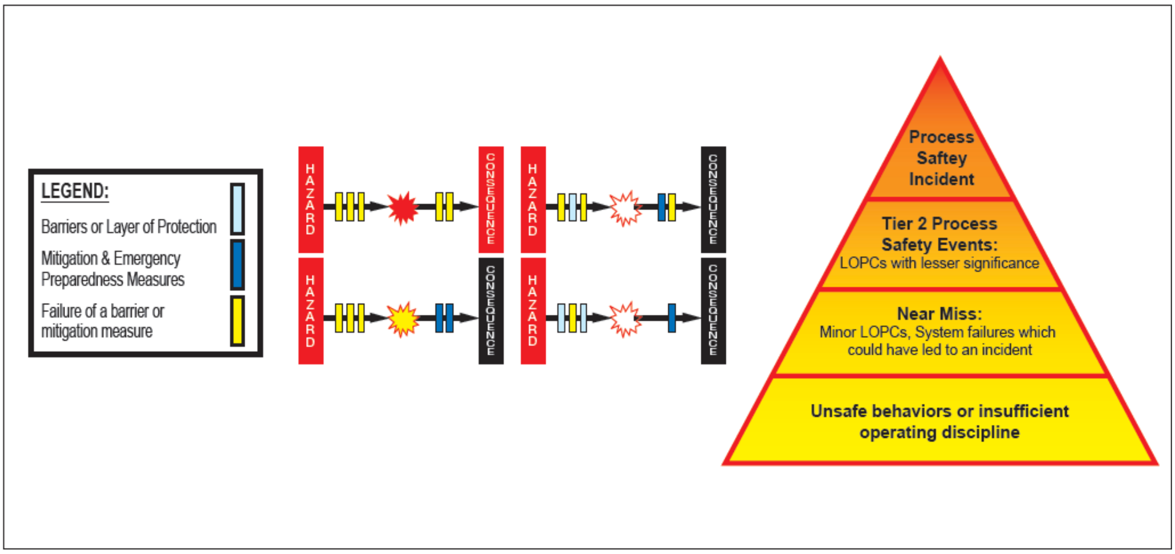

LEGEND:
Barriers or Layer of Protection
Mitigation & Emergency Preparedness Measures
Failure of a barrier or mitigation measure
HAZARD
CONSEQUENCE
HAZARD
CONSEQUENCE
HAZARD
CONSEQUENCE
HAZARD
CONSEQUENCE
Process Saftey Incident
Tier 2 Process Safety Events:
LOPCs with lesser significance
Near Miss:
Minor LOPCs, System failures which could have led to an incident
Unsafe behaviors or insufficient operating discipline

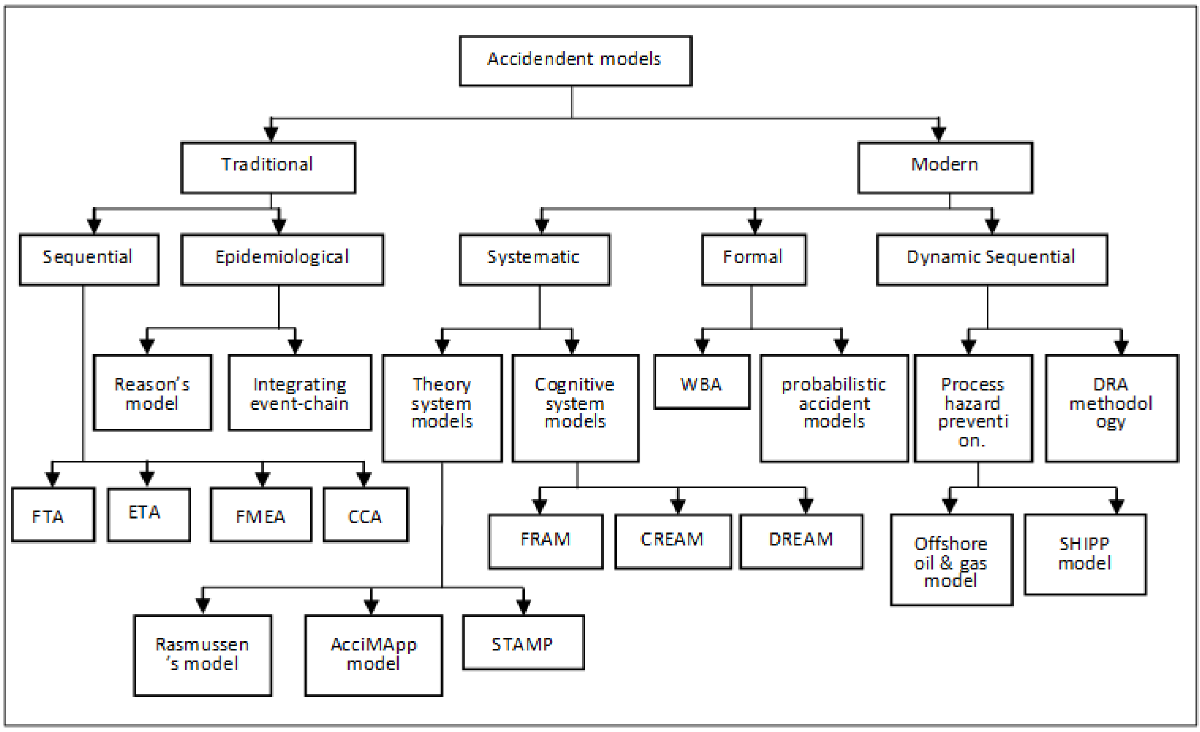
Figure 9. Process safety pyramid/ failed protection layers, adapted from (CCPS, 2011)

The (Al-shanini et al., 2014) have reported the categorization of different accidents models that can be used for the accident analysis. The main classes of accident models are, as illustrated in the Figure 10:

- Sequential;
- Epidemiological;
- Systematic;
- Formal;
- Dynamic.

The accuracy, capability and limitation of accident models vary significantly, depending on their purpose and focus as reported by the (Rathnayaka et al., 2011) and also cited by the (Al-shanini et al., 2014).

The sequential models follow the chain of events, while the epidemiological models focus on the performance deviations and also on the environmental conditions. The systematic models and formal models are the modern accident analysis models. While, a new category is also introduced which is dynamic sequential models. These models apply the traditional sequence methods (e.g. FTA, ETA) to represent an accident scenario and is often combined with some other approaches to represent the non-linearity among the relation. The further detail about these models can be found in the (Al-shanini et al., 2014).



Legend: FTA: Fault Tree Analysis, ETA: Event Tree Analysis, FMEA: Failure Modes and Effects Analysis, CCA: Cause-Consequence Analysis, STAMP: Systems-Theoretic Accidental model and Processes, CREAM: Cognitive Reliability and Error Analysis Method, FRAM: Functional Resonance Accident Model, DREAM: Driver Reliability and Error Model, WBA: Why-Because Model, SHIPP: System Hazard Identification Prevention and Prediction Methodology, DRA: Dynamic Risk Assessment.

Figure 10. Accident model classification, adapted from (Al-shanini et al., 2014)

There are number of other accident models that also consider the possible barriers which can contain/ prevent the evolution of an accident. One such model is represented as Accident Evolution and Barrier Function (AEB) model. However, these models cannot be used to quantify the analysis based on the eMARS reporting system because eMARS reporting system seldom provide information about the barriers which were present to contain the accident evolution.

In this scope of work, it has been decided to use the Reason's Swiss Cheese Model (SCM) to analyse the accidents as provided by the (Reason, 1990) and is also illustrated in the Figure 11. There are following main reasons to choose the Reason's Swiss Cheese Model (SCM) for this analysis:

- Swiss cheese model is quantifiable based on eMARS database;
- Since scope of this work is to quantify the HOF, and Swiss cheese model can provide a logical link among human and organizational factors;
- This model can also be used in prospective way to quantify the HOFs.

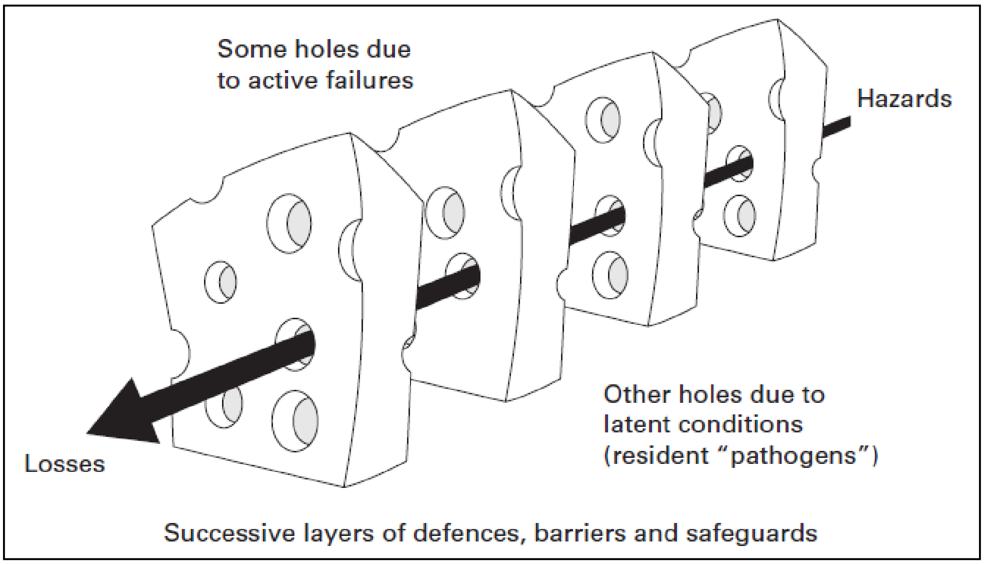


Figure 11. Swiss cheese model, adapted from (Reason, 1990)

According to Swiss Cheese Model (SCM), an accident can occur when different safety layers align in a way so that hazard can find its way to an accident. The holes in these layers represent the flaws in the safety layers. The holes therefore enhance the probability of a hazard to find its way to the accident. The SCM can help to identify different layers that are used or that can be used to prevent/ mitigate an accident. Furthermore, it can also identify the possible factors that can influence the performance of the layers. Therefore, in order to improve the performance of safety layers it is required to improve the influencing factors corresponding to those specific layers.

4.3 Modified Swiss cheese model

In order to study the accidents in chemical process plants, it has been decided to modify the SCM according to the requirements and to obtain a structure which can be quantifiable from the information present in the eMARS database.

The (Reason et al., 2006) has reviewed the SCM and highlighted that although SCM has some limitations but it is so far the widely used accident model. Furthermore, (Reason et al., 2006) also highlighted different forms of the SCM. The (ATSB, 2008) has adapted a form of SCM, which is highlighted in the Figure 12. In this model it is assumed that an organization achieve its production goals through a combination of various events and conditions. In most cases the production goals can be achieved. However, in some cases various events and conditions will combine to produce unnecessary events. Therefore, risk controls should be in place to ensure that system is safe or at least the consequences of an unnecessary action can be minimized. At the same time, other risk controls in the form of "prevention" can also be used to minimize the likelihood of deviation from normal operations. However, performance of the risk controls is always subject to a number of factors termed as "organizational factors" (ATSB, 2008).

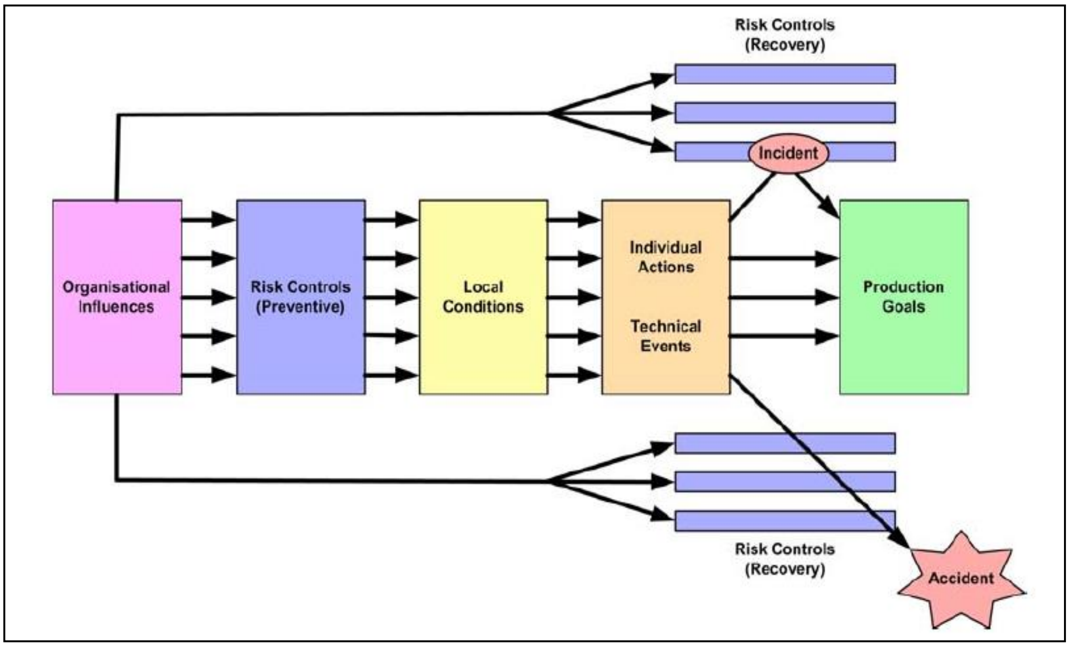


Figure 12. ATSB adaption of the Reason model, adapted from (ATSB, 2008)

The safety indicators can be used for each of the involved elements to ensure the safety and integrity of operations.

In this scope of work, SCMs are adapted in their different forms according to the initiating cause to an accident and failure of subsequent prevention/ mitigation safety layers. All the layers are classified into two main states:

- Operational;
- Prevention/ mitigation.

The state of a layer represents its activity/ role according to the design/ control philosophy of a plant. The errors in the operational layer correspond to those errors which happen during the normal operations. While, prevention/ mitigation errors are the errors which can happen when the system is already in an undesired situation. At this point in time, actions could be preventive or mitigative depending upon the allowable fluctuation of process parameters. However, definitions of preventive and mitigative terms are not fixed and subject to variations according to the design/ control philosophy of a specific plant.

A form of the adapted SCM is illustrated in the Figure 13, in which layers are classified into two main states: "operational" and "prevention/ mitigation". Two main elements are considered for each of the state:

- Technical;
- Human.

These two elements represent the two main actors of a chemical process plant and failures/ errors are associated to each of the elements. The "technical" element is usually considered in the risk calculations by means of the failure rate of an equipment (i.e. λ) while "human" element is considered by means of a failure probability (i.e. HEP). Moreover, as highlighted by vast published literature that performance of both of these elements subject to change by specific PSFs as detailed in the section 3. In this analysis "organizational" PSF are considered for both of the elements. While, "stress/ fatigue" and "meteorological" PSF are considered for human and technical elements, respectively. The holes in any of the layers represent the flaws in that layer depend upon the performance/ quality of associated PSF. However, it is also considered that each layer has its own inherent flaws and holes represented by failure rate (i.e. λ) and probability of failure for technical and human elements, respectively.

Therefore, more the weaknesses in a layer, the bigger will be the holes. Hence, more will be the chances that hazard will find its way to an accident. In this analysis, only those technical aspects (i.e. failure) are considered for which there is an effect of PSFs.

The SCM illustrated in the Figure 13 corresponds to the model 1A, according to the Table 19.

In the model 1A, a failure of all the layers lead to an accident. In this work, nine different forms of the SCM have been developed as summarized in the Table 19. It can be observed from this table that initiating causes to an accident are divided into three main alternatives:

- Technical & human;
- Technical;
- Human.

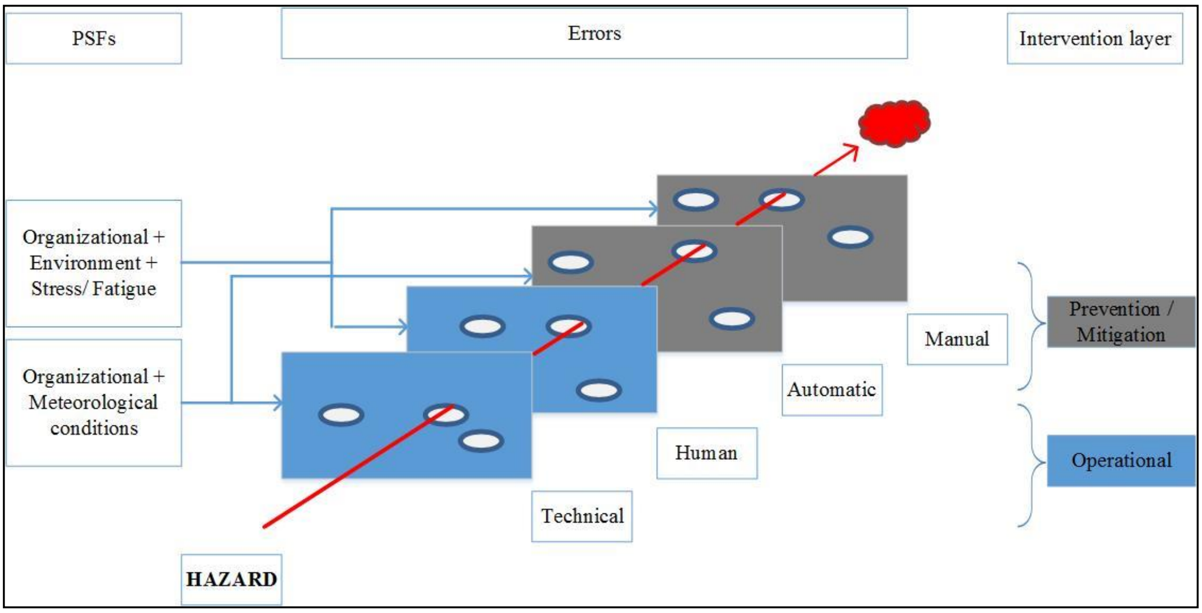


Figure 13. Modified Swiss cheese model, adapted from Reason's Swiss cheese model

Therefore, it has been assumed that accidents can occur due to the coupling of "technical" and "human" failures or due to failure of one of the aspects in "technical" and "human" failures.

It can also observed from the Table 19 that different prevention/ mitigation layers correspond to different forms of SCMs. In this work two main prevention/ mitigation layers are considered:

- Automatic;
- Manual.

In the Table 19, three possible alternatives are considered according to the safety barriers in the prevention/ mitigation state:

- Automatic & manual
- Automatic / manual
- Not observed

The “Automatic & manual” cases correspond to those instances when both barriers were present and failed. While, during “automatic/ manual” cases only one of the barriers (i.e. automatic or manual) was present and failed. However, in some instances no barriers were observed that represents by the “Not observed” status.

The automatic safety layer corresponds mainly to the automatic safety function (e.g. PSVs, SIFs, BDVs and ESDs etc). The manual safety layer corresponds to the supervision activities mainly performed by a supervisor.

Table 19: Forms of the SCM “Accidents models”, adapted from Swiss cheese model

No.	Model name	Initiating cause	Prevention / mitigation layer
1	1A	Technical & Human	Automatic & manual
2	1B	Technical & Human	Automatic/ manual
3	1C	Technical & Human	Not observed
4	3A	Technical	Automatic & manual
5	3B	Technical	Automatic/ manual
6	3C	Technical	Not observed
7	5A	Human	Automatic & manual
8	5B	Human	Automatic/ manual
9	5C	Human	Not observed

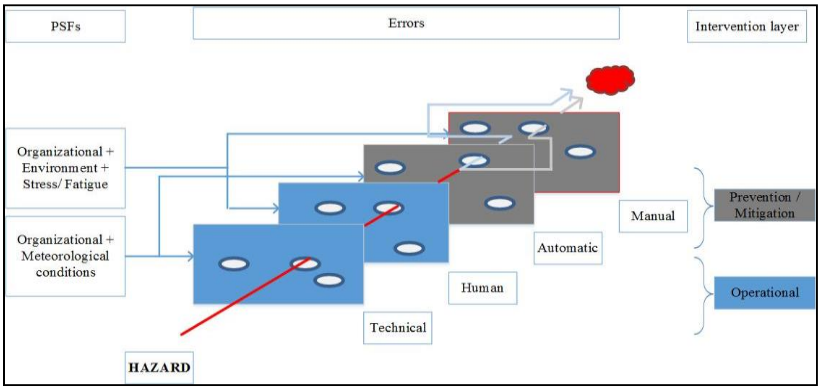


Figure 14. Swiss cheese model, model 1B

The Figure 14 depicts the scenario corresponds to model 1B in the Table 19. This model is same as model 1A or model 1C considering the initiating causes. While, this model only considers one of the safety barriers (i.e. either automatic or manual). Therefore, in the Figure 14 two possible accident paths can be observed in the “prevention/ mitigation” state.

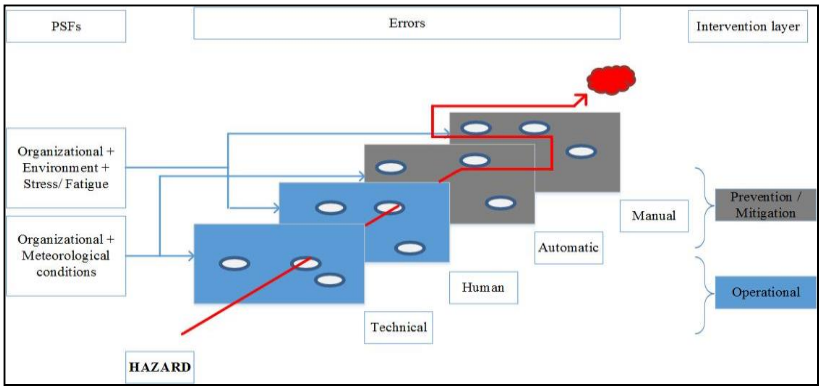


Figure 15. Swiss cheese model, model 1C

The Figure 15 represents those instances for which no safety layer (i.e. prevention/ mitigation) was observed during the accident as identified in the post-accident investigation and reported in the eMARS. This model corresponds to the model 1C in the Table 19.

In the model 3S, only one of the initiating cause (i.e. technical) was present, but the safety barrier layer (i.e. prevention/ mitigation) follows the same order as observed in the model 1. The Figure 16 illustrates the model 3A corresponding to Table 19, in which both safety layers were present and failed consequently led to an accident.

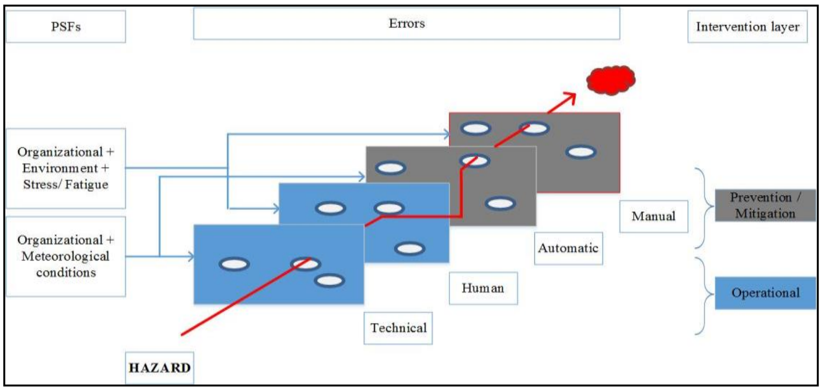


Figure 16. Swiss cheese model, model 3A

The Figure 17 corresponds to those instances when either one (i.e. automatic or manual) safety barrier was present and failed during the accident. It can be expected that accidents corresponding to model A should be fewer than the model B, since in model A double safety layers are present. The model in the Figure 17 corresponds to model 3B in the Table 19.

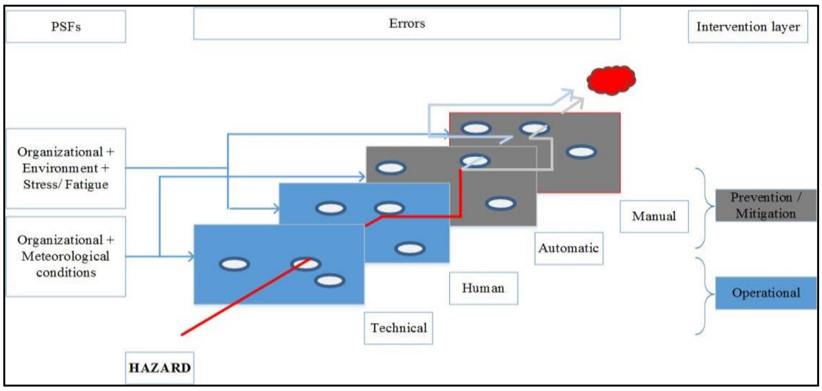


Figure 17. Swiss cheese model, model 3B

In the model 3C as represented by the Figure 18, failure in the “technical” element corresponds to initiating cause while there is no safety barriers present to prevent / mitigate an un-desired situation.

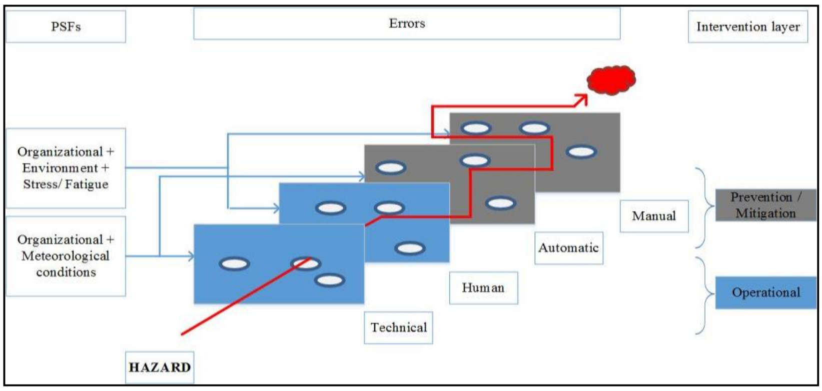


Figure 18. Swiss cheese model, model 3C

In the model 5s, only “human” initiating cause is present. The Figure 19 corresponds to situations when there were both safety layers were present and failed.

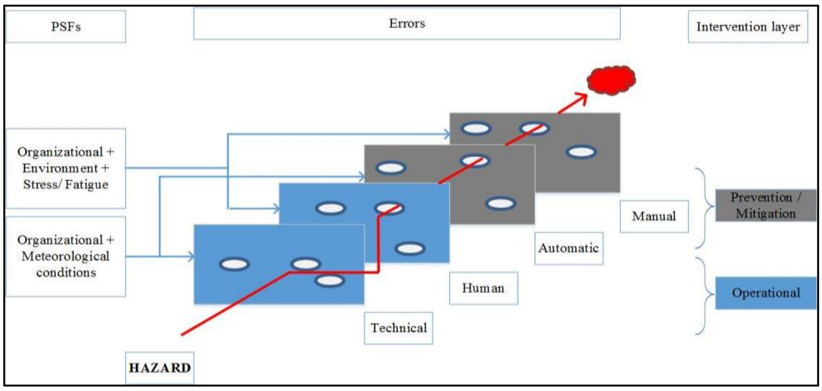


Figure 19. Swiss cheese model, model 5A

This situation corresponds to model 5A in the Table 19. During the accident analysis all the accidents involving “human” initiating cause were studied in-detail.

The Figure 20 shows the failure of either one of the safety barriers. It is interested to observe the performance of safety barriers (i.e automatic or manual) when already a “human” failure has happened.

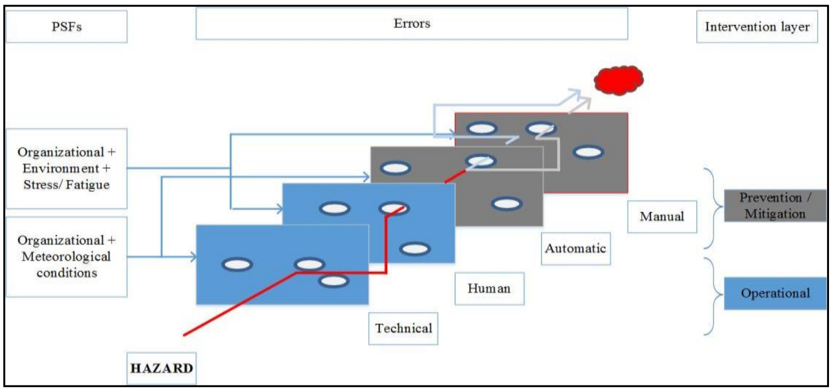


Figure 20. Swiss cheese model, model 5B

The last accident model is represented by the Figure 21, in which “human” initiating cause was present and there was no subsequent safety layer which can prevent the further accident escalation. This model corresponds to model 5C in the Table 19.

In this analysis, only the immediate causes to accidents are considered. Since, sometimes operator has to intervene following some minor abnormality in the process but abnormality is

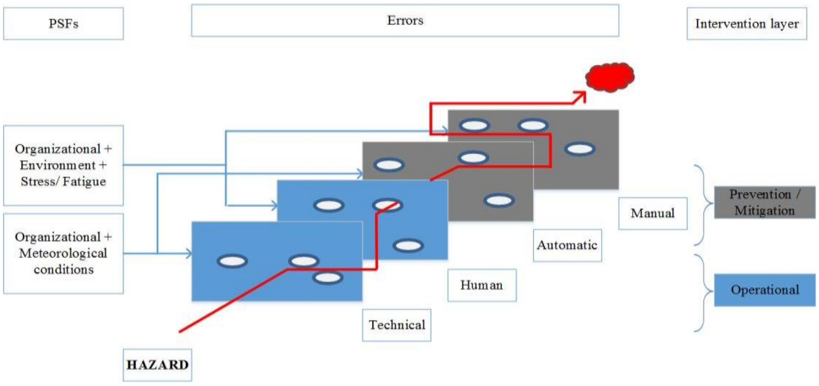


Figure 21. Swiss cheese model, model 5C

not severe enough so that it alone can cause an accident. If abnormal escalation occurs as a result of operator's intervention leading to an accident, in this case the initiating cause of accident is "human". Another important aspect is that; an operator can interact with the automated safety barriers in following two conditions:

- Normal operating conditions;
- Maintenance conditions (i.e. proof testing of SISs etc).

Both of these operator's interactions are considered in the operational state during the development of this work.

Therefore, in this analysis an assumption has been made that an accident escalation follows one of the nine aforementioned generic models in the Table 19. However, there are certain instances when a classification is not possible. This is mainly when the accident escalation exhibits more complex situation or due to insufficient information in the eMARS reports.

4.4 Newly developed taxonomies for human and organizational factors

As described earlier, the causal factors to accidents have been identified based on the subjective judgment. However, in order to ensure the consistency throughout the analysis, taxonomies and corresponding checklists have been developed for the Human and organizational factors (HOF). The main rationale behind the selection of these taxonomies are:

- Taxonomies should be quantifiable based on the information present in the eMARS accident reports;
- Taxonomies should cover as much as possible all failure attributes as observed during the preliminary analysis of accidents.

The human factor taxonomy is a behavioural/ action based taxonomy which is slightly modified compare to the PHEA taxonomy to cover different types of human/ operator actions. The detail about the PHEA method can be found in the section 3.2.2. The human factors taxonomy is reported in the Table 20.

Table 20: Human and organizational factors taxonomies

Human factor taxonomy	Organizational factor taxonomy
Monitoring equipment from field (M)	Training (To)
Monitoring/ operating equipment from control room (A)	Design (Do)
Communication (C)	Procedures (Po)
Manual tasks on-field (F)	Management (Mo)
Reporting (R)	Safety culture (So)

The organizational factor taxonomy has been modified from the taxonomy proposed by (Øien, 2001) to include the main organizational influencing factors.

4.4.1 Considered parameters

In this analysis, some other parameters are also considered to provide a comparison from results and to draw some conclusions, if possible. These parameters are reported in the Table 21. However, it is not possible to quantify all the parameters based on the available information in the eMARS reports.

Table 21: parameters considered in the analysis

Equipment involved	Type of hazard	Operator’s skill level	Plant’s conditions
Pipework	Flammable	Skilled	Normal operations
Vessel	Toxic	Novice	Start up
In-line equipment	Both	No info	Shutdown
			Maintenance

However, some further modifications have been made to certain parameters to consider all possible situations. The contractor’s actions are considered in “Novice” operator skill level. The justification behind this concept is that contractor are less familiar to operations than a full-time working operator. Hence, situations involving contractors are more prone to the failures. The loading/ unloading and fluid addition operations are also considered as "normal operations" even though these operations are conducted in batches.

The detail of the equipment is provided in the Table 22. Furthermore, involved equipment are divided into three main classes according to the main function of the equipment. DNV's Phast Hazard analysis software divide the equipments into two main classes: Vessel and Pipeline). The (Bellamy et al., 1989) also divides the equipments into two main classes: Pipework and in-line equipment.

In this scope of work, it has been decided to divide the equipments into three main classes according to their functionality as illustrated in the Table 22. The Table 22 reports the non-exhaustive list of equipments to provide an idea about the types of equipments considered in each of the class.

Table 22: Classes of equipments

Pipework	Vessels	In-line equipment
Pipeline (Fixed, flexible, buried)	Storage tanks	Pumps
Welds	Reactors	Compressors
Pipe joints	Absorbers / adsorbers	Valves
Tees	Distillation column	Sight glasses
etc	etc	Heat exchangers
		Boilers
		Sensors
		Flanges
		Seals
		etc

5 Results of accident analysis

This section will illustrate the main results obtained from the accident analysis. The 1st section demonstrates the quantitative results of the analysis, while in the 2nd section the developed checklists will be presented.

5.1 Quantitative results of the analysis

As mentioned earlier the Table 18 provides the list of industry types present in the eMARS database at the time of present work. The eMARS contains about 775 accident reports from 1988-2012 at the time of this work, of which about 438 accident reports were related to considered industry types. A list of considered industrial types can be seen in the Table 18. The Figure 22 shows the total number of accidents and accidents caused by the HOF from 1988 to 2012. During the analysis about 197 accidents (i.e. 45 % of total accidents) were observed, when there was Human and Organizational Factors (HOF) was the or one of causes to the accident.

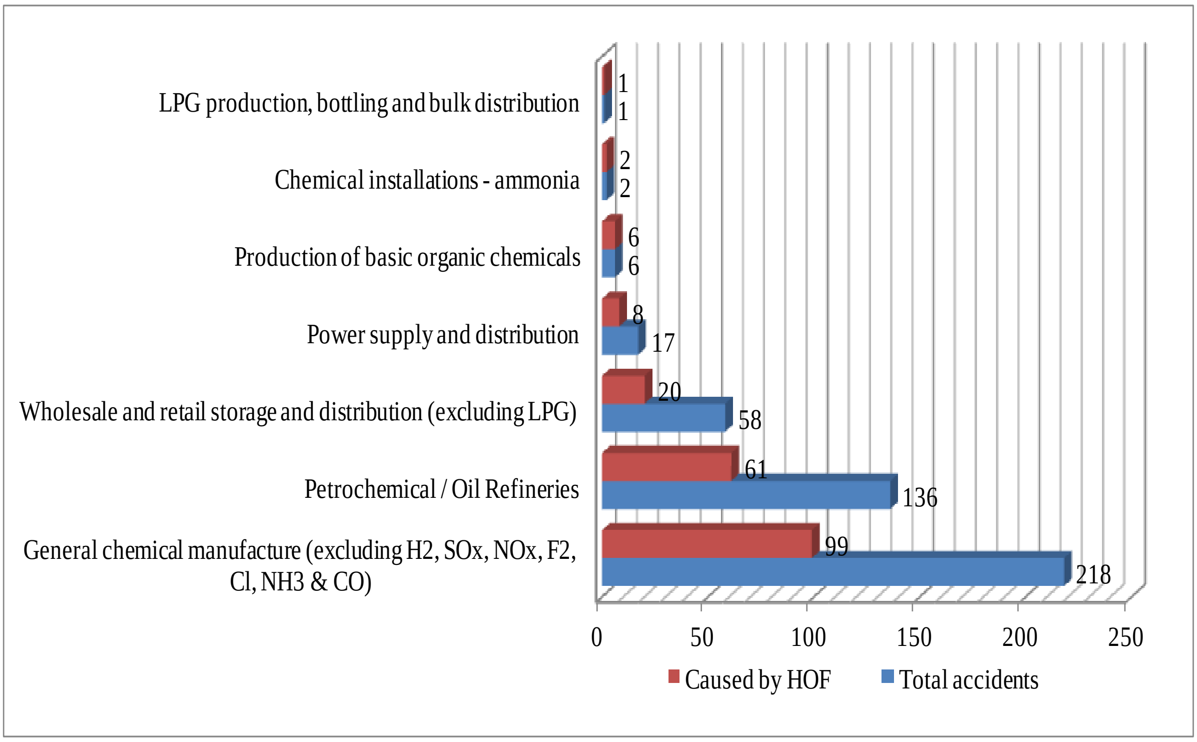


Figure 22. Total accidents versus accidents caused by HOF (1988-2012)

However, those accidents for which investigation are still underway are not considered in this analysis. At the same time, only those accidents are considered for which there is credible information about the causal factors to the accidents. The recommendations following an accident are not considered during the quantification assessment part. During the quantification assessment part only the causal factors to the accidents are considered. This is to ensure that failure factors are estimated correctly. However, recommendations following an accidents are considered in this scope of work and included in other ways mainly future suggestions generated from this work.

According to the Seveso Directive, all the Seveso establishments in the European Union (EU) Member States have to report their accidents to the European Commission based on the criteria set by the Seveso Directive (EC, 2012). This criteria can also be found in the Appendix III. In this scope of work accidents were reported to the European Commission according to reasons highlighted in the Table 23. As can be observed that the total number of accident reporting reason is higher than the total number of accidents studied in this work, this is due to the fact that for some accidents more than one reporting reason may present.

Table 23: Reason for reporting accidents to the European Commission

Reasons for reporting the accidents	Number
Substances involved: greater than 5% of quantity in column 3 of Annex I, of Directive (2012).	80
Injury to persons: ≥ 1 fatalities, ≥ 6 hospitalizing injuries etc.	73
Immediate damage to the environment (according to Annex VI) of Directive (2012).	17
Damage to property: onsite >2 M €, Offsite > 0,5 M€	35
Cross-border damage: transboundary accidents	0
Interesting for lesson learned	13
Not mentioned	30

The highest number of accidents were reported due to the “amount of release substances” followed by the “injury to persons”. At the same time about 13 accidents were reported when an accident does not meet the quantitative criteria to report the accident but it was considered to be worth reporting by the establishment (or by Member States) in order to share the lesson learned from the accident. In these 13 accidents about 40% of accidents were reported in the

2nd half (i.e. 2000-2012) of the analysed time period.

In order to observe the trend of accidents on a time scale, the total time period has been divided into two halves as can be seen from Table 24. It can be observed that the total number of accidents decrease slightly in the second half but number of accidents caused by HOF haven't decreased by the same ratio. This phenomenon can be explained by the fact that with the time, process control and safety have been enhanced but at the same time this also adds more complexity into the system. Therefore, human interaction can become more complex and can add more failures into the system.

Some other conclusions are also drawn from this analysis; since all the accidents have been studied according to the plant's/ unit's operational state when accident has occurred or when the main abnormality has been induced into the system. These aspects can be seen from Figure 24 in which all the accidents caused by HOF and the accidents occurred due to the involvement of contractor into the operations against plant's different operational stages is illustrated. The main contribution from contractor can be seen during the maintenance operations, when almost 41% of accidents caused due to the involvement of contractor into the operations. This aspect can be observed in reality, since number of industries rely on contractors to carry out the maintenance operations.

Another important point worth mentioning here is the %age of accidents occurred during the shut-down conditions. During plant's shut-down conditions apart from the maintenance, waste disposal activities may also be carried out that could potentially lead to accidents. Another cause of failures during the shut-down conditions comes from the hazardous wastes, that still require the supervision. But due to the shut-down conditions this supervision can be overlooked hence leading to potential accident.

Table 24: Comparison of total accidents and accidents caused by the HOF

Time period	Total accidents	Accidents caused by HOF	%age of accidents
1988-2000	240	103	43
2000-2012	198	94	47

During this accident analysis, type of hazard (according to the characteristic of released material) is also observed. It can be seen from the Figure 23 that major accidents involving HOF occurred, when flammable material was present (≈51%). It can be said that toxic materials have an enhanced protection, therefore had led to fewer number of accidents compare to flammable materials. However, in some of the cases it was difficult to classify the material into one of the considered types which is about 7% of the cases. The higher number of flammable hazard could also be possible due to vast usage of flammable materials (i.e. hydrocarbons) in chemical process plants.

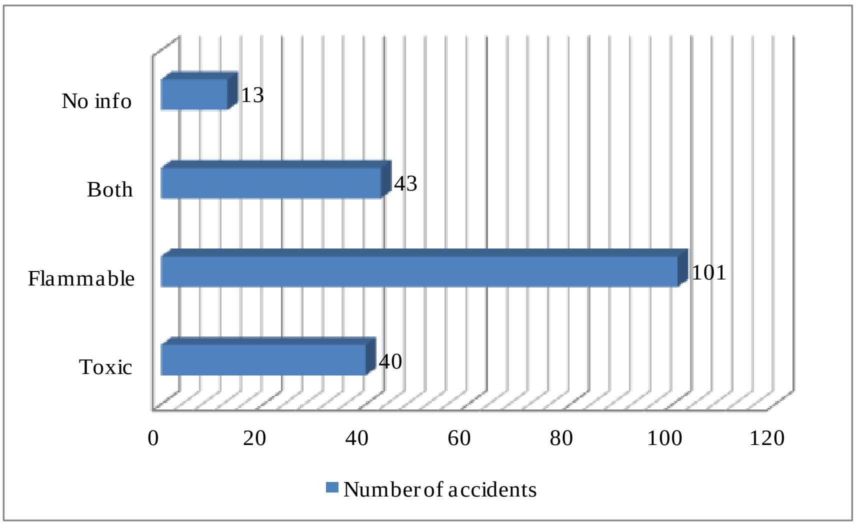


Figure 23. Accident involving different materials

As described earlier that accidents have been studied according to their initiating causes and the safety barriers, which were observed to prevent or mitigate the initiating causes.

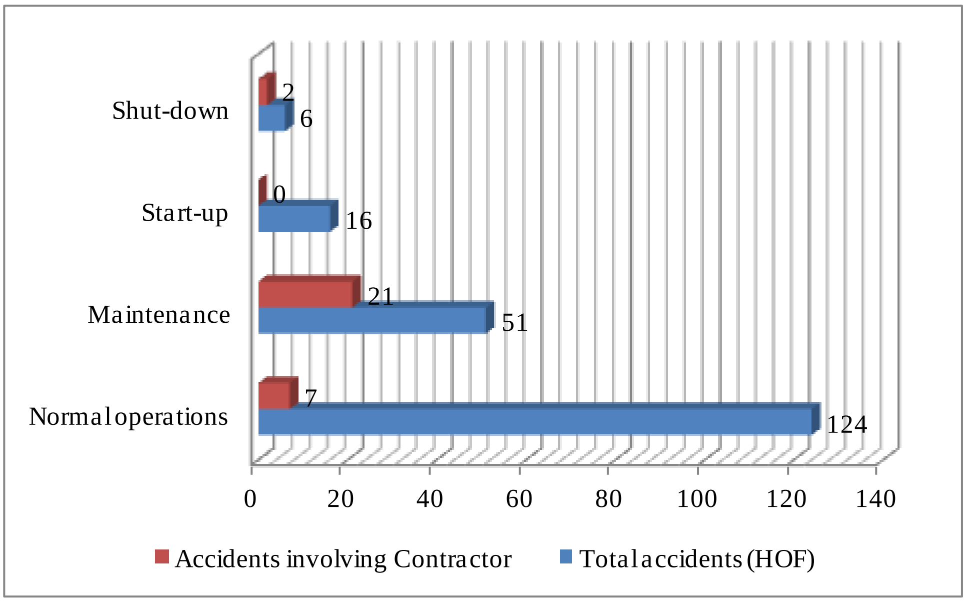


Figure 24. Total accidents (HOF) and accidents involving contractor in plant’s different operational stages

The description of accident models can be found in section 4.3 (Table 19).

The Figure 25 reports the number of accidents occurred in each of the accident models. In order to ease the understanding of accidents models, the following explanation has been provided. The prefix “1” corresponds to failure of both “technical” and “human” aspects during the initiating cause. The prefix “3” corresponds to failure of “technical” aspects while prefix “5” corresponds to failure of “human” aspects, as initiating causes. It can be observed that accident models with prefix “5” have the highest number of accidents since they correspond to “human” failures, which observed implicitly and explicitly during this analysis compare to the “technical” failures (i.e. prefix “3”) which only observed when affected by the human and organizational factors. Therefore, it can be said that models “3” can provide an insight into the value change of λ (i.e. failure rate) as affected by the organizational parameters (e.g. to operator and maintain equipments in operations). However, modification of failure rate according to the organizational attributes is not scope of this work, that required a detailed analysis focused on the failure of the technical equipments.

However, for certain accidents it was difficult to classify them into one of the accident models or the accident evolution exhibits too complex situation to identify them into any of the adapted models. These accidents are considered in category “others”.

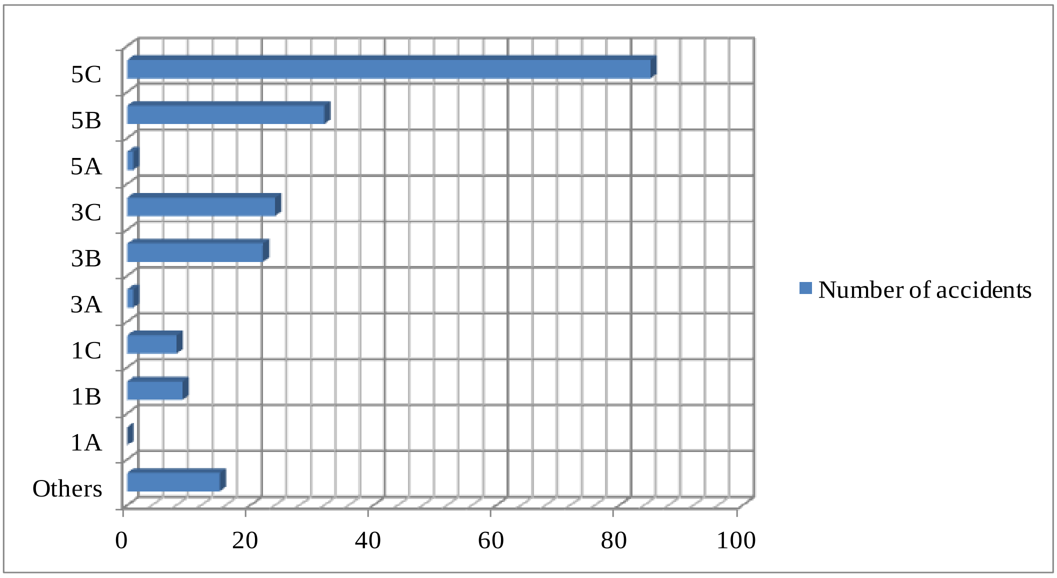


Figure 25. Number of accidents occurred in each of the accident models

The other comparison of the accident models and their %age share can be seen from Figure 26 which reports the ratio of accidents occurred in each of the operational layers. As described earlier, the suffix of a model only changes with the change in the subsequent safety barriers (i.e. prevention/ mitigation safety layers). The models with suffix “A” shows that both “manual and automatic” safety barriers were present and failed hence led to an accident. The models with suffix “B” shows that only one of the safety barriers among “manual and automatic” was present and failed, while for the models with suffix “C” no safety barriers were observed.

A fewer ratio has been observed for the models with suffix “A”, since both manual and automatic safety barrier were present for these models (e.g. 1A, 3A, 5A). However, these estimations based on assumption that accident reports (or post-accident investigation) includes all the information about the possible safety barriers during an accident.

Furthermore, in order to see the effectiveness of the barriers (i.e. automatic or manual) against different initiating causes (e.g. technical or human failure) a comparison is shown in the Figure 26. The Figure 26 illustrates the %age of accidents against each of the accident models and against each of the initiating causes (i.e. technical & human, technical, human) correspond to 1,3 and 5, respectively.

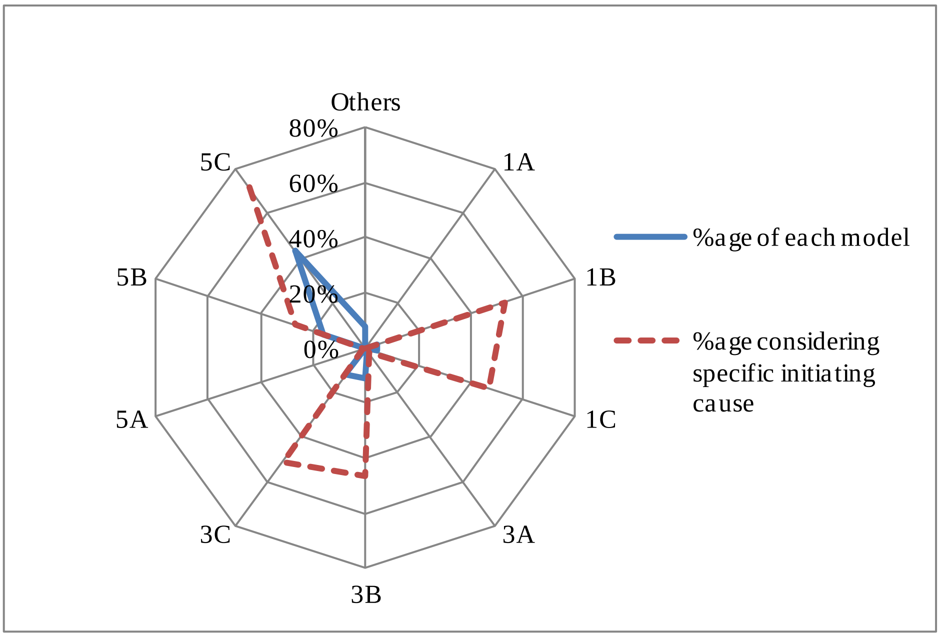


Figure 26. Ratio of accidents across accident models

It can be observed from the Figure 26 that the models with prefix “3” and “1” exhibit negligible variation when moving among the models of same class. If it is assumed that for the models with suffix “B” only human barriers were present, since scope of this work is to observed the human and human initiated technical failures. Then it can be said that “human” role as safety barrier against the technical initiated failures is less effective compare to when applied to human initiated failures. Since, for human initiated failures (i.e. prefix 5) much higher ratio is observed when no safety barriers were available (i.e. 5C) compared to when a safety barrier is available (i.e.5B).

However, it could also be possible that human initiating causes are mitigated by the technical safety barriers. However, most of the human failure (as initiating cause) occurred due to lack/ insufficient manual supervision of the operations.

The Figure 27 illustrates the number of accidents and the main equipments involved in the accident. It can be seen from the Figure 27, that majority of accidents are caused due to vessel type equipment (i.e. 40%) followed by the pipework (i.e. 31%) and in-line equipment (i.e. 26%). The details about the equipment and their specification can be found in the Table 22. However, in some cases (i.e. 3%) it was not possible to identify the main involved equipment due to insufficient information in eMARS database.

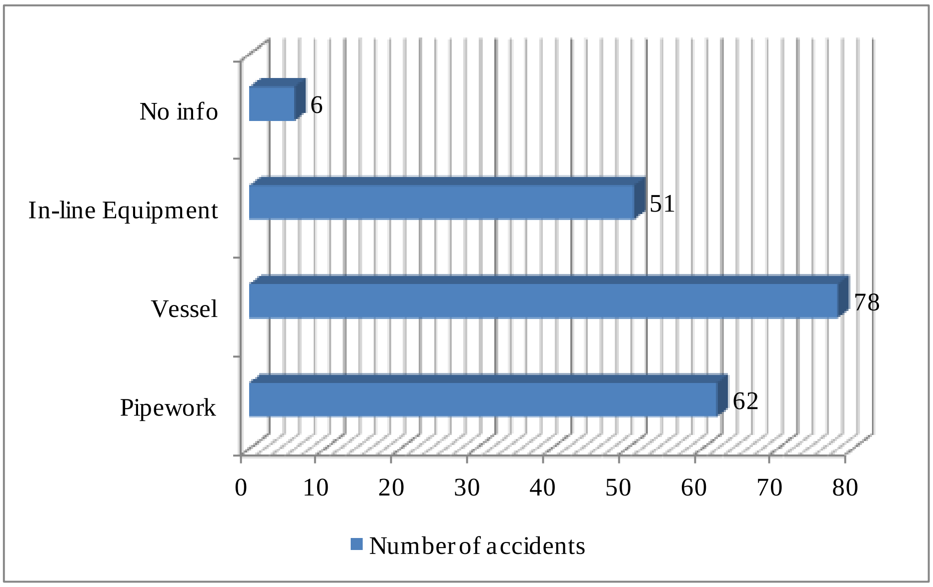


Figure 27. Number of accidents for different equipment types

Furthermore, a comparison between initiating causes and the type of equipments has also been done. The details about the initiating causes can be found in the Table 19.

The Figure 28 illustrates a comparison of the initiating causes to the accidents and the involved equipments. It can be seen that vessel types equipment was involved during majority of human failures (as initiating causes).

The human failures that corresponds to vessel type equipment are mainly related to the cleaning / maintenance activities of toxic/ flammable storage tanks. Since these activities are usually carried out by the contractors and therefore in the absence of an effective safety management system or procedures, failure are more probable to occur.

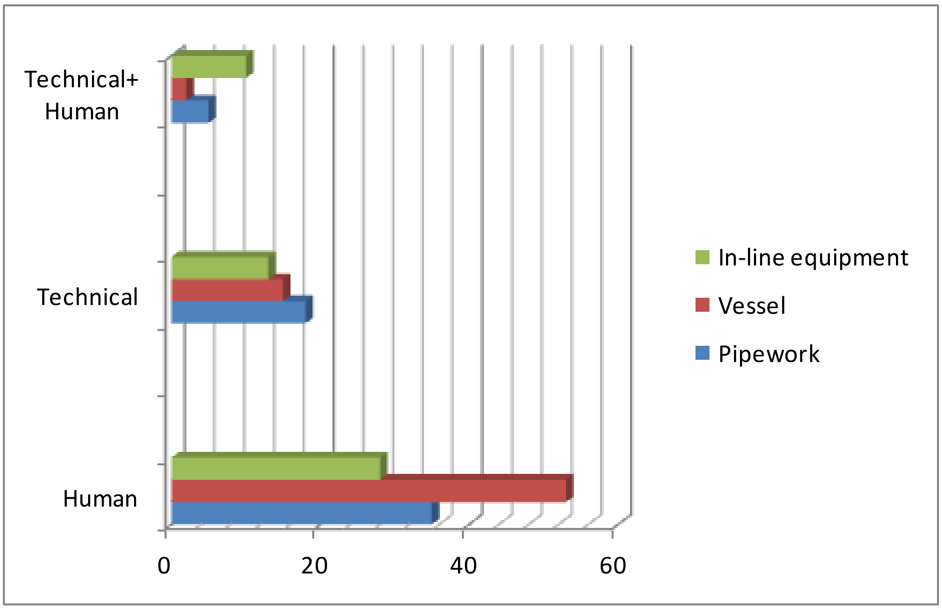


Figure 28. Comparison of initiating causes and type of equipment

Another possible explanation of these failures could be that these activities are usually overlooked during the initial risk assessment studies (i.e. HAZID/ HAZOP, QRA etc). Therefore, it is recommended to consider these maintenance activities during the preliminary risk assessment studies and therefore can be reflected during more detail risk assessment studies in later stages of a project.

In contrary, the technical failures correspond mainly to the pipework compared to other equipment types. This could be due to the wide usage of paperwork in chemical process industry.

In similar way, a comparison can also be made between the initiating causes to accidents and the substances released, as shown by the Figure 29. This phenomenon can be explained that in general toxic substances have better protection that the flammable substances assuming that both types of substances are equally used in chemical process plants.

However, the fewer accidents during the “technical” failures cannot be compared as such with the other initiating causes. Since, in this scope of work the emphasis has been done on the human factors and human factors related failures than the technical failures. In order to draw more absolute conclusions in this regard require to determine the scope of accident analysis, accordingly.

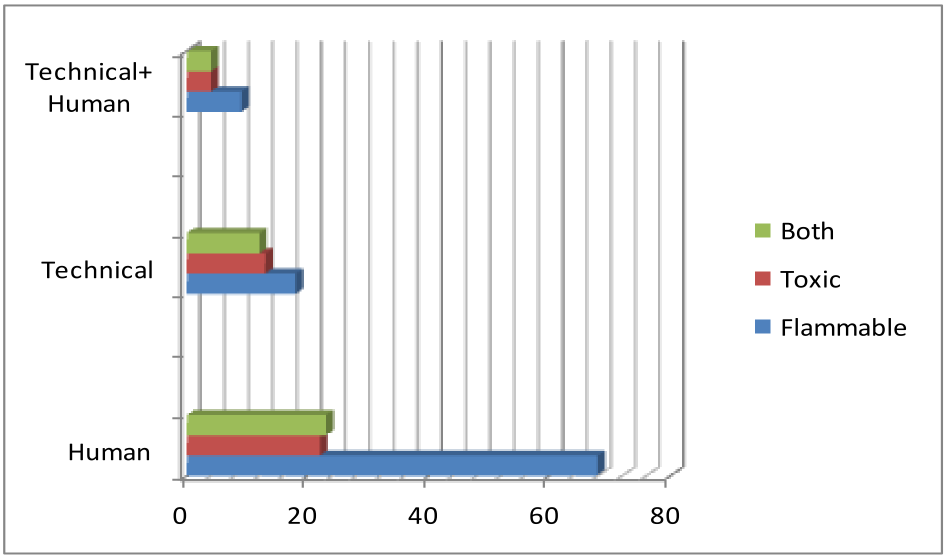


Figure 29. Comparison of initiating causes and type of substance

5.2 Checklists for human and organizational factors

The checklists have been developed for the human and organizational factor according to the attributes which were observed during the accident analysis.

The checklists are a useful way to identify that known hazards and threats have been identified and assessed. The checklists are normally drawn from standards and operational experience and therefore focus on areas where the potential for mistake is high or where the problem has already occurred in the past (ISO 17776, 2000). Therefore, in this work it has been decided to develop the checklists to identify the potentially critical human and organizational attributes based on analysis of past accidents.

In the MEDIA methodology, the Human Error Identification (HEI) checklists were originally adapted from the error classification developed by the (Embrey, 1992) and then later modified/ improved in the light of observed accidents. The human activity and errors against the selected human factors taxonomy class can be seen in the Table 25. This table has been developed as the result of the accident analysis and most of the reported aspects had led to the accident in the past with sufficient threshold that accidents were reported to the eMARS. In the Table 25 and in the 3rd column, underlined errors/ deviations are those errors that have led to accidents in the past.

The rationale to collect the specific activity and errors against each of the taxonomy are following:

- It helps to remain consistence throughout the accident analysis, since aspects can be considered in same taxonomy class according to their description:
- Aspects collected in the Table 25 can also assist an analyst to identify the potentially critical human interventions and associated errors, prospectively.

During the proposed methodology, it is recommended to use the checklists in the Table 25 to identify the potentially critical human interventions. Since these aspects have already led to accidents therefore it is much likely that they can cause accidents again.

Similarly, Table 26 reports the human interventions and associated errors/ deviations during the recovery actions, when there is already a failure or abnormal situation.

There are number of instances, where it is difficult to classify the interventions among operational or recovery layers. For example, for supervision activities it is difficult to classify them clearly among the operational or recovery layer. In this scope of work, actions by a supervisor and relevant failures are considered in the recovery layer, while monitoring / supervision of process parameters are usually considered in the operational layer.

The accident sequences have also helped to classify the actions among the operational or recovery layers. For example, when it is first technical or human failure then it has been considered in the operational layer but when there is already a failure and then the role of intervention is to mitigate the consequences then they are considered in the recovery layer.

The Table 27 reports the organizational factor taxonomy and the relevant organizational attributes which were overlooked and hence led to the accidents or had a contribution to the human / technical failures, that ultimately led to an accident.

During the organizational factor taxonomy, it has been assumed that an organization has to carry out certain actions in a plant’s life from design through operation to decommissioning. If an organization fails to carry out these tasks in-time, it may lead to technical or human failures and consequently cause an accident. In this scope of work, mainly design and operational stage of a plant have been considered while overlooked the decommissioning phase. Since, most of the accidents reported to eMARS were in the operational stage and have contribution from the design phase or actions were overlooked during the design phase of a project.

Table 25: MEDIA human action and error classification during operations

Human factor Taxonomy classes	Related activity types	Relevant errors/ deviations
10 100:Monitoring equipment from field	10 110: Monitoring of vibrations (e.g. vibration from pump operations etc).	10 111: Monitoring omitted 10 112: Monitoring incomplete
	10 120: Visual checks for leaks and gas release (e.g. flaring etc).	10 121: Monitoring omitted 10 122: Monitoring incomplete
	10 130: Monitoring of automated safety functions (e.g. to ensure if not disarmed etc).	10 131: Monitoring omitted 10 132: Monitoring incomplete
	10 140: Monitoring of alarms / indicators / equipments / PH displays (i.e. display monitoring / readings etc).	10 141: Monitoring omitted 10 142: Monitoring incomplete / wrong
	10 150: Supervision for potentially wrong sequence of operations.	10 151: Monitoring omitted 10 152: Monitoring incomplete
	10 160: Supervision of maintenance operations / hazardous / contractor's operations (e.g. cleaning/ maintenance of units, welding operations etc).	10 161: Monitoring omitted 10 162: Monitoring incomplete
	10 170: Supervision of potentially risky operations (e.g. loading / unloading operations, fluid transfer operations etc).	10 171: Monitoring omitted 10 172: Monitoring incomplete
	10 180: Monitoring / visual inspection of valves positions, seals, flanges etc.	10 181: Wrong/ Incomplete monitoring

		10 182: Monitoring omitted
	10 190: Visual monitoring for possible external corrosion (e.g. external corrosion of pipelines and storage tank basements etc).	10 191: Action omitted 10 192: Action incomplete / insufficient
10 200: Monitoring/ operating equipments from control room	10 210: Monitoring / actions related of remotely operated valves (e.g. ESD valves. flow control valves etc).	10 211: Action omitted 10 212: Action too little / too much 10 213: Action in wrong direction
	10 220: Monitoring / actions related to process parameters (e.g. change in pressure, temperature and flow etc).	10 221: Action omitted 10 222: Actions too much/ too little
	10 230: Monitoring / actions related to switching of units (e.g. switching between multiple standby or parallel units etc).	10 231: Action in wrong direction
	10 240: Monitoring / actions related to unit start-up and shut-down (e.g. especially in plant start-up and maintenance operations etc).	10 241: Wrong action on right object 10 242: Right action on wrong object
	10 250: Monitoring / actions related to process alarms in control room.	10 251: No detection 10 252: Undue silencing of alarms (i.e. violations) 10 253: Action cannot diagnose correctly following an alarm

	10 260: Supervision for potentially wrong sequence of operations (e.g. in case of multiple steps are performed to attain an objective).	10 261: Supervision omitted 10 262: Supervision incomplete / insufficient
	10 270: Supervision of maintenance operations / hazardous / contractor’s operations (e.g. cleaning/ maintenance of units, welding operations etc), where applicable from CR instead from field.	10 271: Supervision omitted 10 272: Supervision incomplete
	10 280: Supervision of potentially risky operations, where applicable from CR.	10 281: Supervision omitted 10 282: Supervision incomplete
	10 290: Monitoring of actions related to the isolation of pipelines and process units.	10 291: Action omitted
10 300: Communication	10 310: Communication between shifts.	10 311: Information / communication not transmitted 10 312: Wrong information / communication transmitted 10 313: Information / communication transmission incomplete
	10 320: Communication between process operators and supervisors.	10 321: Information / communication not transmitted 10 322: Wrong information / communication transmitted 10 323: Information / communication transmission incomplete

	10 330: Communication among process operators (e.g. control room and manual on-field operations, truck operators in case of fluid transfer operations) - in case when multiple parties are involved during an operation.	10 331: Information / communication not transmitted
		10 332: Wrong information / communication transmitted
		10 333: Information / communication transmission incomplete
	10 340: Communication between different personnel (e.g. process plant personnel and maintenance personnel especially when carried out by an outside contractors etc).	10 341: Information / communication not transmitted
		10 342: Wrong information / communication transmitted
		10 343: Information / communication transmission incomplete
	10 350: Communication among supervisors.	10 351: Information / communication not transmitted
		10 352: Wrong information / communication transmitted
		10 353: Information / communication transmission incomplete
10 400: Manual tasks on-field	10 410: Manual operation related to valves / pumps / sealing kits / flanges screws etc.	10 411: Action omitted (e.g. left valve open /close, blind flange operations etc)
		10 412: Action in wrong direction

		(i.e. open / close a valve when required to do the opposite operation)
		10 413: Action too little / too much (e.g. for partially open / close valves etc)
		10 414: Right action on wrong object
		10 415: Un-necessary action (i.e. including violation, wilful disobedience etc).
	10 420: Manual operations related to on-field alarms (i.e. Switching off /silencing an alarm).	10 421: Switched off/ silencing an alarm (required for prevention/ mitigation safety operations)
		10 422: Violation in alarm operations.
	10 430: Manual testing/ calibration of on-field operations.	10 431: Action omitted
		10 432: Right action on wrong object
		10 433: Wrong action on right object
	10 440: Manual maintenance operations (e.g. welding, opening / cleaning of unit, isolation operations (use of blanking plate or spectacle blind for unit isolation), pigging operations, change of filters, pressure test and operations related to SISs).	10 441: Action mistimed/ not correct
		10 442: Violation in maintenance operations

		10 443: Wrong action on right object
		10 444: Right action on wrong object
	10 450: Fluid addition/ transfer operations (e.g. loading / unloading operations, fluid addition and mixing operation).	10 451: Action omitted
		10 452: Action mistimed, not correct
		10 453: Right action on wrong object
		10 454: Procedures not followed (i.e. Violations)
	10 460: Manual operations related to pipe / flexible hose connections or relevant pipe work operations.	10 461: Right action on wrong unit
10 500: Reporting	10 510: Report about faulty operation.	10 511: Information not transmitted
		10 512: Wrong information transmitted
		10 513: Information transmission incomplete or in-sufficient.
	10 520: Report about equipment faulty state, discovered during the operations (e.g. alarms taken off, removal of certain instrumentation from process etc).	10 521: Information not transmitted
		10 522: Wrong information transmitted
		10 523: Information transmission incomplete

Table 26: MEDIA human action and error classification during recovery (i.e. prevention / mitigation)

Human factor Taxonomy classes	Related activity types	Relevant errors/ deviations
30 100: Monitoring	30 110: Supervision of potentially risky operations (e.g. loading / unloading operations, fluid transfer operations, valve operations etc).	30 111: Not provided in-time monitoring / supervision
	30 120: Monitoring of PH or other process parameters for fluid mixing operations (where applicable).	30 121: Monitoring of PH or process parameter omitted / insufficient monitoring.
	30 130: Monitoring of the pipe connection operations.	30 131: Action incomplete/ not timed.
30 200: Monitoring / operating equipments from control room	30 210: Monitoring / actions related to process parameters (e.g. pressure, temperature, flow rate etc) followed by an accident.	30 211: Action too much/ too little
	30 220: Monitoring / actions related to process alarms (i.e. followed by a severe abnormal situation compare to operational errors).	30 221: Undue silencing of alarms
	30 230: Actions related to pipe works followed an accidents (e.g. loss of containment) (i.e. isolations or pipe connection).	30 231: Error of commission
30 300: Communication	Not observed	
30 400: Manual tasks on-field	30 410: Operations followed an accident (i.e. spill / leak etc).	30 411: Error of commission
	30 420: Operations following an in-line unit failure (i.e. valve, disc etc).	30 421: Error of commission
	30 430: Actions related to pipework followed an accident (e.g. loss	30 431: Violations (i.e. procedures not

	of containment) (i.e. isolations or pipe connection).	followed)
	30 440: Operator actions related to automatic control systems (i.e. SISs) followed an abnormal situation.	30 441: Error of commission
30 500: Reporting	Not observed.	

Table 27: MEDIA organizational factor taxonomy and error classification

Organization factor taxonomy class	Related organizational actions (attributes)	Relevant errors/ deviations
20 100: Training	20 110: Training about normal operations with a refresher.	20 111: Training inadequate
	20 120: Enhanced training about most hazardous scenarios / actions as identified in a safety report (e.g. pressurized equipment).	20 121: Training omitted 20 122: Training inadequate
	20 130: Training about response during an emergency situation (e.g. spill or leak).	20 131: Training omitted
	20 140: Training about the maintenance activities / operations.	20 141: Training omitted
20 200: Design	20 210: Ensure equipment requirements and specifications (e.g. flanges, heat exchangers, vessel type) according to the potential risk.	20 211: Action omitted
	20 220: To provide necessary interlocks / automatic valves (with verification of shutting time provided by interlocks, verification of set pressure of rupture disks etc).	20 221: Action omitted
	20 230: Calculate risk for all the operations and incorporate during the design phase (e.g. loading/unloading operations, power failure	20 231: Action omitted

scenario and dirt deposition scenario etc).	
20 240: Consider periodic maintenance of units and adjust accordingly in design phase of a plant (e.g. trap of units to collect the spillage, access to perform the maintenance operations etc).	20 241: Action omitted
20 250: Consider potential human errors during operations and incorporate in design phase of the plant (e.g. including ergonomics etc).	20 251: Action omitted
20 260: Consider vibrations of units and pipelines due to diversions (e.g. fatigue fracture due to vibrations can led to a leak in pipeline and fittings etc).	20 261: Action omitted
20 270: Provide redundancy (i.e. double alarms and interlocks) for potentially high risk operations (e.g. loading and unloading operations etc).	20 271: Action omitted
20 280: Consider proper type/class of an equipment/ material/ monitoring devices (e.g. pumps, heat exchangers, building material, scaling devices, filter upstream to safety valves especially after columns) depending upon the operations and involved substances.	20 281: Action omitted
20 290: Consider to add double drainage valves (where appropriate) in case of valve opening due to solid plug of materials. (to avoid the material release to atmosphere).	20 291: Action omitted
20 2100: To provide the trap for units, where there is a possibility for leakage/ seepage (e.g. pump carrying hazardous material etc).	20 2101: Action omitted
20 2110: To provide the layers of protection (where it seems credible) (e.g. add the alarms, double alarms etc) before starting the automatic emergency sequences.	20 2111: Action omitted

20 300: Procedures	20 310: Provide procedures for the normal operations.	20 311: Action omitted/ Insufficient
	20 320: Provide procedures for the abnormal / emergency operations (e.g. pipeline de-blocking Spill, leak etc).	20 321: Action omitted
	20 330: Provide safe procedures / tools for the maintenance operations (maintenance of units, protective clothes in work, permits for hazardous work etc).	20 331: Action omitted
	20 340: Provide more strict procedures for hot work applications / hazardous scenarios (Hazardous fluid addition, cleaning of tanks).	20 341: Action omitted
	20 350: Provide procedures for the outsource contractor's work (e.g. maintenance related activities, loading operations etc), also ensure the active supervision of all operations related to contractors.	20 351: Action omitted
	20 360: Assess the Implementation of procedures (i.e. with respect to difficulty / impracticality etc).	20 361: Action omitted
	20 370: To update the procedures following changes (add as an integral part of the "management of change" framework).	20 371: Action omitted
	20 380: Procedures for un-expected weather patterns leading to a hazardous situation (e.g. wind speed, direction etc), if required.	20 381: Action omitted
	20 390: Provide procedures for the inspection of critical components (e.g. critical flanges, critical storage tanks etc).	20 391: Action omitted
	20 3100: Provide non-routine job procedures (e.g. for temporary or infrequent operations).	20 3101: Action omitted
	20 3110: Provide procedures for equipments use / maintained by	

	contractor at different facility (e.g. pressure test procedures for temporary storage tanks prior to their application) or at least should have detail knowledge about adapted procedures by the contractor.	20 3111: action omitted
20 400: Management	20 410: Adequate manning level in accordance with the safety studies (to carry out the desired actions etc).	20 411: Action omitted
	20 420: Define roles / responsibilities for operators, accordingly.	20 421: Action omitted
	20 430: Eliminate/ minimize the communication problems among different involved parties (e.g. different departments or parties etc)	20 431: Action omitted
	20 440: To Follow latest / proper safety standards / rules / software and ensure to provide adequate process /risk analysis (e.g. to provide product or off-spec storage in case of any natural hazard and calculations of anticipated corrosion rate should be based on international standards).	20 441: Action omitted
	20 450: Provide adequate knowledge about the properties of chemicals / fluids used in a plant, also to share layout of critical plant sections with all involved parties.	20 451: Action omitted
	20 460: Handling/ communication of management of change.	20 461: Action omitted
	20 470: To update the process/ control according to risk assessment/ safety studies.	20 471: Action omitted 20 472: Action insufficient
	20 480: To carry out the risk assessment studies comprehensively/ before and following major modifications.	20 481: Action omitted
	20 490: To provide / ensure an effective maintenance/ inspection.	20 491: Action omitted

	plan.	
	20 4100: To provide standard for temporary pieces (e.g. T-piece to be used during maintenance operations), standard / procedure to use an old pipelines (e.g. pressure test, check for leaks before to use for transportation of fluid).	20 4101: Action omitted
20 500: Safety culture	20 510: Ensure the adequate safety leadership / culture.	20 511: Action omitted
	20 520: Ensure an efficient and effective safety communication (e.g. accident and lessons learned from accidents).	20 521: Action omitted
	20 530: Ensure to provide adequate response to complaints related to operations and existing safety stature.	20 531: Action omitted
	20 540: Ensure steps to avoid the blame culture inside the organization.	20 541: Action omitted

6 Quantification of human and organizational factors

This section presents the procedures adapted to estimate the human error probability from the accident analysis, assumptions and limitations. Furthermore, weightage of organizational factors on human reliability as obtained from the analysis is also presented.

6.1 Estimation of human error probabilities

The estimation of HEPs is always subject to some assumptions, especially if it is based on the past experience. In order to define the HEP, it is not only necessary to know the number of errors that have occurred for each task and how often the task was performed but also the circumstances under which the task was performed (OECD, 1998).

Furthermore, as stated by the (OECD, 1998) that the HRA methods can be classify according to the level of the data scale. For example, three main scales have been identified as:

- Absolute scale
- Relative scale
- Ordinal scale

The absolute scale can provide the HEP in the range from 0 to 1, where 0 means no error and 1 means a sure failure. The relative scale can provide information about the two tasks in comparison, for example task 1 has twice as higher probability of failure as the task 2. While, the ordinal scale can provide information like task 1 is more likely than the task 2. The ordinal scale cannot identify the extent of the scale.

Normally, HEP can be estimated by an equation of the form (i.e. n/N) where n is the observed frequency of failure of events and N is total observable events. However, if one decides to use the past experience (i.e. accident analysis) to quantify the HEP then aforementioned equation is not valid, since accidents are always reported by a certain threshold value. The reporting threshold values are determined by the management or authorities. In this scope of work, the reporting threshold is determined by the Annex VI of the “Seveso Directive”. This aspect is also highlighted by the (Sträter, 2000) who has further illustrated the problem of determining the probabilities from the operational experience because from operational experience one can only determine the limited frequencies having the following form shown in the Eq. 9.

$$\text{h(erroneous action of type i | event above a certain reporting threshold)} \qquad \text{Eq. 9}$$

Therefore, if one decides to calculate the HEP from operational experience then total number of events related to an action type are unknown and also the total failures are unknown since errors are only reported above a certain threshold.

Furthermore, the comparison of HEP (i.e. from THERP) with the operational data as adapted in this work is only permissible if one can demonstrate that as argued in the CAHR method (Sträter, 2000):

- The number of requirements in the collected events corresponds to those of HEP values;
- The data from the Swain and Guttman (i.e. THERP) also have the same statistical information as of the obtained data from the operational experience.

The rule based behaviour is associated to make the choices, sometimes these choices could lead to accidents. Since, the rule based behaviour is connected to the idea that how much an operator is familiar with the task. This can be assume to be attainable through the idea that how often an operator perform a certain action of type of i (i.e. frequency of use) (Sträter, 2000). Therefore, it can be assumed that the HEP (i.e. from THEPR) can be compared with the operational experience (frequencies of failure).

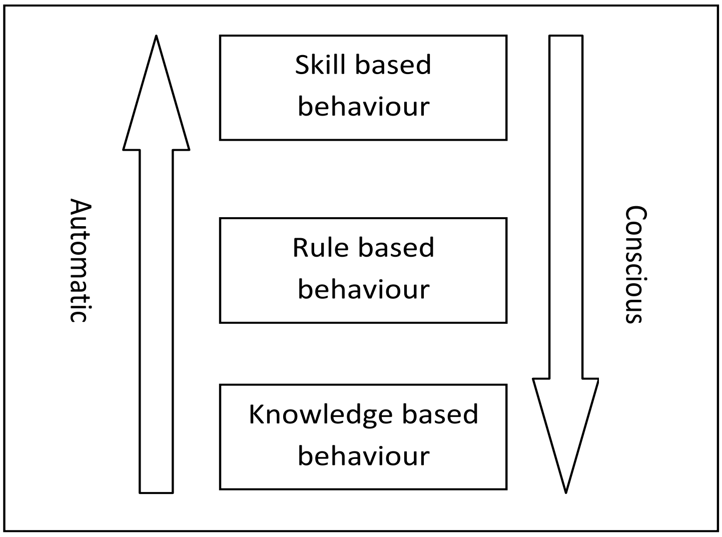


Figure 30. Different types of operator's behavior and their requirements

The Figure 30 illustrates the different types of operator's behaviour and their requirements. It can be observed that for the rule based behaviour, that is guided by rules/ procedures, recognition of the situation. Therefore, right procedures play a role in rule based behaviour. The skill based behaviour is based on the spontaneous response of the operator. This response can be driven by the learned skills. However, this response is rather automatic and less rely on the cognitive traits of the operator. On the other hand, the knowledge based behaviour is driven by the conscious of the operator (i.e. cognitive skills etc) and less automatic compare to the other response types. At the same time, it can also be assumed with certain confidence that same kind of operational experience has been utilized in the THERP database (i.e. used in this scope of work) without precise knowledge of the system. Therefore, based on these arguments it is justifiable to compare the observed frequencies (from the operational experience) with the THERP database.

The Figure 31 illustrates the concept that has been used in the newly developed methodology (i.e. MEDIA). It has been assumed that humans have a tendency to make errors even in an ideal working condition, these types of errors are interpreted as the inherent errors or failures.

Then there are errors that are caused by the affect of the PSFs that can be interpreted as the errors caused by the external PSFs.

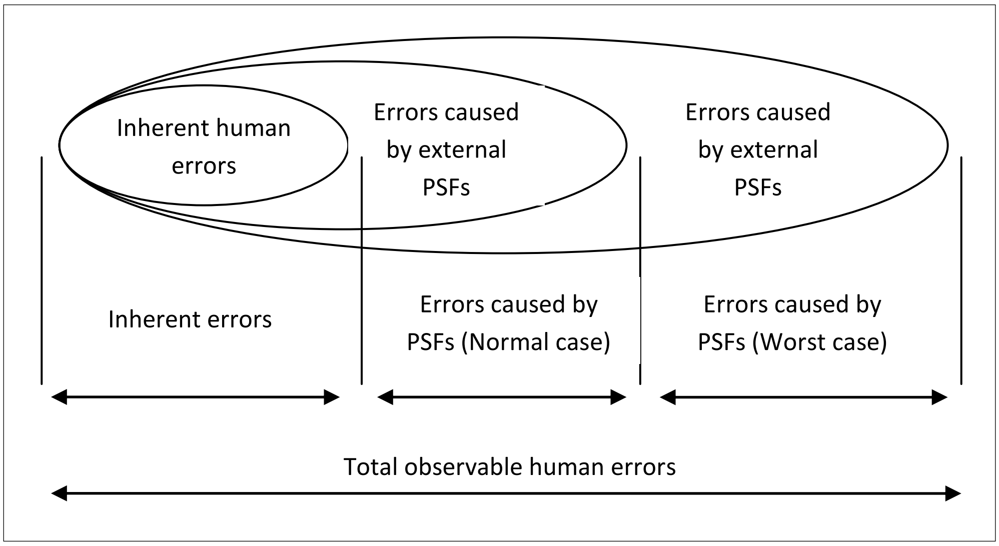

Inherent human errors
Errors caused by external PSFs
Errors caused by external PSFs
Inherent errors
Errors caused by PSFs (Normal case)
Errors caused by PSFs (Worst case)
Total observable human errors

Figure 31. Inherent human errors and errors causes by the PSFs

The rate of accidents (i.e. failures) caused by the external PSFs is determine by the situation of the PSFs. The better the situation of the PSFs, the lower is the error rate caused by the external PSFs. However, worst situation of the external PSFs can enhance the error rate caused by the external PSFs.

It can also be argued that external PSFs might also have a +ve effect on the human error rate. But, currently the +ve effect of the PSFs is not considered in this scope of the work.

The main uncertainties in this assessment are caused due to the following elements, some of these elements have been identified by the (Swain and Guttmann, 1983) :

1. The stochastic variability within an individual and among the performance of different individuals;
2. Identification of the all relevant PSFs, their interactions and effects on the

performance of an operator;

3. Deficiencies/ limitations in the post-accident investigation / reporting to identify the causal factors that have led to the accidents;
4. The insufficient number of events corresponding to an action class;
5. Limitation due to the subjective nature of the assessment (e.g. the accident analysis performed by two different individuals might lead to different results to identify the causal factors to an accident).

The first type of uncertainty can be handled by the assumption of selecting a range ratio (used in the lognormal distribution) that is based on some of studies in the field of the adult intelligence (e.g. Wechsler range ratio etc). While, the second type of uncertainty can be minimized by an improved reporting in the eMARS system. The 3rd type of uncertainty cannot be addressed in this scope of work, that is related to the post-accident investigation procedures. The 4th type of uncertainty can be considered in defining the Error Factor (EF) against a HEP value. The less the HEP corresponding to fewer observed events hence the more will be its corresponding uncertainty. This concept has been considered in defining the EF. The last type of uncertainty can be improved by extended the analysis to more than one individuals. However, given the subjective nature of whole risk assessment process, this type of uncertainty has been accepted at the moment.

Furthermore, the considered taxonomy for human factors (from Table 20) has been recorded for number of instances observed during the accident analysis. The model for the inherent human errors and the total human errors can be observed in the Figure 31.

The Table 28 reports the observed instances against the considered human factor taxonomy in both inherent and total human errors cases. It can be observed from the Table 28 that major accidents occurred when operators are performing manual tasks on-field operations. Since, high numbers of daily operations are carried out by the operators as manual task on-filed in the chemical process plant.

Surprisingly, a high number has also been obtained in case of “diagnostic” monitoring task. These cases correspond to those situations when operator/ supervisor were responsible to carry out the supervision activities and failed to manage it, hence led to the accidents. Meanwhile, monitoring task in the “Operational” layer also corresponds to number of accidents. These are operator’s monitoring activities that an operator should have carry out but failure in carrying out led to accidents. At the same time, a lower number has been observed corresponding to the control room actions compare to other actions types. Therefore, it can be said that in general control room actions might not be as critical as other action types.

Table 28: Number of instances observed for different action types

Human factor taxonomy	Instances – Inherent human errors	Instances – Total human errors
Monitoring equipment from field (M)	5	14
Monitoring/ operating equipment from control room (A)	1	5
Communication (C)	3	9
Manual tasks on-field (F)	40	107
Reporting (R)	1	3
Diagnostic: Monitoring	8	16
Diagnostic: Control room action	4	10
Diagnostic: Manual tasks on-field	3	8

6.1.1 Lognormal distribution

The lognormal distribution is used quite frequently in reliability and safety studies, primarily due to its characteristic of skewness at one end of the distribution (Red Book, 1997). The lognormal distribution has also been adapted in the THERP database (Swain and Guttmann, 1983). The use of log normal distribution for the Human Error Probability (HEP) has been justified based on the following main aspects:

- Since the performance of the skilled persons tend to bunch up towards the lower end of the distribution, that can be justifiable by using a non-symmetric distribution (i.e. log normal distribution);
- The log normal distribution can readily be adapted to the human reliability studies, since its parameters can be using its two percentiles in contrary to other non-symmetrical distributions.

Therefore, a log normal distribution has been used in this work providing the absence of strong data to contradict its use and due to its use in the existing human reliability studies (e.g. THERP etc).

The relationship to a normal distribution is as follows: If a stochastic variable ln (X) has a normal distribution, then X has a lognormal distribution. The Probability Density Function (PDF) of a lognormal distribution is provided by the Eq. 10, as reported in the (Red Book, 1997):

$$f(X) = \frac{1}{x\sigma\sqrt{2\pi}} .\ \exp\left[-\ \frac{\{\ln(X)\text{ -}\mu\}^2}{2\sigma^2}\right] \qquad \text{Eq. 10}$$

Whereas:

σ is the standard deviation.

μ is the Mean, location parameters of the distribution.

The Error Factor (EF) for lognormal distribution is defined as follows:

$$EF = \sqrt{\frac{X_{0.95}}{X_{0.05}}} = \frac{X_{0.95}}{X_{median}} = \frac{X_{median}}{X_{0.05}}$$

Whereas:

$X_{0.95}$ is the 95th percentile,

$X_{0.05}$ is the 5th percentile

These percentiles are also called the upper and lower Uncertainty Bounds (UCBs). The upper UCBs (i.e. 95th) means that the HEP would be higher than this value no more than 5% of the cases, while the lower UCBs (i.e. 5th) means that HEP would be lower than this value no more than 5% of the cases. Therefore, it can be said that the HEP would lie in the region defined by the UCBs around 90% of the cases.

The sigma (σ) "standard deviation" can be calculated as follows:

$$\sigma = \frac{\ln(EF)}{Z_{0.95}} = \frac{\ln(EF)}{1.645}$$

Therefore, following form of the log normal distribution (i.e. PDF) can be obtained by using the values of sigma (σ), as represented in the Eq.11.

$$\mathrm{f(X)} = \frac{1}{\mathrm{x}.\frac{\ln(\mathrm{EF})}{1.645}.\sqrt{2\pi}} \, . \, \exp^{\left[-\frac{1}{2}\left(\ln(\mathrm{X}) - \mu / \frac{\ln(\mathrm{EF})}{1.645}\right)^{2}\right]} \qquad \text{Eq.11}$$

The median of the log normal distribution is given by (Red Book, 1997):

$$\mathrm{X}_{\mathrm{median}} = \exp^{\mu}$$

The mean of the log normal distribution is given by:

$$\mathrm{X}_{\mathrm{mean}} = \exp^{(\mu + 0.5\sigma^{2})}$$

The variance of the log normal distribution is given by:

$$\mathrm{Var\ (X)} = \exp^{(2\mu+\sigma^{2})} \left\{\exp^{\sigma^{2}} - 1\right\}$$

However, in order to use the log normal distribution for the HEPs, it is required to apply the hypothesized distribution as shown in the Figure 5 and has been proposed by the THERP database.

The hypothesized distribution has been obtained by assuming a standard deviation of 0.42 that can be obtained by assuming a 4:1 range ratio between the percentiles. The range ratio of 4:1 assume that abilities of the best person are 4 times higher than the abilities of the worst person in a random group. The selected range ratio also accounts for the uncertainty coming from the variation among people’s abilities to a great extent. Providing the lack of information to provide more sophisticated approach, it has been decided to use the information providing in the THERP database.

For the tasks performed under stress, the entire distribution tends to move towards right and can be skewed on the left rather than on the right. Therefore, task performed under stress tend to have a higher probability of failure than the tasks performed under normal conditions.

However, the EF across the median HEPs in the THERP database are asymmetric in-contrary to the hypothesized distribution shown in the Figure 5. This was an unnecessary refinement as also argued by the (Swain and Guttmann, 1983). Furthermore, a generic table has been proposed in the THERP database in order to assign the EF against the HEPs. The main assumption of this proposed table is that, the lower HEPs values corresponds to the higher EF values due to the infrequent nature of the actions as can be observed from the Table 14.

Therefore, in this scope of work the HEPs are provided according to the log normal distribution and UCBs are based on the EF illustrated in the Table 14. However, future work can be extended to provide further guidelines on the selection of the EF either based on a distribution (i.e. symmetric EFs) or based on more insight to defines the error factors (i.e. asymmetric EFs). The asymmetric EFs can be defined based on either the values of the HEPs itself or different actions types assuming the different levels of uncertainty or the stress levels.

As mentioned earlier that in this work, HEPs have been obtained from the past accidents analysis. In order to obtain the HEPs from the past accidents, the obtained failure frequencies (or modified frequencies) are compared with the corresponding THERP HEPs by using a probabilistic model. The section 6.1 has already provided the justifications for the comparison of THERP HEPs to the failure frequencies obtained from the accident analysis.

6.1.2 The probabilistic Rasch model – Application of CAHR

The Rasch model has been developed by the George Rasch that can help to analyse the data as a trade off between the difficulty and ability parameters (Rasch, 1960). The (Choppin, 1983) has described the Rasch model as a model that can link the probability of outcome of a single person for an item according to the characteristics of the person and the item. Therefore, the Rasch model is termed as the model for the latent-trait measurements.

During the CAHR development, number of approaches had been applied for the calibration of the observed frequencies (i.e. failure) and had found that the probabilistic Rasch model provides the maximum agreement to the THERP HEP values. Since, more events were collected during the CAHR development compared to the existing study, so it has been decided to use the probabilistic Rasch model to calibrate the observed frequencies according to the approach used in the CAHR model.

According to the Rasch model the response of individuals to the items of an intelligence test can be derived as shown in the Eq.12 and is adapted from (Rasch, 1960), p. 168. It has been assumed in this model, that response of different persons to the same item as well as the responses of each person to all items are stochastically independent. This assumption is also

valid in case of human operations in chemical process industry in which the human operations are independent to a greater extent until there are operations in a series.
The probability of correct response (i.e. $\theta_{\nu i}$) of a person (ν) to an item (i) is expressed as:

$$\theta_{\nu i} = \frac{\xi_\nu}{\xi_\nu + \delta_i} \qquad \text{Eq.12}$$

Whereas:

ξ_ν is a parameter related to a person (i.e. ability).

δ_i is the parameter related to the item (i.e. difficulty).

During some further transformation and simplification, new parameters had been defined for the person's ability and item's difficulty. For example, ξ_ν = W and δ_i = W, against a constant "W" as also mentioned by the (Choppin, 1983). Furthermore, these parameters can also be defined by $\xi_\nu = W^{\xi_\nu}$ and $\delta_i = W^{\delta_i}$, whereas W is again a constant.
However, in some further simplifications introduced by the Rasch and also used in the literature is to fix the constant "W" to the natural logarithmic base (e), as mentioned in the (Choppin, 1983).
After simplifying the Eq.12 by introducing the logarithmic base (e) as a constant, the following form is obtained:

$$\theta_{\nu i} = \frac{e^{\xi_\nu}}{e^{\xi_\nu} + e^{\delta_i}}$$

Dividing both numerator and denominator by e^{δ_i}:

$$\theta_{\nu i} = \frac{e^{t}}{1 + e^{t}}$$

Whereas:

e^t = (ξ_ν - δ_i)

In order to simplify the used terminology in these equations, the following further simplification has been carried out:

ξ_{ν} = X (i.e. ability parameter)

δ_{i} = D (i.e. difficulty parameter)

Therefore, above equation can be re-written as:

$$\theta_{\nu\mathrm{i}} = \frac{e^{(X - D)}}{1 + e^{(X - D)}}$$

The aforementioned equation can be modify in order to obtain the probability of failure as shown by the Eq.13. The Eq.13 had been already been used in the CAHR method and is therefore adapted from the (Sträter, 2000):

$$P_{\mathrm{Failure}} = \frac{e^{(D - X)}}{1 + e^{(D - X)}} \qquad \text{Eq.13}$$

One of the assumptions of the Rasch model is that the latent value and true value of a property are interconnected by an Item Characteristic Curve (ICC). The ICC provides the output value of a property from 0 to 1, therefore it can provide the results in a range that can be used as a probability estimates. As argued by the (Sträter, 2000), that due to this reason the probabilistic Rasch model is suitable for comparing the operational experience with the THERP HEP values.

The parameters of the ICC have been estimated by the (Sträter, 2000) and are as follows:

$$\mathrm{Chances}_{\mathrm{Failure\ of\ task\ of\ type\ i}} = D_{\mathrm{i}} - X$$

In the aforementioned relation, $X = 0$, Since the ability parameter can only be estimated by observing the successful events. However, in this work estimation to the ability cannot be provided as failures have been observed. Also, the ability parameters can be considered as a constant due to the provided education / training compare to the technical system.

The difficulty parameter can further estimate by the following relation:

$$D_{\mathrm{i}} = \frac{n`_{\mathrm{i}} - \mu}{S_{\mathrm{n}}}$$

Whereas:

D_i is estimation of difficulty of task i

$n`_i$ is the anticipated frequency of error of type i

μ is the mean value

S_n is the anticipated deviation

Therefore, based on the newly defined parameters, the following equation can be obtained:

$$P_{\text{Failure of type i}} = \frac{e^{D_i}}{1 + e^{D_i}} = \frac{e^{\left(\frac{n`_i - \mu}{S_n}\right)}}{1 + e^{\left(\frac{n`_i - \mu}{S_n}\right)}} \qquad \text{Eq.14}$$

The Eq.14 can provides the probability of failure of type i event, that are observed n_i times. While, the parameter "S_n" was estimated by iterations using least square method and to find the condition that can provide the maximum agreement with the THERP HEP values.

The anticipated frequencies can be calculated from the observed frequency by the Eq.15 as mentioned in the (Sträter, 2000):

$$n`_i = \left[\frac{m}{m_i}\right] \times n_i \qquad \text{Eq.15}$$

Whereas:

$n`_i$ is the anticipated frequency for task i

m is the number of all events (i.e. 172)

m_i is the number of events for task i (i.e. total human errors).

n_i is the number of events with inherent failure characteristics for task i (i.e. inherent human errors).

The advantage of using the anticipated frequencies rather than the absolute frequencies is that the different action types can be compared on the same scale. Because, some action types might occur more or less frequent than other action types (consequently more or less failure frequencies). This aspect can be taken into account by modifying the absolute frequencies into the anticipated frequencies. Furthermore, (Sträter, 2000) has argued that by using the anticipated frequencies instead of absolute frequencies more correlation can be found between frequencies and the THERP HEP. Another advantage of using the concept of anticipated frequencies is that, the frequency count become irrespective of the numbers of action types considered during the analysis. For example, one can argue that if consider a taxonomy consist of more than five action types, then the overall frequency count might decrease due to the random distribution of the failures among the action types. Consequently, the overall analysis will depend a lot on the action types considered in a taxonomy. The aforementioned arguments can be explained in this work for two possible conditions:

- If failure frequencies have been observed for an actions type: in this case, the anticipated frequency relation will determine the frequency value based on the model adapted in this work (i.e. Figure 31).
- If no failure frequencies have been observed for an action types: in this case, the used checklists will ensure that the particular activity should be or shouldn't be considered against an action type. Then developed checklists will help to remain consistence during the development phase and the possible prospective application phase.

The further assumptions of the Rasch model and its use to compare the frequencies to the THERP HEP can be found in the (Sträter, 2000).

In order to calibrate the anticipated frequencies to the HEP from the THERP, the least square method has been used.

6.1.3 Fitting the model

The first step to fit the probabilistic model was to collect the corresponding THERP HEPs. It has been tried to collect as much as possible the closet THEPR HEPs against the main types of activities considered in each of the action types. However, due to the nature of the accident analysis and the format of THERP database. It is not possible to find the exact correspondence between the considered action types and the THERP HEPs. The Table 29 illustrates the MEDIA action types and the selected THERP HEPs, corresponding EF and the THERP tables. The rationale behind the selection of a specific table and items can be seen in the Appendix V.

The upper and lower uncertainty bounds of the THERP HEPs values have been calculated by considering the log normal distribution and by using the concepts mentioned in the section 6.1.1. Since, the HEP values in the THERP represent the median values of the lognormal distribution.

Therefore, the THERP median values should be converted into mean value for the comparison with the frequencies that have been observed during the accident analysis. The mean values of HEP have been selected because it can also take into account the skewness at each end of the distribution by considering the standard deviation. The procedure to get the mean values can be seen in the section 6.1.1.

Table 29: MEDIA taxonomy and the corresponding THERP HEP values

Action type	THERP values (Median)	Error Factor	Corresponding THERP tables
Monitoring equipment from field (M)	$3{,}00\times10^{-3}$	10	Table 20-27, item (4)
Monitoring/ operating equipment from control room (A)	$1{,}00\times10^{-3}$	3	Table 20-11, item (1) & item (2)
Communication (C)	$3{,}00\times10^{-3}$	3	Table 20-7, item (2) & item (3)
Manual tasks on-field (F)	$8{,}00\times10^{-3}$	3	Table 20-13, item (4)
Reporting (R)	$1{,}00\times10^{-3}$	5	Table 20-22, item (9)
Diagnostic: Monitoring (M)	$1{,}00\times10^{-3}$	5	Table 20-22, item (4)
Diagnostic: Control room action (A)	$2{,}50\times10^{-2}$	10	Table 20-2, item (2)
Diagnostic: Manual tasks on-field (F)	$8{,}00\times10^{-2}$	5	Table 20-16 (item 6)

The next step after the conversion of the median values into the mean values is the comparison with the anticipated frequencies from the accident analysis. The least square method has been adapted in this study in order to compare the data and to fit the model. The object of the least square method is to minimize the distances as can be seen in the following equation Eq.16.

$$\sum_{i=1}^{n}(y_i - \hat{y}_i)^2 \qquad \text{Eq.16}$$

Whereas:

y_i is the observed values (i.e. THERP)

$\hat{y}_i$ is the predicted values (i.e. from Rasch model)

Another aspect that has been considered during the calculations is the uncertainty bounds of the THERP values. According to the THERP database, HEP can subject to variations according to their uncertainty bounds. As the curve obtained from the Rasch model is a S-shaped curve therefore optimal fitting condition has been obtained by satisfying following two main conditions:

- Minimizing the least square distances;
- Maximizing the %age agreement of the predicted values with the THERP uncertainty bounds;

The Table 30 illustrates the THERP mean values, corresponding Uncertainty Bounds (UCBs), anticipated frequencies (i.e. estimated from the absolute frequencies according to the Eq.15) and the estimated values predicted by the Rasch model.

It can be observed from the Table 30 that for the “Monitoring/ operating equipment from control room (A)” has a very low HEP value compare to other action types. This can be explained by the fewer number of inherent human errors corresponding to this action type.

At present condition (i.e. S_n = 5,41), the 75% of the predicted values are within the THERP uncertainty bounds. The two action types that have values outside the THERP uncertainty bounds are:

- Monitoring/ operating equipment from control room (A);
- Diagnostic: Monitoring.

These two values outside the uncertainty bounds can be explained by a difference in the industry types. Since THERP has been developed in the nuclear industry while this accident analysis has been performed in the chemical process industry. The first action type can be explained in following terms: as most of the failure in chemical process industry occur in manual tasks on-field and lesser are associated with the control room actions as compared to the nuclear industry. In the nuclear industry the generic actions/ interventions are control room centric hence more associated failures can be observed from the control room based actions.

While, the second action types that is associated with the monitoring failures during the diagnostic tasks has obtained a higher value than the THERP estimates. It could be possible that, giving the less criticality of the chemical process industry, human actions can be considered during the diagnostic tasks but due to lack of proper training and tools led to errors.

Table 30: THERP mean values, relative frequencies and estimated HEP values

Action type	THERP values (Mean)	UCBs		n`$_i$	Predicted values (Rasch model)
		Upper	Lower		
Monitoring equipment from field (M)	7,99×10^{-3}	3,00×10^{-2}	3,00×10^{-4}	61,4	1,05×10^{-2}
Monitoring/ operating equipment from control room (A)	1,25×10^{-3}	3,00×10^{-3}	3,33×10^{-4}	34,4	7,21×10^{-5}
Communication (C)	3,75×10^{-3}	9,00×10^{-3}	1,00×10^{-3}	57,3	4,97×10^{-3}
Manual tasks on-field (F)	1,00×10^{-2}	2,40×10^{-2}	2,67×10^{-3}	64,3	1,78×10^{-2}
Reporting (R)	1,61×10^{-3}	5,00×10^{-3}	2,00×10^{-4}	57,3	4,97×10^{-3}
Diagnostic: Monitoring (M)	1,61×10^{-2}	5,00×10^{-2}	2,00×10^{-3}	86,0	5,00×10^{-1}
Diagnostic: Control room action (A)	6,66×10^{-2}	2,50×10^{-1}	2,50×10^{-3}	68,8	4,00×10^{-2}
Diagnostic: Manual tasks on-field (F)	1,29×10^{-1}	4,00×10^{-1}	1,60×10^{-2}	64,5	1,84×10^{-2}

The Figure 32 illustrates the comparison of the THERP HEP values and HEP estimates obtained from the Rasch model against the anticipated frequency scale. It can be observed from the chart in the Figure 32, that as the anticipated frequency increases, the corresponding HEP estimates also tend to increase. The maximum value of the anticipated frequency could become equal to the total number of events observed (i.e. 172). This condition corresponds to a hypothetical condition when all the all the failures become equal to the inherent human failure for an action type. In this case the obtained HEP will become equal to one.

However, If the anticipated frequency of an action type is closer to the median value (i.e. 86) then the predicted estimate of the corresponding HEP is closer to 0,5.

It can be seen from the Figure 32 that the Rasch curve follows the THERP HEP values and can predict the values of HEP based on the anticipated frequencies. But, there is always an uncertainty to predict the values outside the model range.

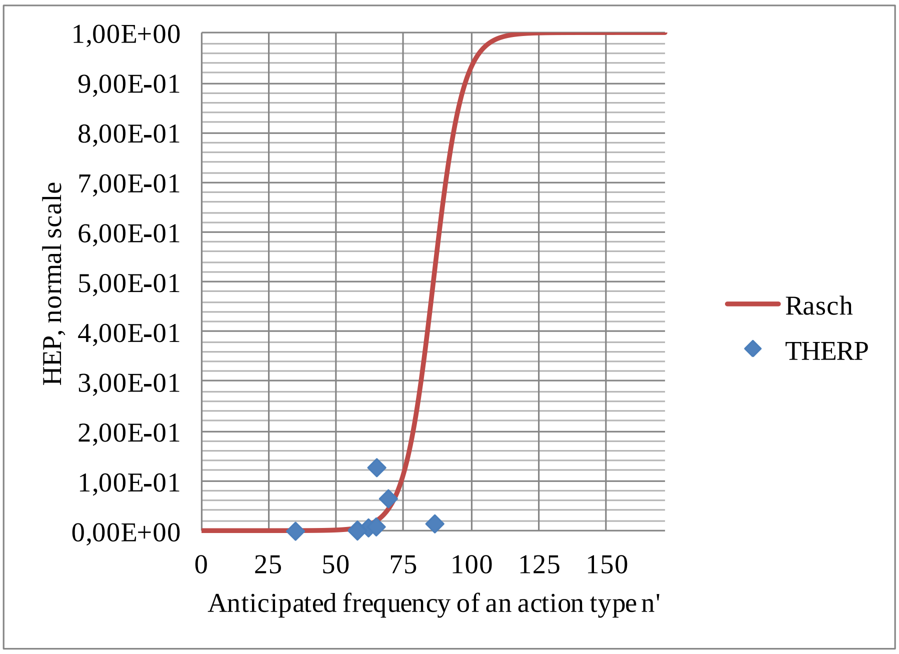


Figure 32: Comparison of THERP values and the estimated values from Rasch (Normal scale)

In order to make more explicit conclusions, there is a need to gather data against more action classes. Hence, required to develop a taxonomy that constitutes much more action types than five. But, this type of taxonomy can pose a challenge during the assessment step and also during the prospective analysis. During the assessment step, the challenge is mainly due to the required detailed information to classify and differentiate among different actions. The more are the actions types, the more information it is required to classify among them. Moreover, the same information acquisition challenge can add more uncertainty into the analysis during the prospective analysis.

In order to observed more precise movement of THERP values along the Rasch curve, the Figure 33 can provide the comparison on the logarithmic scale. The THERP values can be seen along the Rasch curve, however in few cases some deviation has been confirmed, as has already been identified. In order to examine

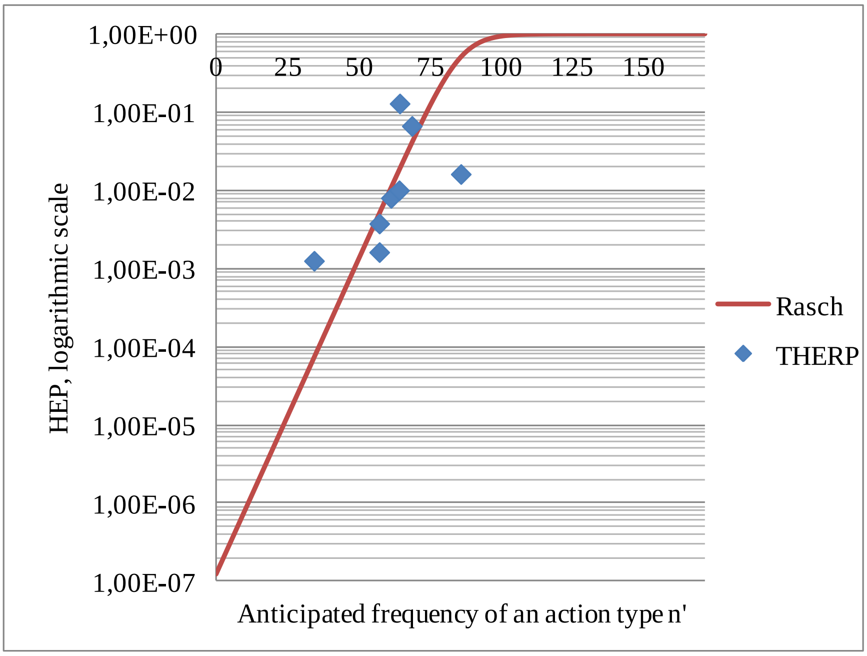


Figure 33: Comparison of THERP values and the estimated values from Rasch (logarithmic scale)

this deviation, the further analysis into the residuals has been carried out.

In order to carry out the residuals analysis, a “residual versus fitted plot” can provide some indication about the outliers and also about any existing trend. The residuals of ith value can be calculated as highlighted in the Eq.17.

$$\text{Residual} = (y_i - \hat{y}_i) \qquad \text{Eq.17}$$

Whereas:

y_i is the observed values (i.e. THERP)

$\hat{y}_i$ is the predicted values (i.e. from Rasch model)

It can be seen from the Figure 34 that due to high fitted value of “Diagnostic: Monitoring” the corresponding residual is also higher. A possible explanation of high fitted value has already been provided.

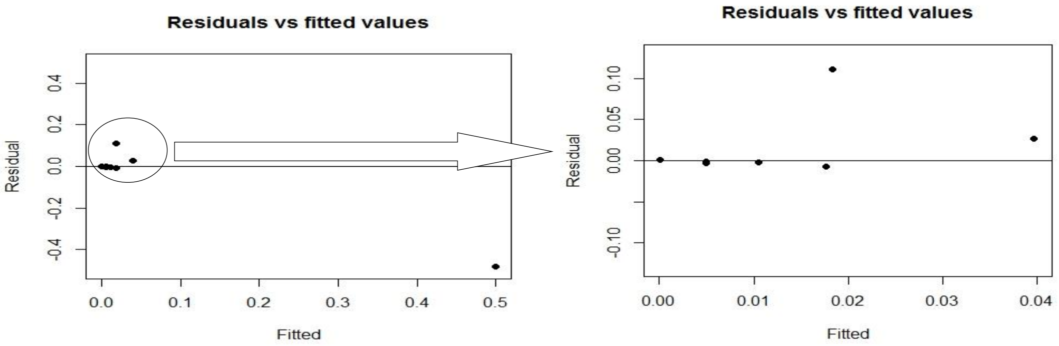


Figure 34. Residuals vs fitted plot

The rest of the plot exhibits a normal behaviour. However, due to lack of data points it is difficult to draw sweeping conclusions from these plots. Based on this analysis, it can be proposed to perform an advanced or at-least more in-details analysis about the diagnostic tasks or the operator’s behaviour during the diagnostic tasks.

In order to employ the uncertainty bounds of the obtained HEPs, the guidelines provided by THERP have been adapted as shown in the Table 14. These guidelines have been used in the absence of any concrete evidence in order to provide more reliable bounds. Therefore, the final obtained HEP with their EFs are presented in the Table 31. The EF presented in the

Table 31 are corresponding to the THERP type A "*step-by-step and under routine circumstances and under optimal stress level*" for the MEDIA action types in the operational layer. However, for the action types in the diagnostic tasks, THERP type E "*task under high stress, e.g. large LOCA; conditions in which the status of the PSFs is not perfectly clear; conditions in which the initial operator responses have proved to be in inadequate and sever time pressure is felt*" has been used. The only exception has been made for the "Diagnostic: Monitoring" tasks for which very high HEP has been obtained and therefore a different rule has been used in this case to keep the upper uncertainty bounds below 1 (i.e. the maximum value for a probability). However, for certain other situations, for example tasks under high stress level and for tasks require more dynamic interplay between operator and system different error factors should be used as suggested by the THERP.

Table 31: MEDIA HEP and relevant EF

Action type	MEDIA values (Median)	EF	Bounds	
			Upper	Lower
Monitoring equipment from field (M)	$1{,}05\times10^{-2}$	5	$5{,}25\times10^{-2}$	$2{,}10\times10^{-3}$
Monitoring/ operating equipment from control room (A)	$7{,}21\times10^{-5}$	10	$7{,}21\times10^{-4}$	$7{,}21\times10^{-6}$
Communication (C)	$4{,}97\times10^{-3}$	3	$1{,}49\times10^{-2}$	$1{,}66\times10^{-3}$
Manual tasks on-field (F)	$1{,}78\times10^{-2}$	5	$8{,}90\times10^{-2}$	$3{,}56\times10^{-3}$
Reporting (R)	$4{,}97\times10^{-3}$	3	$1{,}49\times10^{-2}$	$1{,}66\times10^{-3}$
Diagnostic: Monitoring	$5{,}00\times10^{-1}$	1,5	$7{,}50\times10^{-1}$	$3{,}33\times10^{-1}$
Diagnostic: Control room action	$4{,}00\times10^{-2}$	5	$2{,}00\times10^{-1}$	$8{,}00\times10^{-3}$
Diagnostic: Manual tasks on-field	$1{,}84\times10^{-2}$	5	$9{,}20\times10^{-2}$	$3{,}68\times10^{-3}$

During a risk assessment study, an analyst can select the values between the upper and lower uncertainty bounds with most probable estimates closer to the median values. However, these values can subject to modification under specific conditions, required for an assessment. The HEP in Table 31 are assumed to be distributed according to hypothetical log normal distribution as also assumed in the THERP database and the median values are illustrated in the Table 31.

6.2 Verification of obtained HEPs

This section provides the information about the verifications of the obtained HEP from the MEDIA assessment. However, a validation of the obtained HEP from the end-users relevant to the chemical process industry has not been carried out at the moment. In order to verify the obtained HEPs, three most widely used quantitative human reliability methods have been chosen along with the Probability of Failure on Demand (PFD) values recommended by the International Standard. These are as follows:

- THERP;
- SPAR-H;
- TESEO;
- PFD, adapted from (IEC 61511, 2003).

The Figure 35 illustrates the comparison of the MEDIA and the THERP HEPs. It can be observed that data points are almost randomly distributed on both sides of the correspondence line. However, due to lack of data points an overall conclusion is difficult to make about the main characteristic of the MEDIA compared to the THERP. In any case, it can be seen that in certain cases, the MEDIA is more pessimistic than the THERP but in fewer cases the MEDIA is more optimistic than the THERP. The pessimistic nature of the MEDIA can be explained by the less criticality of failures in the chemical process industry compared to the nuclear industry.

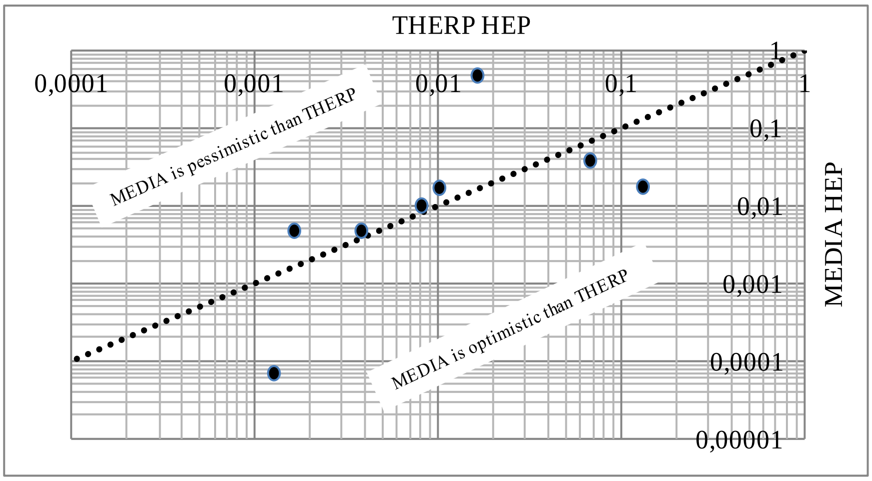


Figure 35: Comparison of MEDIA and THERP HEP

In the SPAR-H method (Gertman et al., 2005), it has been recommended to use the base nominal human error probability equal to 0,001 and 0,01 for action and diagnostic tasks, respectively.

These base HEP subject to modification according to PSFs. The Table 32 illustrates a comparison of MEDIA HEP and HEP recommended by the SPAR-H method. The HEP corresponding to "action" are of same order of magnitude but the "diagnostic" HEP obtained from MEDIA is higher than the HEP recommended by the SPAR-H. Since MEDIA has estimated the HEP by balancing the human inherent HEP and the HEP caused by the PSFs. So, it can be said that in the diagnostic layer more of the HEP are originated by the inherent characteristics than the characteristic influencing by the PSFs especially organizational PSFs.

Table 32: Comparison of MEDIA and SPAR-H HEP

Action type	MEDIA	SPAR-H
Action (i.e. operational layer in MEDIA)	$7{,}66\times10^{-3}$	$1{,}00\times10^{-3}$
Diagnostic	$1{,}86\times10^{-1}$	$1{,}00\times10^{-2}$

The TESEO method provides the information about the probability of failure of the control room operator based on the five aspects as discusses in the section 3.2.1. The human failure probability has been calculated from the five mentioned factors in the TESEO calculations and compared with "control room actions" from MEDIA for both "operational" and "diagnostic" layers.

Table 33: Comparison of MEDIA and TESEO HEP

Layer type	TESEO factors	MEDIA	TESEO
Operational	Simple, routine Time available: 20 s Average Knowledge, training Normal situation Good microclimate, good interface with plant	$7{,}21\times10^{-5}$	$5{,}0\times10^{-4}$
Diagnostic	Not routine Time available: 45 s Average Knowledge, training Situation of potential emergency Good microclimate, good interface with plant	$4{,}00\times10^{-2}$	$6{,}00\times10^{-2}$

The probability against “diagnostic” layer from TESEO has been estimated based on more severe conditions than the “operational” layer. (e.g. not routine and situation of potential emergency).

The Table 33 illustrates a comparison of MEDIA and the TESEO. It can be seen that the values in the “Diagnostic” layer corresponds to each other while a difference exist in the operational layer. Since, TESEO was originally developed for the chemical process industry so it can be argued that TESEO can provide more reliable grounds for comparison compare to other methods. But all the action types from MEDIA cannot be compared with TESEO as TESEO provides failure probability just for control room operator.

The International Standard (IEC 61511, 2003), recommended to use the Probability of Failure on Demand (PFD) values corresponding to human actions mainly during a LOPA assessment. The Table 34, illustrates a comparison of the PFD_{avg} recommended by the International Standard and the most corresponding HEPs obtained from the MEDIA assessment.

Table 34: Comparison of PFD_{avg} and MEDIA HEP

International Standard, adapted from (IEC 61511, 2003), p. 49		MEDIA	
Protection layer	PFD_{avg}	MEDIA, action type	HEP
Human performance (trained, no stress)	$1{,}00\times10^{-2}$ to $1{,}00\times10^{-4}$	Manual tasks on-field (F)	$1{,}78\times10^{-2}$
Human performance (under stress)	$5{,}00\times10^{-1}$ to $1{,}00\times10^{0}$	Diagnostic: Monitoring	$5{,}00\times10^{-1}$
Operator response to alarms	$1{,}00\times10^{-1}$	Diagnostic: Control room action	$4{,}00\times10^{-2}$

A correspondence can be seen for actions in the first two classes but a higher value has been observed in case of “operator response to alarms”. In case of “operator response to alarms” some assumptions have been made in order to compare the values from the International Standard with the MEDIA HEP. It has been assumed that alarms will be in the control room and it must be alarmed after an abnormal situation, requiring an action from the operator.

In all of the aforementioned comparisons, an absolute comparison cannot be made. This is mainly due to the differences in the assessment procedures and also the differences in considering the PSFs. However, the aforementioned methods can be used to provide the HEP estimates, to be used in other risk assessment studies. Therefore, this verification step has been carried out since one of the purposes of the MEDIA is to provide the HEP estimates.

6.3 Weightage of organizational factors

The organizational factors that are considered in this scope of work have already been detailed in the Table 20. These organizational factors have been studied for their influencing effect on different action types according to the considered taxonomy. The Table 35 illustrates the obtained weightage of different organizational factors on different human actions. As the human factor taxonomy is an action based taxonomy so in this scope of work it has been assumed that organizational influence can vary among different actions types.

Table 35: Influencing effect of organizational factors on different actions types

	Type of layer	PSFs Failures*	Organizational factors**				
			Training	Design	Procedures	Management	Safety culture
Main contributing factors	Operational layer	Technical	0,11	0,25	0,24	0,38	-
		M	0,25	0,42	0,25	0,08	-
		A	0,14	0,29	0,29	0,29	-
		C	0,44	0,11	0,44	-	-
		F	0,21	0,20	0,37	0,18	-
		R	-	-	-	1	-
	Diagnostic or preventive layer	Technical	0,13	0,50	0,13	0,25	-
		M	0,30	0,10	0,30	0,10	0,20
		A	0,30	0,10	0,50	0,10	-
		F	0,29	-	0,57	0,14	-

* Taxonomy from Table III. ** Only those values are reported with influencing affect ≥ 10%.

The numbers that are reported in the Table 35 are normalized against each action type and only those values are reported that have a considerable influencing affect (i.e. ≥ 10%). It can be seen from the table that "procedures" and "management" exhibit high influencing effect on human reliability compare to other organizational factors. Therefore, it can be said that in order to improve the overall human reliability, “procedures” and “management” attributes should be improved with a priority. The corresponding specific actions/ attributes of the organizational factors can be seen in the Table 27.

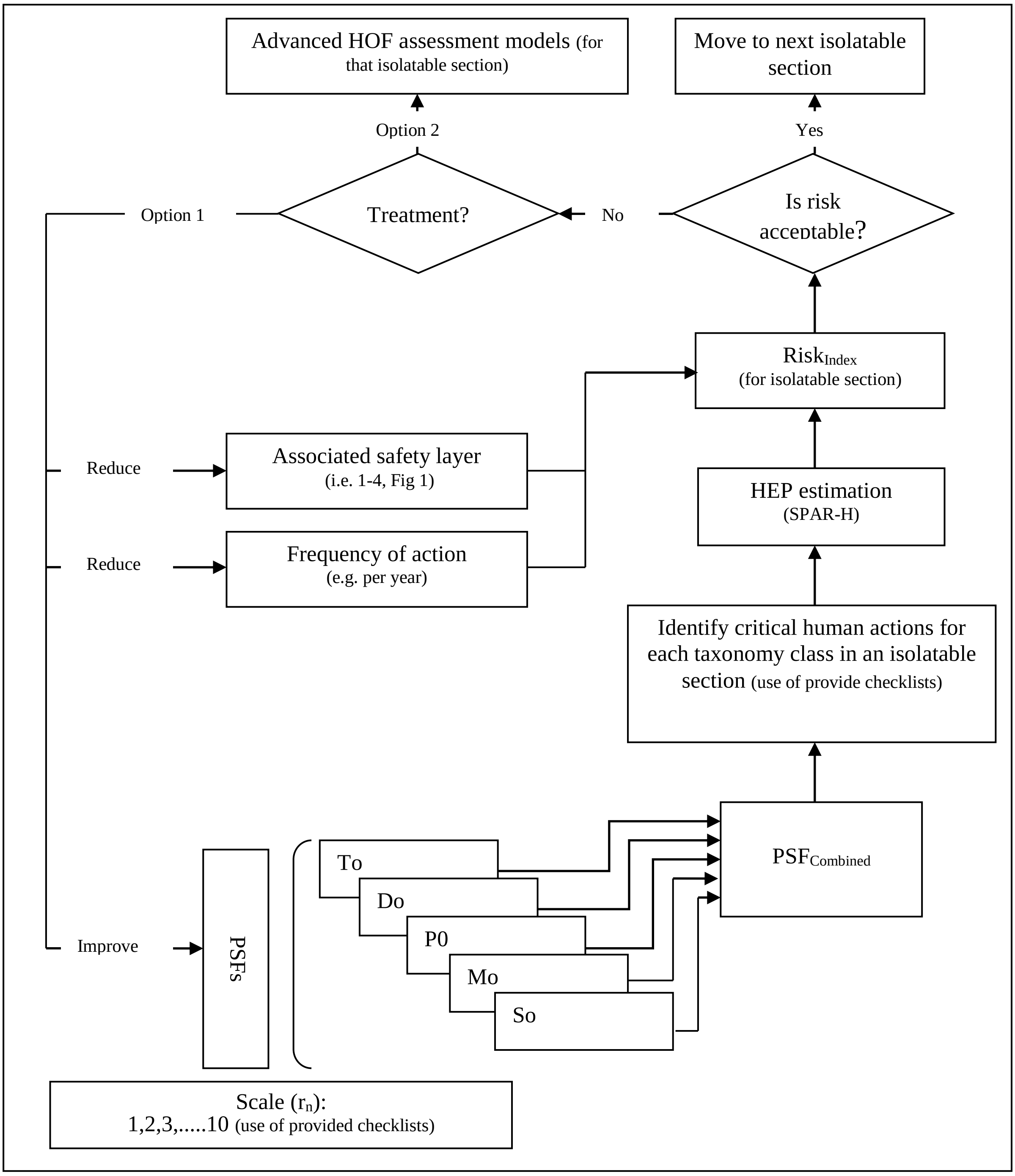
If it is assumed that, situation during an accident is comparable to situation during normal operations with respect to organizational influence on human/ operator actions. Then, estimates from the Table 35 can be used to provide a comparative influence of organizational factors on human actions in the form of weights. The main purpose of estimating the weights of organizational factors is to consider that some of the factors have more influencing affect then the other factors.

In number of existing studies, the weights of influencing factors are calculated by considering the expert’s opinion or by conducting a survey. Some of these methods and corresponding references can be seen in the section 3.3.

7 New methodology: MEDIA

The Figure 36 illustrates the newly developed "Method for Error Deduction and Incident Analysis (MEDIA)" methodology, that has been proposed in this work.

.



Advanced HOF assessment models (for that isolatable section)
Move to next isolatable section
Option 2
Yes
Option 1
Treatment?
No
Is risk acceptable?
Risk$_{Index}$ (for isolatable section)
Reduce
Associated safety layer (i.e. 1-4, Fig 1)
HEP estimation (SPAR-H)
Reduce
Frequency of action (e.g. per year)
Identify critical human actions for each taxonomy class in an isolatable section (use of provide checklists)
PSF$_{Combined}$
To
Do
P0
Mo
So
Improve
PSFs
Scale (r$_n$): 1,2,3,.....10 (use of provided checklists)

Figure 36. Method for Error Deduction and Incident Analysis (MEDIA) methodology

As mentioned earlier, this work consists of several recommendations coming out from the accident analysis, evaluation of HEPs, effect of organizational PSFs and a new methodology “MEDIA”. However, the Figure 36 illustrates the MEDIA methodology that can be used alongside the risk assessment studies that usually are carried out as a project review or during the design phase of a project.

The main advantage of this methodology is that it is coherent to the data collection or the HEPs evaluation step. The newly developed taxonomies and the checklists ensure the consistency among the data collection and prospective analysis steps.

A HOF assessment based on this methodology begins with the rating of the considered PSF. The PSF can be rated on a Likert scale by an analyst using the checklists from the Table 27. After assessing the current situation of the existing organizational factors. The rating of the organizational factors can be performed. The worst situation can take a value close to the maximum value (i.e. 10). Hence, maximizing the multiplicative effect on the human reliability. While, a better organizational factors can take a value close to the minimum value and hence minimizing the effect on the human reliability. This step of rating has not been benchmarked against an existing situation. Therefore, this step can only provide a comparative analysis rather than an absolute result that can be used across multiple plants. The same concept of rating has been proposed in many of the existing relevant approaches.

The weight of each of the factors has been estimated during the accident analysis taking into account their comparative importance as also shown in the Table 35. The combined effect of the PSFs for an action type can be estimated by using the Eq.18.

$$\mathrm{PSF_{Combined}} = \sum_{n=1}^{5} (\omega_n \,.\, r_n) \qquad \text{Eq.18}$$

Whereas:

ω_nWeight of nth PSF, from (Table 35)

r_nRating of nth PSF, from analyst

The weights of the PSF are constant, hence the only variable in this equation is the rating of the PSF. The Eq.18 should be used separately for each of the action types since weight of PSFs on the actions types varies among different human actions types.

The next step in this methodology is the identification of the critical human actions as can be seen from the Figure 36. In this work, emphasis is made to identify the critical human actions based on the Piping and Instrumentation diagrams (P&IDs). Apart from P&IDs, output from the HAZOP can also be used in order to consider potentially critical human interventions, that have been identified during the HAZOP study. In order to ease the identification process, the checklists have been developed during the accident analysis. The checklists to identify the critical human actions are presented in the Table 25.

The Nominal HEP (NHEP) for each of the action types in the MEDIA taxonomy has been estimated during the accident analysis.

After estimating the $\text{PSF}_{\text{Combined}}$, the identification of critical human interventions and the relevant NHEP, it is required to calculate the HEP from the NEHP.

There could be number of ways to calculate the HEP, but in this work the method used in the SPAR-H has been considered. The SPAR-H method to calculate the HEP from the NHEP is shown in the Eq. 5. Since it has been assumed that the human interventions lie in one of the five action types identified in the human factors taxonomy. Therefore, if further modifications are not required then the HEP estimation corresponding to certain actions in a single action class remain the same. However, further refinement can be made depending on the numbers of PSFs that can influence the human reliability in a specific assessment.

The $\text{risk}_{\text{index}}$ corresponding to a section of the plant (e.g. HAZOP nodes, QRA isolatable sections etc) can be derived based on the Eq.19 for n actions in an action type. The Eq.19 is for an action type, since the HEP varies among different action types.

$$\text{Risk}_{\text{index}} = \sum_{i=1}^{n} (\text{HEP}_i \cdot f_i \cdot s_i) \qquad \text{Eq.19}$$

Whereas:

HEP_i is the human error probability of i^{th} action

f_i is the frequency of intervention during a specific time period of i^{th} action (e.g. 1 year)

s_i is the corresponding safety layer of i^{th} action (i.e. 1-4)

Therefore, the $\text{risk}_{\text{index}}$ for a certain section of the plant is based on the numbers of critical interventions, their corresponding frequency and the safety layer.

The concept of safety layer has been adopted in this work to consider the criticality of an action failure. It has been observed that during the accident analysis that whenever failure of an action corresponds to a higher safety layer, the consequence of failure is also severe. This is mainly due to the possible absence of the subsequent safety layers in order to prevent/ mitigate the failure. For example, if monitoring of an alarm to a random column fails for an event and event has been analysed to be credible during the risk assessment studies. Then, there should be subsequent safety layers (e.g. double alarms, SIFs etc) to prevent any possible consequences from the failure in the 1st safety layer. Assuming that the subsequent safety layers will work (when required), these layers have the potential to bring back the system under safe conditions. On the other hand, if a human failure occurs in a higher safety layers (e.g. maintenance of PSVs or proof testing of SISs) and not detected in-time. In this case, due to a possible absence of the subsequent layers, human failure can lead to much severe consequences. The safety layers are shown in the Figure 2, in which the concept is shown as a risk reduction method in the process industries.

However, in order to consider the action frequency into the $Risk_{index}$ calculations, certain assumptions need to be taken. For example, constant monitoring is difficult to be consider in the overall calculations in terms of their frequencies. But, frequency interventions for certain actions (e.g. maintenance of PSVs, proof testing of SISs etc) is relatively easy to be incorporated into the $Risk_{index}$ calculations. Because, these interventions should be considered during the SIL allocation/ verification studies for the automated safety functions. Therefore, a correspondence can be ensured among the SIL and MEDIA studies.

The $Risk_{index}$ can provides an estimation of critical human interventions in a plant or in a section of the plant. Therefore, it can provide possible grounds for a follow up action followed the $Risk_{index}$ estimation. It can also be said that MEDIA methodology can help to screen and to prioritize human interventions or plant sections that need further attention with respect to human and organizational factors. In order to reduce the overall risk level, the following main actions can be taken for a specific interventions as has been shown in the Figure 36:

- To reduce the associated safety layer corresponding to a human intervention;
- To reduce the frequency of human intervention;
- To improve the organizational factors and their impact on the human intervention.

However, decreasing a corresponding safety layer might not be appropriate or practical during most of the cases. But, possible decrease in the safety layers can be considered by adding an extra supervision in the form of the operator/ supervisor. But, there is a need to explore this aspect from practical point of view.

Based on the $\text{Risk}_{\text{index}}$ calculations, an indication can be provided about the critical human interventions or the sections of a plant. For these interventions or the sections, advanced HOF methods can also be used to ensure the safety of these operations as highlighted in the Figure 36. This is an optimizations step, since due to the economic and practical reasons it is close to impossible to carry out the HOF assessment for the whole plant. Therefore, MEDIA can help to identify the critical interventions or the sections, that can be improved by using more advances relevant tools or methods.

Therefore, the MEDIA can provide an indication for possible critical human interventions that should be handled with care. However, it is not an advanced human factors assessment method. So, based on this primary screening step, advanced human or cognitive tools can be used as mentioned earlier.

Furthermore, it has been observed that to fetch the reliable information also require enormous resources that can be limited with the help of MEDIA. At the same time, the identified critical human interventions related to the SIFs can also be consider or least review in the SIL allocation / verification studies. This is only possible, if SIL allocation/ verification studies are to be carried out later than the MEDIA assessment.

It is recommended to carry out the MEDIA study during the project's initial stages preferably after the HAZOP study, as it has been developed keeping in mind the amount of information that can be obtained during project's design phase. At the same time, MEDIA can assist during some other risk assessment studies (e.g. SIL allocation / verification, QRA etc).

Another advantage of the MEDIA study is that it can identify those organizational areas that have an influence on the human's reliability and also on the equipment's reliability. Therefore, project's management can take steps to ensure the appropriate level of the organizational influencing factors. A number of organizational factors find a correspondence to the Process Safety Management (PSM) studies. Therefore, during plant's operational stages a possible PSM study sever an advanced tool to quantify the organizational factors possibly based on the Key Performance Indicators (KPIs). For example, possible KPIs can be developed for the "training" and "procedures" organizational factors.

8 A case study: MEDIA

In this chapter an insight will be provided into the case study that has been carried out based on the newly developed methodology “MEDIA”. The case study has been performed for a gas treatment plant. The objective of this treatment plant is to recover the gas reserves, separation and treatment of the fluids extracted from the production facility.

In the following section, some details about the plant will be provided along with the information/ steps required to perform the MEDIA assessment.

In order to ensure the project’s/ facility’s confidentiality, the sensitive information will be kept anonymous. However, where necessary and appropriate imaginary names/tags might be used.

8.1 Gas treatment plant

The main units of this gas treatment facility are as follows:

- Pig receiver;
- Slug catcher;
- Compressor;
- Dehydration unit;
- Fractionating unit;
- Storage unit.

The purpose of the pig receiver is to remove the pig that is loading into a pipeline earlier to clean the pipelines. The purpose of slug catcher is to collect liquids that have settled in flow lines and may cause a damage to downstream units. The compressor works to compensate for the pressure drop in the flow lines and can provide the necessary head to the gas flow. The dehydration unit is used mainly to prevent any hydrates formation in order to transport the gas for long distances. The fractionating units are used to separate the raw gas into its constituents according to the difference in their volatilities. Following the treatment of the gas it is required to store the gas for a certain time before its transfer out of the facility. This objective is obtained in a storage unit.

In order to perform the MEDIA assessment on the gas treatment plant and especially on the aforementioned units. It is required to gather the necessary information to carry out this assessment. During this case study, the following main documents have been considered in order to collate the necessary information:

- Piping & Instrumentation Diagrams (P&IDs);
- Cause & Effect (C&E) metrics;
- HAZOP report;
- Philosophy of HSE management;
- Emergency and process shutdown philosophy;
- Random documents outlining the maintenance strategy and the intervention frequency related to the Pressure Safety Valves (PSVs), Safety Instrumented Systems (SISs) and the automatic flow control valves.

The P&IDs can help to identify some of the required human interventions (e.g. related to automatic valves, indicators, alarms, PSVs etc). The C&E matrix can help to identify the effect of failure of some of the human interventions (e.g. related to the double alarms, SISs etc). The HAZOP report can identify some of the critical human interventions that had already been identified during the HAZOP session. The HAZOP report is regarded as a valuable information, since the HAZOP is usually performed in a team consist of respective field experts and their expertise are reflected in a typical HAZOP report.

The HSE management philosophy can help to identify the scope of various HSE studies and to understand the relevant documents. While, the emergency and process shut down philosophy provides the information about the design and functionality of process alarms and shutdowns sequences.

However, documents may vary from one project to the project, therefore it is recommended to consider any other relevant documents that can assist to refine the output from this study. For example, maintenance interventions for some of the units might not be available at earlier stages of a project. However, based on the expert’s judgment it can be considered with a possibility of modification at later stages of a project.

The P&IDs related to the considered units are shown in the Appendix VI. In this case study, five nodes have been considered corresponding to the HAZOP studies. Since, HAZOP has already been performed for this project therefore HAZOP report has been used as input during this case study. The five nodes are as follows:

1. Pig Receiver and Slug Catcher;
2. Booster Compressor, (i.e. Booster Compressor Suction Scrubber, Booster Compressor, Booster Compressor after Cooler);

3. Depropanizer (i.e. Depropanizer tower, Depropanizer Rebolier, Depropanizer Condenser, Depropanizer Reflux drum and Pump);
4. Debutanizer (i.e. Debutanizer tower, Debutanizer Rebolier, Debutanizer Condenser, Debutanizer Reflux drum and Pump);
5. Propane Storage (i.e. Propane Storage Bullet, Propane Transfer Pump).

These nodes can be found in the Appendix VI with the highlighted instrumentation that required any kind of human intervention.

8.2 Assessment procedure

In this case study, five HAZOP nodes have been studied but in this document only one node (i.e. Node 2) will be described in-detail. Since the assessment procedures are similar for all the nodes. While, the results from all five nodes will be presented.

The main instrumentation components that may require any kind of human intervention (i.e. normal or maintenance) are indicators, alarms and the safety functions (i.e. SIS, PSVs etc). It is required to identify all (critical) instrumentation in order to identify the relevant human interventions. Therefore, in order to make this identification process easy. The following sheet in the Figure 37 can highlight what kind of instrumentation should be consider. The input from the following main documents have been considered in order to gather the required information:

- P&IDs;
- HAZOP report;
- C&E matrix;

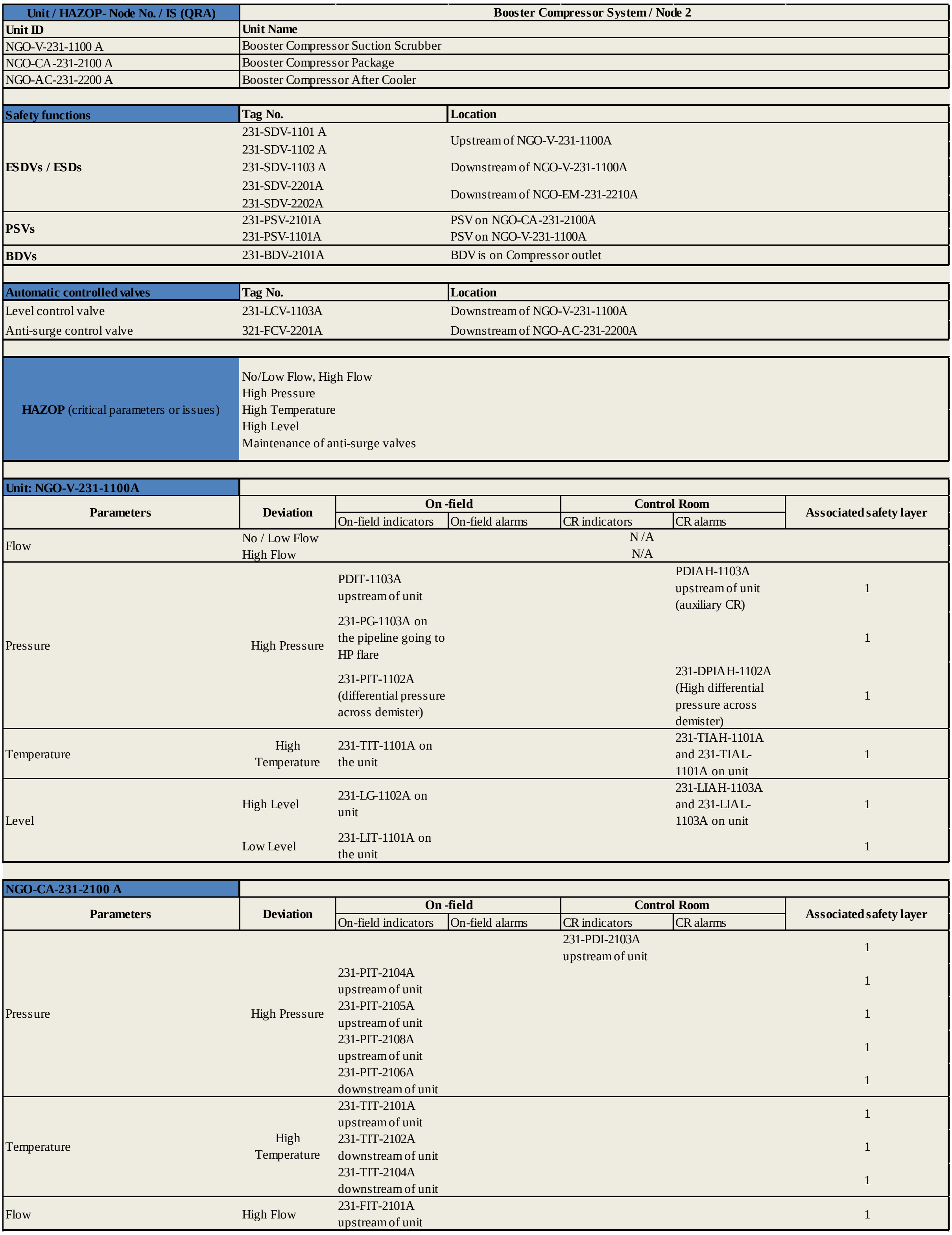
As mentioned earlier that the imaginary tag numbers have been used where seems appropriate in order to maintain the project's confidentiality. The following main steps have been carried out in the assessment procedures:

1. To identify the critical parameters (e.g. pressure, temperature, flow etc) for a particular node. For this purpose, information from the HAZOP can be considered along with generic process analysis;
2. To list the main indicators and the safety functions corresponding to the critical parameters for all main units in that node. (shown in the Figure 37);
3. To study the human factors checklists for any potentially critical human intervention. (shown in the Figure 38);

4. To calculate the risk index for that node. (shown in the Figure 38).

The step 2 &3 can also provide the input to identify the human related common cause failures

Figure 37.Identification of critical process controls



Unit / HAZOP- Node No. / IS (QRA)	**Booster Compressor System / Node 2**
Unit ID	**Unit Name**
NGO-V-231-1100 A	Booster Compressor Suction Scrubber
NGO-CA-231-2100 A	Booster Compressor Package
NGO-AC-231-2200 A	Booster Compressor After Cooler

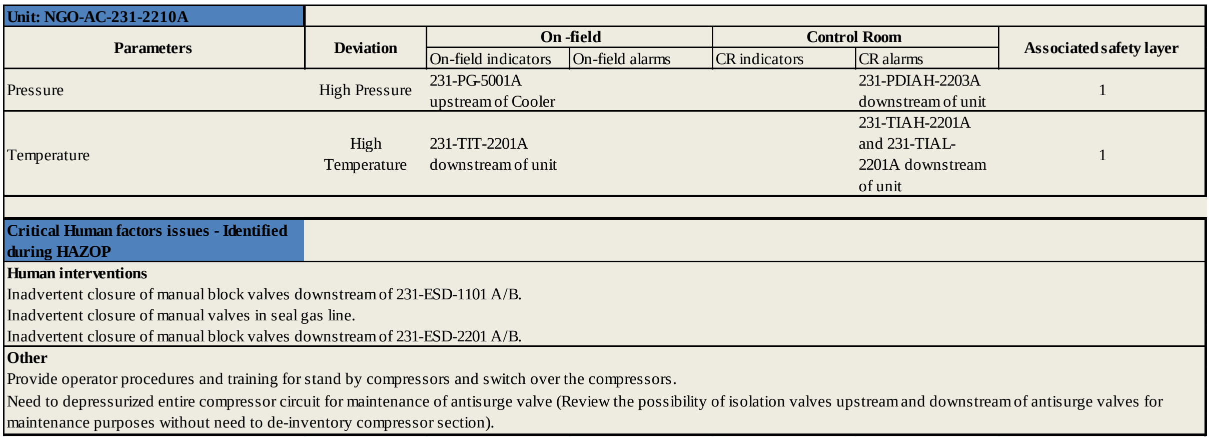
Safety functions	**Tag No.**	**Location**
ESDVs / ESDs	231-SDV-1101 A	Upstream of NGO-V-231-1100A
	231-SDV-1102 A	
	231-SDV-1103 A	Downstream of NGO-V-231-1100A
	231-SDV-2201A	Downstream of NGO-EM-231-2210A
	231-SDV-2202A	
PSVs	231-PSV-2101A	PSV on NGO-CA-231-2100A
	231-PSV-1101A	PSV on NGO-V-231-1100A
BDVs	231-BDV-2101A	BDV is on Compressor outlet

Automatic controlled valves	**Tag No.**	**Location**
Level control valve	231-LCV-1103A	Downstream of NGO-V-231-1100A
Anti-surge control valve	321-FCV-2201A	Downstream of NGO-AC-231-2200A

HAZOP (critical parameters or issues)	No/Low Flow, High Flow High Pressure High Temperature High Level Maintenance of anti-surge valves

Unit: NGO-V-231-1100A						
Parameters	**Deviation**	**On -field**		**Control Room**		**Associated safety layer**
		On-field indicators	On-field alarms	CR indicators	CR alarms	
Flow	No / Low Flow			N /A		
	High Flow			N/A		
Pressure	High Pressure	PDIT-1103A upstream of unit			PDIAH-1103A upstream of unit (auxiliary CR)	1
		231-PG-1103A on the pipeline going to HP flare				1
		231-PIT-1102A (differential pressure across demister)			231-DPIAH-1102A (High differential pressure across demister)	1
Temperature	High Temperature	231-TIT-1101A on the unit			231-TIAH-1101A and 231-TIAL-1101A on unit	1
Level	High Level	231-LG-1102A on unit			231-LIAH-1103A and 231-LIAL-1103A on unit	1
	Low Level	231-LIT-1101A on the unit				1

NGO-CA-231-2100 A						
Parameters	**Deviation**	**On -field**		**Control Room**		**Associated safety layer**
		On-field indicators	On-field alarms	CR indicators	CR alarms	
Pressure	High Pressure			231-PDI-2103A upstream of unit		1
		231-PIT-2104A upstream of unit				1
		231-PIT-2105A upstream of unit				1
		231-PIT-2108A upstream of unit				1
		231-PIT-2106A downstream of unit				1
Temperature	High Temperature	231-TIT-2101A upstream of unit				1
		231-TIT-2102A downstream of unit				1
		231-TIT-2104A downstream of unit				1
Flow	High Flow	231-FIT-2101A upstream of unit				1



Unit: NGO-AC-231-2210A						
Parameters	**Deviation**	**On -field**		**Control Room**		**Associated safety layer**
		On-field indicators	On-field alarms	CR indicators	CR alarms	
Pressure	High Pressure	231-PG-5001A upstream of Cooler			231-PDIAH-2203A downstream of unit	1
Temperature	High Temperature	231-TIT-2201A downstream of unit			231-TIAH-2201A and 231-TIAL-2201A downstream of unit	1

Critical Human factors issues - Identified during HAZOP

Human interventions
Inadvertent closure of manual block valves downstream of 231-ESD-1101 A/B.
Inadvertent closure of manual valves in seal gas line.
Inadvertent closure of manual block valves downstream of 231-ESD-2201 A/B.

Other
Provide operator procedures and training for stand by compressors and switch over the compressors.
Need to depressurized entire compressor circuit for maintenance of antisurge valve (Review the possibility of isolation valves upstream and downstream of antisurge valves for maintenance purposes without need to de-inventory compressor section).

for the safety function as recommended by the (IEC 61511, 2003) and detailed in the section 3.1.4 of this document.

The use of the checklists can ensure that any of the critical human actions are not overlooked during the assessment. Therefore, this assessment can also provide a base point for the sequential safety studies during later stages of a project that may consider human factors issues in any capacity.

However, in order to estimate the Risk$_{\text{index}}$ for a node, it is required to make some simplifications. These simplifications are necessary to consider the frequency of actions and the corresponding safety layers as mentioned earlier. The simplifications to consider the frequency of actions are listed in the Table 36. While, the simplifications to consider the corresponding safety layer are listed in the Table 37. The frequency of actions is considered for a time period of one year (i.e. 8760 hrs). For certain actions this data is available, while for some other it is required to use the justifiable assumptions.

Table 36. Simplification to identify the frequency of operations

Assumed frequency/ year	Action
1	Instrumentation require constant monitoring (e.g. pressure indicators, alarm etc).
2	Maintenance interventions (e.g. SISs, pigging operation, conditions in plant’s start-up/ shut-down state etc.), where data is not-available.

The instrumentation that require constant monitoring assumed to have a frequency of one. While, some other interventions mostly the maintenance activities are considered according to their anticipated frequencies. But, if the frequency values are not possible to obtain, then the values from the Table 36 can be used. The affect on the final output will vary according to a linear relation. So, higher the values the more affect it will have. The higher frequency value (i.e. 2) has been considered due to high number of failure for maintenance activities compare to the normal operations, as observed during the accident analysis.

In this scope of work, certain assumptions have been taken about the frequencies but it is recommended to use the information as accurate as possible. At the same time, it is also suggested for the future to define the procedures in order to include the "constant monitorings" into the assessment.

The simplifications that have been considered in order to include the associated safety layers are listed in the Table 37. While, the concept of the safety layers has been illustrated in the Figure 2.

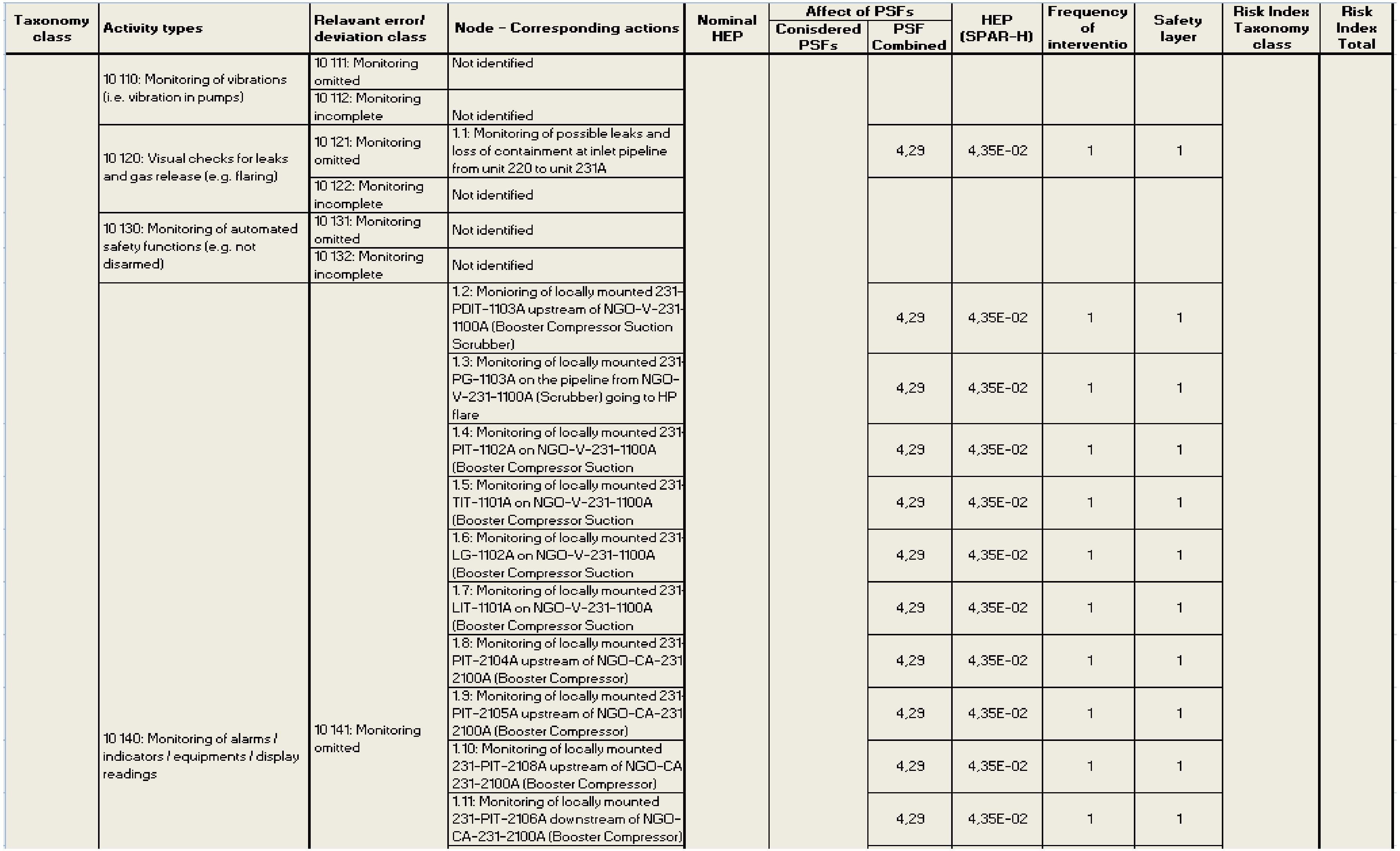
The first four safety layers are considered in this scope of work. The first two safety layers are usually correspond to the normal process controls while the subsequent two safety layers correspond to the abnormal process control. The definitions of "prevention" and "mitigation" safety layers subject to change and could be interchangeable according to a specific project. The following main aspects need to be highlighted here:

- Automatic valves are considered in the 2nd safety layer, since it is desirable to keep track of their position all the time especially when they are at a critical location or controlling to a critical parameter;
- Normal maintenance is also considered in the 2nd safety layers, as it has been observed during the accident analysis that considerable number of accidents occur during the maintenance operations;
- Reporting about the faulty state of a safety function especially when they are critical are considered in the 4th safety layer. It could be possible that operator or maintenance personnel fail to report a faulty element in a critical safety function. Therefore, due to high consequences of this action failure, the corresponding actions are considered in the highest safety layer (i.e.4);
- Mechanical Pressure Safety Valves (PSVs) and the pneumatic Blow Down Valves (BDVs) are considered in the 4th safety layer. Since, these instruments are the last line of defence in case of any pontifical abnormal situation.

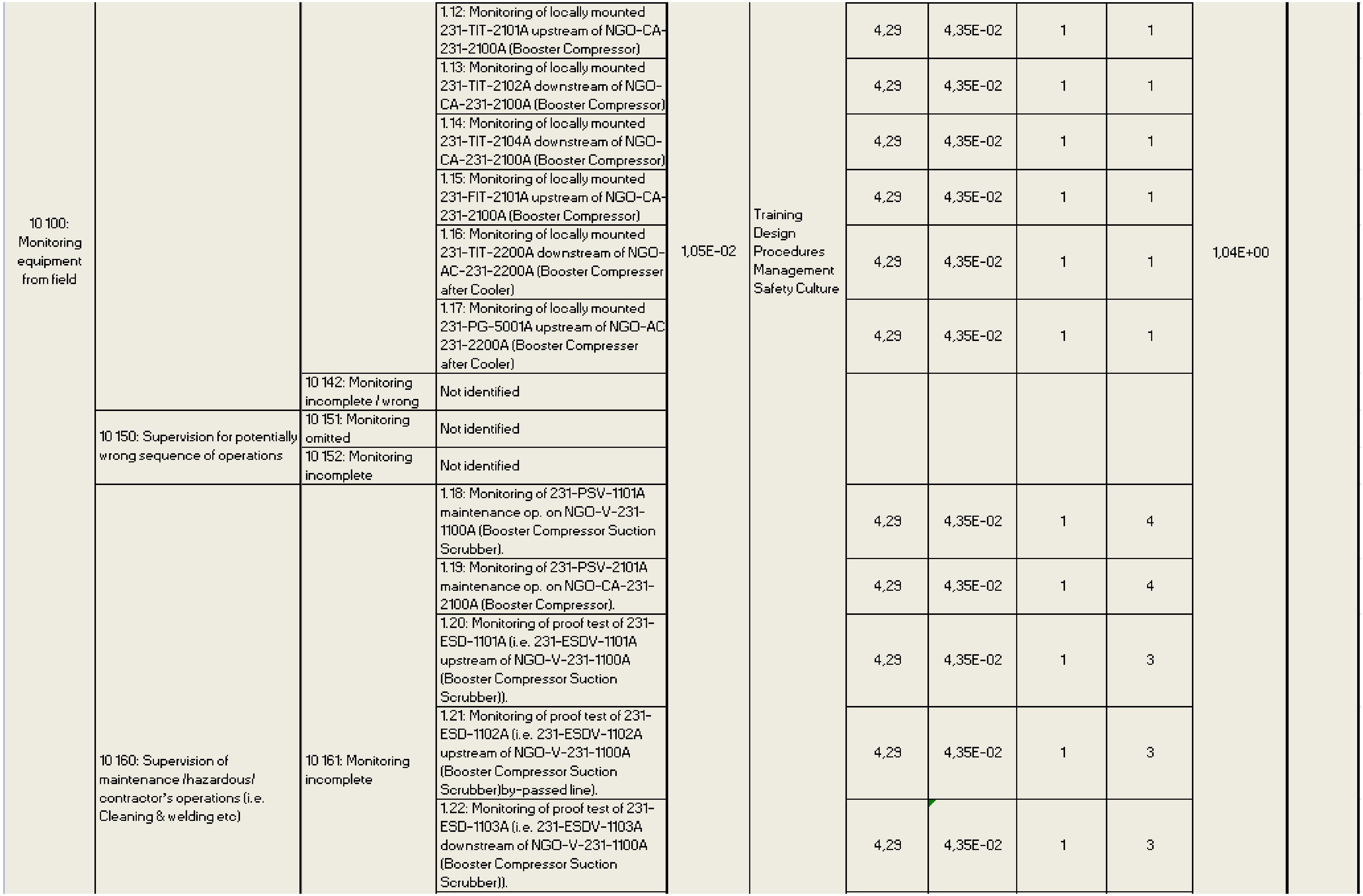
Table 37. Simplification to identify the corresponding safety layers

Safety layer	Action type (IEC 61511)	Actions
1	Process	Normal process control • Monitoring of indicators and alarms corresponding to parameters (e.g. temperature, pressure and flow etc).
2	Control and Monitoring	Normal process control • Monitoring of indicators and alarms for parameters (e.g. temperature, pressure and flow etc), a step prior to the tripping emergency automatic functions (e.g. SIFs). • Monitoring of critical process deviation alarms (i.e. high/ low deviation alarms associated with the SIFs). • Monitoring of position of critical automatic controlled values (e.g. automatic pressure and flow control valves etc). • Other critical operations (e.g. switching between critical parallel components etc). Maintenance operations • Critical maintenance interventions (e.g. pigging, cleaning of vessels etc).
3	Prevention	Abnormal process control • Actions associated with the automatic protective systems (e.g. SISs etc). Maintenance operations • Maintenance operations associated with the automatic protective devices (e.g. proof testing of SISs etc).
4	Mitigation	Abnormal process control • Actions associated with the mechanical or pneumatic mitigation devices (e.g. PSVs, BDVs etc). Maintenance operations • Maintenance operations associated with the mechanical or pneumatic mitigation devices (e.g. maintenance of PSVs and BDVs etc). Reporting • Reporting of faulty state of critical safety functions (e.g. PSVs, SISs, BDVs, F&G system etc).

Figure 38.Identification and quantification of critical human action



Taxonomy class	Activity types	Relavant error/ deviation class	Node – Corresponding actions	Nominal HEP	Affect of PSFs		HEP (SPAR-H)	Frequency of interventio	Safety layer	Risk Index Taxonomy class	Risk Index Total
					Conisdered PSFs	PSF Combined					
	10 110: Monitoring of vibrations (i.e. vibration in pumps)	10 111: Monitoring omitted	Not identified								
		10 112: Monitoring incomplete	Not identified								
	10 120: Visual checks for leaks and gas release (e.g. flaring)	10 121: Monitoring omitted	1.1: Monitoring of possible leaks and loss of containment at inlet pipeline from unit 220 to unit 231A			4,29	4,35E-02	1	1		
		10 122: Monitoring incomplete	Not identified								
	10 130: Monitoring of automated safety functions (e.g. not disarmed)	10 131: Monitoring omitted	Not identified								
		10 132: Monitoring incomplete	Not identified								
	10 140: Monitoring of alarms / indicators / equipments / display readings	10 141: Monitoring omitted	1.2: Moniоring of locally mounted 231-PDIT-1103A upstream of NGO-V-231-1100A (Booster Compressor Suction Scrubber)			4,29	4,35E-02	1	1		
			1.3: Monitoring of locally mounted 231 PG-1103A on the pipeline from NGO-V-231-1100A (Scrubber) going to HP flare			4,29	4,35E-02	1	1		
			1.4: Monitoring of locally mounted 231 PIT-1102A on NGO-V-231-1100A (Booster Compressor Suction			4,29	4,35E-02	1	1		
			1.5: Monitoring of locally mounted 231 TIT-1101A on NGO-V-231-1100A (Booster Compressor Suction			4,29	4,35E-02	1	1		
			1.6: Monitoring of locally mounted 231 LG-1102A on NGO-V-231-1100A (Booster Compressor Suction			4,29	4,35E-02	1	1		
			1.7: Monitoring of locally mounted 231 LIT-1101A on NGO-V-231-1100A (Booster Compressor Suction			4,29	4,35E-02	1	1		
			1.8: Monitoring of locally mounted 231 PIT-2104A upstream of NGO-CA-231 2100A (Booster Compressor)			4,29	4,35E-02	1	1		
			1.9: Monitoring of locally mounted 231 PIT-2105A upstream of NGO-CA-231 2100A (Booster Compressor)			4,29	4,35E-02	1	1		
			1.10: Monitoring of locally mounted 231-PIT-2108A upstream of NGO-CA 231-2100A (Booster Compressor)			4,29	4,35E-02	1	1		
			1.11: Monitoring of locally mounted 231-PIT-2106A downstream of NGO-CA-231-2100A (Booster Compressor)			4,29	4,35E-02	1	1		



10 100: Monitoring equipment from field			1.12: Monitoring of locally mounted 231-TIT-2101A upstream of NGO-CA-231-2100A (Booster Compressor)	1,05E-02	Training Design Procedures Management Safety Culture	4,29	4,35E-02	1	1	1,04E+00	
			1.13: Monitoring of locally mounted 231-TIT-2102A downstream of NGO-CA-231-2100A (Booster Compressor)			4,29	4,35E-02	1	1		
			1.14: Monitoring of locally mounted 231-TIT-2104A downstream of NGO-CA-231-2100A (Booster Compressor)			4,29	4,35E-02	1	1		
			1.15: Monitoring of locally mounted 231-FIT-2101A upstream of NGO-CA-231-2100A (Booster Compressor)			4,29	4,35E-02	1	1		
			1.16: Monitoring of locally mounted 231-TIT-2200A downstream of NGO-AC-231-2200A (Booster Compresser after Cooler)			4,29	4,35E-02	1	1		
			1.17: Monitoring of locally mounted 231-PG-5001A upstream of NGO-AC 231-2200A (Booster Compresser after Cooler)			4,29	4,35E-02	1	1		
		10 142: Monitoring incomplete / wrong	Not identified								
	10 150: Supervision for potentially wrong sequence of operations	10 151: Monitoring omitted	Not identified								
		10 152: Monitoring incomplete	Not identified								
	10 160: Supervision of maintenance /hazardous/ contractor's operations (i.e. Cleaning & welding etc)	10 161: Monitoring incomplete	1.18: Monitoring of 231-PSV-1101A maintenance op. on NGO-V-231-1100A (Booster Compressor Suction Scrubber).			4,29	4,35E-02	1	4		
			1.19: Monitoring of 231-PSV-2101A maintenance op. on NGO-CA-231-2100A (Booster Compressor).			4,29	4,35E-02	1	4		
			1.20: Monitoring of proof test of 231-ESD-1101A (i.e. 231-ESDV-1101A upstream of NGO-V-231-1100A (Booster Compressor Suction Scrubber)).			4,29	4,35E-02	1	3		
			1.21: Monitoring of proof test of 231-ESD-1102A (i.e. 231-ESDV-1102A upstream of NGO-V-231-1100A (Booster Compressor Suction Scrubber)by-passed line).			4,29	4,35E-02	1	3		
			1.22: Monitoring of proof test of 231-ESD-1103A (i.e. 231-ESDV-1103A downstream of NGO-V-231-1100A (Booster Compressor Suction Scrubber)).			4,29	4,35E-02	1	3		

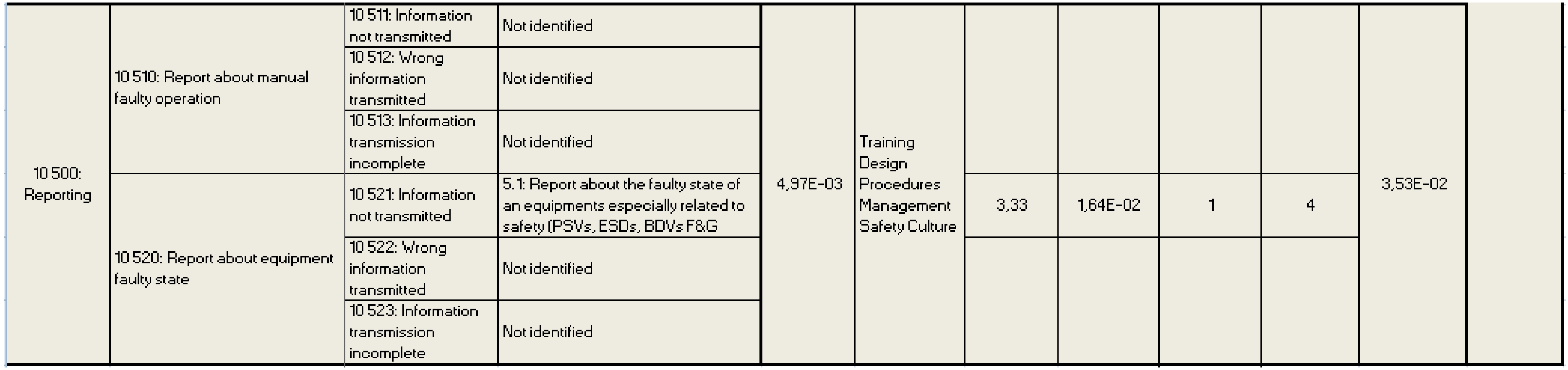
			1.23: Monitoring of proof test of 231-ESD-2201A (i.e. 231-ESDV-2201A downstream of NGO-AC-231-2200A (Booster Compressor after Cooler)).			4,29	4,35E-02	1	3		
			1.24: Monitoring of proof test of 231-ESD-2202A (i.e. 231-ESDV-2202A downstream of NGO-AC-231-2200A (Booster Compressor after Cooler)by-passed line).			4,29	4,35E-02	1	3		
		10 162: Monitoring omitted	Not identified								
	10 170: Supervision of potentially risky operations (i.e. loading op. / transfer op.)	10 171: Monitoring omitted	Not identified								
		10 172: Monitoring incomplete	Not identified								
	10 180: Monitoring, visual inspection of valve positions, seals, flanges clearances etc	10 181: Wrong/incomplete monitoring of valve positions	Not identified								
		10 182: Monitoring omitted	Not identified								
	10 190: Visual monitoring of externel corrosion	10 191: Action omitted	Not identified								
		10 192: Action in-complete / in-	Not identified								
	10 210: Monitoring/ actions related to remotely operated / ESD valves.	10 211: Action omitted	2.1: Monitoring of proof test (and unintentional by-passed) of 231-ESD-1101A (231-ESDV-1101A upstream of NGO-V-231-1100A (Booster Compressor Suction Scrubber))			7	5,04E-04	1	3		
			2.2: Monitoring of proof test (and unintentional by-passed) of 231-ESD-1102A (231-ESDV-1102A upstream of NGO-V-231-1100A (Booster Compressor Suction Scrubber))			7	5,04E-04	1	3		
			2.3: Monitoring of proof test (and unintentional by-passed) of 231-ESD-1103A (231-ESDV-1103A downstream of NGO-V-231-1100A (Booster Compressor Suction Scrubber))			7	5,04E-04	1	3		
			2.4: Monitoring of proof test (and unintentional by-passed) of 231-ESD-2201A (231-ESDV-2201A downstream of NGO-AC-231-2200A (Booster Compressor after Cooler))			7	5,04E-04	1	3		
			2.5: Monitoring of proof test (and unintentional by-passed) of 231-ESD-2202A (231-ESDV-2202A downstream of NGO-V-231-1100A (Booster Compressor Suction			7	5,04E-04	1	3		

10 200: Monitoring / operating equipment from control room (CR)			2.6: Monitoring of position of 231-LCV-1103A (Liquid level control valve downstream of NGO-V-231-1100A (Booster Compressor Suction Scrubber))	7,21E-05	Training Design Procedures Management Safety Culture	7	5,04E-04	1	2	5,07E-03	**2,24E+00**
			2.7: Monitoring of position of 321-FCV-2201A (Anti-surge valve) downstream of NGO-AC-231-2200A (Booster Comprresoer after Cooler))			7	5,04E-04	1	2		
			2.8: Monitoring of 231-BDV-2101A (i.e To ensure that 231-BDV-2101A is not overrided, level 2 shutdown initiated by high pressure at			7	5,04E-04	1	4		
		10 212: Action too little / too much	Not identified								
		10 213: Action in wrong direction	Not identified								
	10 220: Monitoring/ actions related to process parameters (i.e. P,T, F)	10 221: Action omitted	Not identified								
		10 222: Action too much / too little	Not identified								
	10 230: Monitoring/ actions related to switching of units	10 231: Action in wrong direction / not correct	2.9: Monitoring of switching between running /standby Compressors (i.e. To provide enough procedures and training to operator to switch between Compressors)			7	5,04E-04	1	2		
	10 240: Monitoring/ actions related to unit on/off	10 241: Wrong action on right object	Not identified								
		10 242: Right action on wrong object	Not identified								
	10 250: Monitoring/ actions related to process alarms	10 251: No detection (intentionally ignored)	2.10: Monitoring of CR (auxiliary CR) mounted High differential pressure alarm PDIAH-1103A upstream of unit NGO-V-231-1100A.			7	5,04E-04	1	1		
			2.11: Monitoring of CR mounted high differential pressure alarm 231-DPIAH 1102A on unit NGO-V-231-1100A.			7	5,04E-04	1	1		
			2.12: Monitoring of CR mounted 231-TIAH-1101A and 231-TIAL-1101A on unit NGO-V-231-1100A.			7	5,04E-04	1	1		
			2.13: Monitoring of CR mounted high /low level alarm 231-LIAH-1103A and 231-LIAL-1103A on unit NGO-V-231-1100A.			7	5,04E-04	1	1		
			2.14: Monitoring of CR mounted high /low temperature alarm 231-TIAH-2201A and 231-TIAL-2201A downstream of unit NGO-AC-231-2200A.			7	5,04E-04	1	1		

			2.15: Monitoring of high differnetial pressure alarm 231-PDIAH-2203A downstream of unit NGO-AC_231-2200A.			7	5,04E-04	1	1		
		10 252: Undue silencing of alarms	Not identified								
	10 260: Supervision for potentially wrong sequence of operations	10 261: Supervision omitted	Not identified								
		10 262: Supervision incomplete	Not identified								
	10 270: Supervision of maintenance / hazardous / contractor's (i.e. cleaning/ welding etc) operations	10 271: Supervision omitted	Not identified								
		10 272: Supervision incomplete	Not identified								
	10 280: Supervision of potentially risky operations	10 281: Supervision omitted	Not identified								
		10 282: Supervision incomplete	Not identified								
	10 290: Action reltated to isolations of the pipelines	10 291: Error of omission	Not identified								
10 300: Communication	10 310: Communication between shifts	10 311: Info/comm. not transmitted	Not identified	4,97E-03	Training Design Procedures Management Safety Culture					5,28E-02	
		10 312: Wrong info/comm.	Not identified								
		10 313: Info/comm. transmission incomplete	3.1: Communication between shits especially during the start-up, shut-down and maintenance conditions and also during the switching of compressor units.			5	2,44E-02	2	2		
	10 320: Communication between process operators and supervisors.	10 321: Info/comm. not transmitted	Not identified								
		10 322: Wrong info/comm.	Not identified								
		10 323: Info/comm. transmission incomplete	Not identified								
	10 330: Communication among process operators and among multiple parties especially when contractor are involved	10 331: Info/comm. not transmitted	Not identified								
		10 332: Wrong info/comm.	Not identified								
		10 333: Info/comm. transmission incomplete	Not identified								

	10 340: Communication between plant personnel (i.e. shift in-charge) and maintenance contract operators	10 341: Info/comm. not transmitted	Not identified								
		10 342: Wrong info/comm.	Not identified								
		10 343: Info/comm. transmission incomplete	Not identified								
	10 350: Communication among the supervisors.	10 351: Info/comm. not transmitted	Not identified								
		10 352: Wrong info/comm.	Not identified								
		10 353: Info/comm. transmission incomplete	Not identified								
	10 410: Manual operations of valves/ pumps/ safety mountings / sealing kits / flanges screws etc	10 411: Action omitted	Not identified								
		10 412: Action in wrong direction	Not identified								
		10 413: Action too little / much	Not identified								
		10 414: Right action on wrong object	Not identified								
		10 415: Un-necessary action (i.e. Inc. Violation, willful disobedience etc).	4.1: Inadvertent closure of manual block valves downstream of 231-ESD-1101 A/B			3,93	6,64E-02	1	1		
			4.2: Inadvertent closure of manual valves in seal gas line			3,93	6,64E-02	1	1		
			4.3: Inadvertent closure of manual block valves downstream of 231-ESD-2201 A/B			3,93	6,64E-02	1	1		
	10 420: Operations related to alarms (i.e. Switch off un-intentionally)	10 421: Switched off an alarm (req. for prevention/mitigation	Not identified								
		10 422: Violation in alarm op.	Not identified								
	10 430: Testing/ calibration operations	10 431: Action omitted	Not identified								
		10 432: Right action on wrong object	Not identified								
		10 433: Wrong action on right object	Not identified								
			4.4: Maintenance (i.e. proof test) of 231-ESD-1101A (231-ESDV-1101A upstream of NGO-V-231-1100A (Booster Compressor Suction Scrubber))			3,93	6,64E-02	1	3		

10 400: Manual tasks on-field	10 440: Maintenance operations	10 441: Action mistimed/ not corrected	4.5: Maintenance (i.e. proof test) of 231-ESD-1102A (231-ESDV-1102A upstream of NGO-V-231-1100A (Booster Compressor Suction Scrubber))	1,78E-02	Training Design Procedures Management Safety Culture	3,93	6,64E-02	1	3	1,10E+00	
			4.6: Maintenance (i.e proof test) of 231-ESD-1103A (231-ESDV-1103A downstream of NGO-V-231-1100A (Booster Compressor Suction Scrubber))			3,93	6,64E-02	1	3		
			4.7: Maintenance (i.e proof test) of 231-ESD-2201A (231-ESDV-2201A downstream of NGO-AC-231-2200A (Booster Compressor after Cooler))			3,93	6,64E-02	1	3		
			4.8:: Maintenance (i.e. proof test) of 231-ESD-2202A (231-ESDV-2202A downstream of NGO-V-231-1100A (Booster Compressor Suction Scrubber))			3,93	6,64E-02	1	3		
			4.9:: Maintenance of 231-PSV-1101A on NGO-V-231-1100A (Booster Compressor Suction Scrubber)			3,93	6,64E-02	1	4		
			4.10: Maintenance of 231-PSV-2101A on NGO-CA-231-2100A (Booster Compressor)			3,93	6,64E-02	1	4		
		10 442: Violation in maintenance op.	Not identified								
		10 443:Wrong action on right object	Not identified								
		10 444: Right action on wrong object	Not identified								
	10 450: Fluid addition/ transfer operations in vessel (inc. loading/unloading and mixing)	10 451: Action omitted	Not identified								
		10 452: Action mistimed, not correct	Not identified								
		10 453:Right action on wrong object	Not identified								
		10 454: Procedures not followed (i.e. Violations)	Not identified								
	10 460: Operations related to pipe/flexible hose connections	10 461: Right action on wrong unit	Not identified								



10 500: Reporting	10 510: Report about manual faulty operation	10 511: Information not transmitted	Not identified	4,97E-03	Training Design Procedures Management Safety Culture					3,53E-02	
		10 512: Wrong information transmitted	Not identified								
		10 513: Information transmission incomplete	Not identified								
	10 520: Report about equipment faulty state	10 521: Information not transmitted	5.1: Report about the faulty state of an equipments especially related to safety (PSVs, ESDs, BDVs F&G			3,33	1,64E-02	1	4		
		10 522: Wrong information transmitted	Not identified								
		10 523: Information transmission incomplete	Not identified								

8.3 Results of the case study

This section illustrates the result of all five nodes that have been obtained as a result of the case study. The Table 38 illustrates the considered nodes and the obtained $\text{Risk}_{\text{index}}$ from the MEDIA case study.

Table 38. Nodes and $\text{Risk}_{\text{index}}$

Node	Node description	$\text{Risk}_{\text{index}}$
1	Pig receiver and slug catcher	1,63E+00
2	Booster compressor	2,24E+00
3	Depropanizer	2,26E+00
4	Debutanizer	2,26E+00
5	Propane storage	2,72E+00

It can be seen from the Table 38, that the $\text{Risk}_{\text{index}}$ is same for Depropanizer and Debutanizer sections of the plant. Since, both of these sections have almost the same units (e.g. distillation tower etc), instrumentation and hence corresponding human interventions.

The $\text{Risk}_{\text{index}}$ for the node corresponding to “Propane storage” is higher among all the five nodes. This is due to the fact that most number of human interventions correspond to this node and also most of them are crucial as identified during the past accident analysis. The critical human interventions that are not present in other nodes are related to the cleaning of the storage tanks. These interventions are usually overlooked during the preliminary risk assessment studies (e.g. HAZOP) and can lead to a possible undesired situation during the operational stages.

Therefore, based on the MEDIA assessment described in the Figure 36. It can be said that the node 5 (i.e. Propane storage section) is the most critical section. Therefore, further resources should be spent to improve the HOF issues in this node. At the same time, this assessment is also an indication about the HOF issues that should be considered by the management during a project. It is important to highlight that the $\text{Risk}_{\text{index}}$ number is not an absolute number, however it can be seen in a comparison.

The obtained results from MEDIA case study are compared with the risk calculations that are usually performed during the QRA studies. For this comparison, Location Specific Individual Risk (LSIR) has been selected. The LSIR at a specific location indicates a fatal injury to an individual, hypothetically considering that a worker is permanently positioned at that location. The LSIR at any given location can be calculated by the Eq. 20.

$$\mathrm{LSIR_T} = \sum_{S} \lambda_S \cdot \sum_{T} P_T \cdot \sum_{U} (P_{wind} V(T))_{S,T,U} \qquad \text{Eq. 20}$$

Whereas:

λ_S is release frequency (summation S over release events).

P_T is probability of the scenario, given the release (summation over T outcome scenarios).

P_{wind} is wind direction probability (summation over U wind directions).

$V(T)$ is vulnerability at location T.

In order to perform the MEDIA comparison with the LSIR, it is required to find a correspondence between the HAZOP nodes and QRA isolatable sections. The LSIR is usually calculated for the main risk areas identified on the plant layout. It has been observed that a correspondence can be consider but this correspondence is not a precise correspondence. Since, some random changes among HAZOP nodes and QRA isolatable are possible. But, despite that it can provide reasonable grounds for the comparison.

Both LSIR and MEDIA-Risk$_{index}$ are on separate scales so cannot be compared as such but can be compared among different nodes. The LSIR is calculated mainly from the technical failure (i.e. loss of containment events). The LSIR at a specific location (i.e. risk area) inside an isolatable section can have some contribution from the nearby sections according to the release scenarios. The main information providing by the LSIR is about the source terms rather than a specific location at a given location. As for two multiple locations, the same location parameter (i.e. permanent individual presence) is assumed hence can be considered as a constant.

It can be seen from the Figure 39 that at one location the LSIR can be lower but MEDIA-Risk$_{index}$ can be higher compare to other nodes. Therefore, it can be said that integrity of a node or isolatable section can be impaired by the human interventions to a considerable extent. As major contribution of loss of containment events scenarios comes from the failure rate of a unit (i.e. λ) overlooking the human /operator aspects during the operations.

Therefore, MEDIA methodology can help to identify the critical sections (i.e. nodes/

isolatable sections) in a plant that require further attention to ensure the safety of operations. Although, in this study the output from the QRA report has been considered for the comparison purposes. But, it is recommended to use the MEDIA methodology prior to the QRA study. In this case, the MEDIA can identify the potentially critical human interventions and sections of a plant. The critical human interventions can be considered as the possible process deviation events during a QRA study. The obtained critical sections of the plant can be looked into more detail during a QRA study.

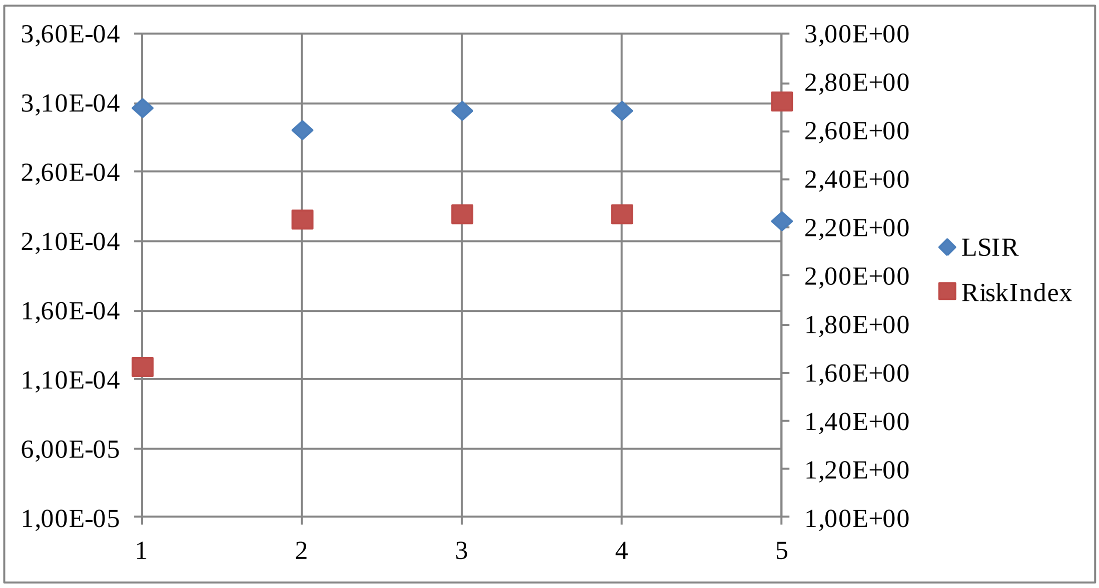


Figure 39. Comparison of LSIR and MEDIA-Risk$_{\text{index}}$ against risk areas and considered nodes

9 Conclusions

The Human and Organizational Factors (HOF) cannot be overlooked during the risk assessment studies due to their critical contribution. It has been observed that these factors had led to a considerable percentage of accidents especially in the chemical process industry, that is the main focus in this study.

The integration of HOF around the technical aspects has been studied in this work, to ensure the optimal use of the available resources.

A number of critical aspects have been observed and highlighted in the section 3.2 related to the existing and the mostly widely used HOF methods. Furthermore, a review has been done related to the new and developing concepts and the methods that can enhance the effectiveness of HOF assessment, as can be seen in the section 3.3.

A new action based taxonomy has been developed for the HOF that can account for all major actions in the chemical process plants.

The past accident analysis has been performed in order to learn lessons and to provide a quantification of the HOF. In this work, a total of 438 accidents of 25 years (1988-2012) have been studied related to the Seveso establishments in the EU, of which 197 accidents (i.e. about 45 % of total accidents) were caused due to the HOF.

The Swiss cheese model has been modified in order to structure and to synchronize the accident analysis. A total of nine forms of the Swiss cheese model have been developed that can account for the main accident evolution paths.

The probabilistic Rasch model has been adapted in this work in order to obtain the Human Error Probabilities (HEPs) from results of the accident analysis, according to the CAHR application. Furthermore, the weightage of the organizational Performance Shaping Factors (PSF) has also been obtained from the accident analysis. The further details about the quantification of the HOF can be found in the section 6.

Consequently, a new methodology “Method for Error Deduction and Incident Analysis (MEDIA)” has been developed in this work based on the accident analysis. The MEDIA can help to identify the critical sections or the interventions in a plant with respect to human actions and the technical failures. The MEDIA provides an integrated and optimized solution with respect to the HOF and the technical failure. This methodology can be used integrated with the HAZOP, QRA and the SIL studies. The further details about the MEDIA can be found in the section 7.

A number of recommendations are also proposed in this work based on lessons learned from the accident analysis. The following main recommendations are as follows:

1. It is recommended to use the developed checklists related to the organizational factors during the HAZID studies. The HAZID study is usually performed with the checklists proposed in the International Standard (ISO 17776, 2000);
2. It is recommended to report the accidents/ near misses to the European Commission by the EU Member States, when the HOF have a contribution to the accidents. The aforementioned statement should be fulfil even if the existing reporting criteria identified in the Seveso directive (EC, 2012) does not meet. The existing criteria to report accidents to the Commission can be seen in the Appendix III. In the section II of this existing reporting criteria it is stated that "*accidents or near-misses which Member States regard as being of particular technical interest for preventing major accidents and limiting their consequences and which do not meet the quantitative criteria above should be notified to the Commission*".

   Therefore, giving the existing lack of information and ambiguity about the HOF and their role especially during the abnormal situations. It is recommended to learn more about the HOF and their role during the abnormal situations. A possible way to learn more about these factors is to learn through the past accidents. This learning can help to mitigate some of the uncertainty about the HOF. Therefore, in this work it is high recommended to have a legal obligation for the EU Member States to report their industrial accidents to the European Commission when among others caused by the HOF as identified during the post-accident investigation. This potential modification to the existing reporting criteria can help to learn lessons from the HOF issues to a greater extent.
3. It is also recommended to modify the eMARS' existing report structure. The existing eMARS structure can be seen in the Appendix IV. It has been observed that there are certain ambiguous areas in the "*Cause of the accident*" section especially related to the "*Organizational*" and "*Human*" elements. Therefore, it is required to modify the existing "*Organizational*" and "*Human*" elements and their details. It is proposed to consider taxonomy for both "*Organizational*" and "*Human*" elements that can cover all possible failure attributes. For example, MEDIA organizational and human factor taxonomy is an action based five factors taxonomy. However, in case of eMARS report structure it might require more than five factors that can cover all possible failure attributes.

4. It is highly recommended to consider the maintenance activities during the preliminary risk assessment studies (e.g. HAZOP). It has been observed during the accident analysis that a considerable number of failures were occurred during the maintenance activities or relevant tasks. One possible explanation of these failures is that these activities are usually overlooked during the preliminary risk assessment studies (e.g. HAZOP), hence reflect in the same way during the subsequent risk assessment studies. In this regard, the main human failures were observed during the vessel cleaning activities.

References

Al-shanini, A., Ahmad, A., Khan, F., 2014. Accident modelling and analysis in process industries. J. Loss Prev. Process Ind. 32, 319–334. doi:10.1016/j.jlp.2014.09.016.

Alvarenga, M.A.B., Frutuoso e Melo, P.F., Fonseca, R.A., 2014. A critical review of methods and models for evaluating organizational factors in Human Reliability Analysis. Prog. Nucl. Energy 75, 25–41. doi:10.1016/j.pnucene.2014.04.004.

ATSB, 2008. Analysis, Causality and Proof in Safety Investigations. ATSB Transport Safety Report - Australian Transport Safety Bureau (ATSB), Canberra City.

Aven, T., Sklet, S., Vinnem, J.E., 2006. Barrier and operational risk analysis of hydrocarbon releases Part I . Method description. J. Hazard. Mater. A 137, 681–691. doi:10.1016/j.jhazmat.2006.03.049.

Baber, C., Stanton, N.A., 1996. Human error identification techniques applied to public technology : predictions compared with observed use. Appl. Ergon. 27, 119–131.

Bell, J., Holroyd, J., 2009. Review of human reliability assessment methods, RR679. Health and Safety Executive, Buxton.

Bellamy, L.J., Geyer, T.A., 2007. Development of a working model of how human factors, safety management systems and wider organisational issues fit together, RR 543. Health and Safety Executive.

Bellamy, L.J., Geyer, T.A.W., Astley, J.A., 1989. Evaluation of the human contribution to pipework and In-line equipment failure frequencies. Technica Consulting Scientists and Engineers, Health and Safety Executive (HSE), London.

Bello, G.C., Colombari, V., 1980. The Human Factors in Risk Analyses of Process Plants: The Control Room Operator Model “TESEO.” Reliab. Eng. 1, 3–14.

CCPS, 2011. Process Safety Leading and Lagging Metrics.. You Don’t Improve What You Don't Measure. Center for Chemical Process Safety (CCPS), American Institute of Chemical Engineers.

CCPS, 2000. Guidelines for Chemical Process Quantitative Risk Analysis, Second. ed. American Institute of Chemical Engineers, New York.

CCPS, 1994. Guidlines for Preventing Human Error in Process Safety. Center for Chemical Process Safety (CCPS), American Institute of Chemical Engineers, New York.

CEI/IEC 61882, 2001. Hazard and operability studies (HAZOP studies) - Application guide, First. ed. International Electrotechnical Commission (IEC), Geneva.

Choppin, B., 1983. The Rasch Model for Item Analysis. Center for the Study of Evaluation, University of California, Los Angeles.

DNV, 2007a. Accident statistics for floating offshore units on the UK Continental Shelf 1980-2005. Prepared by Det Norske Veritas (DNV) for the Health and Safety Executive (HSE), UK.

DNV, 2007b. Accident statistics for fixed offshore units on the UK Continental Shelf 1980-2005. Prepared by Det Norske Veritas (DNV) for the Health and Safety Executive (HSE), UK.

EC, 2012. Directive 2012/18/EU of the European Parliament and of the Council of 4 July 2012 on the control of major-accident hazards involving dangerous substances. Official Journal of the European Union, L 197/1.

Emars, n.d. Emars [WWW Document]. URL https://emars.jrc.ec.europa.eu/ (accessed 8.1.15).

Embrey, D.E., 1992. Quantitative and Qualitative Prediction of Human Error in Safety Assessments. I. Chem. E. Symposium series No.130, pp. 329–350.

Everdij, H.C.M., Blom, A.P.H. (Eds.), 2013. Safety Methods Database. NLR - Netherlands Aerospace Centre.

Gertman, D., Blackman, H., Marble, J., Byers, J., Smith, C., 2005. The SPAR-H Human Reliability Analysis Method. NUREG/CR-6883 INL/EXT-05-00509.

Gowland, R., 2006. The accidental risk assessment methodology for industries (ARAMIS)/ layer of protection analysis (LOPA) methodology: A step forward towards convergent practices in risk assessment ? 130, 307–310. doi:10.1016/j.jhazmat.2005.07.007.

Green, D.W., Maloney, J.O. (Eds.), 1997. Perry’s Chemical Engineers' Handbook, Seventh. ed. McGraw-Hill, New York.

Hollnagel, E., 1993. Human reliability analysis: Context and control. Academic Press, London.

IEC 31010, 2009. Risk management - Risk assessment techniques. International Electrotechnical Commission (IEC), Geneva.

IEC 61508, 1997. Functional safety of electrical/electronic/ programmable electronic safety-related systems. International Electrotechnical Commission (IEC), Geneva.

IEC 61511, 2003. Functional safety: Safety instrumented systems for the process industry sector, First. ed. International Electrotechnical Commission (IEC), Geneva.

ISO 17776, 2000. Petroleum and natural gas industries - Offshore production installations - Guidelines on tools and techniques for hazard identification and risk assessment, First.

ed. International Organization for Standardization (ISO), Geneva.

Kirchsteiger, C., 1999. Status and functioning of the European Commission's major accident reporting system. J. Hazard. Mater. 65, 211–231. doi:10.1016/S0304-3894(98)00264-7.

Kirwan, B., 1996. The validation of three Human Reliability Quantification techniques - THERP , HEART and JHEDI : Part 1 - technique descriptions and validation issues. Appl. Ergon. 27, 359–373.

Kirwan, B., Kennedy, R., Taylor-adams, S., Lambert, B., 1997. The validation of three Human Reliability Quantification techniques - THERP , HEART and JHEDI : Part II - Results of validation exercise. Appl. Ergon. 28, 17–25.

Laumann, K., Rasmussen, M., 2015. Suggested improvements to the definitions of Standardized Plant Analysis of Risk-Human Reliability Analysis (SPAR-H) performance shaping factors, their levels and multipliers and the nominal tasks. Reliab. Eng. Syst. Saf. 145, 287–300. doi:10.1016/j.ress.2015.07.022.

Loer, K., Holz, J., Athanassiou, G., Straeter, O., 2011. Learning from Maritime Accidents by Applying Connectionism Assessment of Human Reliability, in: ERGOSHIP 2011(the First Conference on Maritime Human Factors). Goteborg.

Mannan, S. (Ed.), 2012. Lees's Loss Prevention in the Process Industries, Hazard Identification, Assessment and Control, Fourth Edi. ed. Elsevier Butterworh-Heinemman, Waltham, MA, USA (2012).

Mosleh, A., Goldfeiz, E., Shen, S., 1997. The ω-Factor Approach for Modeling the Influence of Organizational Factors in Probabilistic Safety Assessment. Proceedings of the IEEE sixth Annual Human Factors Meeting, Orlando.

Nivolianitou, Z., Konstandinidou, M., Michalis, C., 2006. Statistical analysis of major accidents in petrochemical industry notified to the major accident reporting system (MARS). J. Hazard. Mater. 137, 1–7. doi:10.1016/j.jhazmat.2004.12.042.

NTNU, 2014. NTNU [WWW Document]. URL https://www.ntnu.edu/ross/info/acc-data (accessed 3.15.14).

OECD, 1998. Critical Operator Actions: Human Reliability Modelling and Data Issues. Principal Working Group No. 5 - Task 94-1. Organization for Economic Cooperation and Development (OECD), Nuclear Energy Agency (NEA), Paris.

OGP, 2010. Risk Assessment Data Directory - Human factors in QRA, Report No. 434 -5, International Association of Oil and Gas Producers.

Øien, K., 2001. A framework for the establishment of organizational risk indicators. Reliab. Eng. Syst. Saf. 74, 147–167. doi:10.1016/S0951-8320(01)00068-0.

Papazoglou, I.A., Bellamy, L.J., Hale, A.R., Aneziris, O.N., Ale, B.J.M., Post, J.G., Oh, J.I.H., 2003. I-Risk : development of an integrated technical and management risk methodology for chemical installations 16, 575–591. doi:10.1016/j.jlp.2003.08.008.

Purple Book, 2005. Guidelines for quantitative risk assessment CPR 18 E, PGS 3. Committee for the Prevention of Disasters, The Hauge.

Rasch, G., 1960. Probabilistic Models for some Intelligence and Attainment Test. With a foreword and afterword by Benjamin D. wright, MESA Press, Chicago.

Rathnayaka, S., Khan, F., Amyotte, P., 2011. SHIPP methodology : Predictive accident modeling approach . Part I : Methodology and model description. Process Saf. Environ. Prot. 89, 151–164. doi:10.1016/j.psep.2011.01.002.

Reason, J., 1990. Human Error. Cambridge University Press, Cambridge.

Reason, J., Hollnagel, E., Paries, J., 2006. Revisiting the <<SWISS CHEESE>> Model of Accidents. EuroControl Experimental Centre, EuroControl Agency, Bruxelles.

Red Book, 1997. Methods for determining and processing probabilities CPR 12E. Committee for the Prevention of Disasters, The Hauge.

Robson, J.K., 2003. Ship / platform collision incident database (2001). Prepared by Serco Assurance for the Health and Safety Executive (HSE), UK.

Sales, J., Mushtaq, F., Christou, M.D., 2007. Analysis of Major Accidents Reported to the MARS Database During the Period 1994-2004. European Commission Joint Research Centre (JRC), Luxembourg.

Schönbeck, M., Rausand, M., Rouvroye, J., 2010. Human and organisational factors in the operational phase of safety instrumented systems : A new approach. Saf. Sci. 48, 310–318. doi:10.1016/j.ssci.2009.11.005.

Shirley, R.B., Smidts, C., Li, M., Gupta, A., 2015. Validating THERP : Assessing the scope of a full-scale validation of the Technique for Human Error Rate Prediction. Ann. Nucl. Energy 77, 194–211. doi:10.1016/j.anucene.2014.10.017.

Stanton, N.A., Salmon, P.M., Walker, G.H., Baber, C., Jenkins, D.P., 2005. Human Factors Methods: A Practical Guide for Engineering and Design. Ashgate Publishing Limited, Hampshire.

Sträter, O., 2000. Evaluation of Human Reliability on the Basis of Operational Experience. Gesellschaft für Anlagen und Reaktorsicherheit (GRS) GmbH.

Sträter, O., Bubb, H., 1999. Assessment of human reliability based on evaluation of plant experience : requirements and implementation. Reliab. Eng. Syst. Saf. 63 63, 199–219. doi:10.1016/S0951-8320(98)00047-7.

Swain, A.D., Guttmann, H.E., 1983. Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications. Sandia National Laboratories, Albuquerque, NM.

Williams, J.C., 1986. A proposed Method for Assessing and Reducing Human Error, in: Proceedings of the 9th Advance in Reliability Technology Symposium, University of Bradford. p. B3/R/1.

Wood, M.H., Arellano, A.L.V., Wijk, L. van, 2013. Corrosion-Related Accidents in Petroleum Refineries, Lessons learned from accidents in EU and OECD countries. European Commission Joint Research Centre (JRC), Luxembourg. doi:10.2788/379

List of Appendices

Appendix I: SIS safety life cycle overview, adapted from (IEC 61511, 2003) p.36

Safety life-cycle activity	Objectives	Require-ments clause or subclause (IEC 61511-1)	Inputs	Outputs
Hazard and risk assessment	To determine the hazards and hazardous events of the process and associated equipments, the requirement for risk reduction and the safety functions required to achieve the necessary risk reduction.	8	Process design, layouts, manning arrangements, safety targets	A description of the hazards, of the required safety function (s) and of the associated risk reduction.
Allocation of safety functions to protection layers	Allocation of the safety functions to protection layers and for each SIF, the associated safety integrity level	9	A description of the required safety instrumented function(s) and associated safety integrity levels	Description of allocation of safety requirements.
SIS safety requirement specification	To specify the requirements of each SIS, in terms of required safety instrumented functions, and their safety integrity	10	Description of allocation of safety requirements	SIS safety requirements, software safety requirements
SIS design and engineering	To design the SIS to meet the requirements for safety instrumented functions and safety integrity	11 and 12.4	SIS safety requirements software safety requirements	Design of the SIS in conformance with the SIS safety requirements, planning for the SIS integration test
SIS installation, commissioning and validation	To integrate and test the SIS To validate that the SIS meets all aspects the requirements for safety in terms of the required safety instrumented functions and the required safety integrity	12.3, 14, 15	SIS design, SIS integration test, SIS safety requirements, plan for the safety validation of	Fully functioning SIS in conformance with the SIS design results of SIS integration test, Results of the

Safety life-cycle activity	**Objectives**	**Require-ments clause or subclause (IEC 61511-1)**	**Inputs**	**Outputs**
			the SIS	installation, commissioning and validation activities
SIS operations and maintenance	To ensure that the functional safety of the SIS is maintained during operations and maintenance	16	SIS requirements, SIS design, plan for SIS operations and maintenance	Results of the operations and maintenance activities
SIS modifications	To make corrections, enhancements or adaption of the SIS, ensuring that the required safety integrity level is achieved and maintained	17	Revised SIS safety requirements	Results of SIS modifications
Decommissioning	To ensure proper review, sector organization, and ensure SIF remain appropriate	18	As built safety requirements and process information	SIF places out of service
SIS verification	To test and evaluate the outputs of a given phase to ensure correctness and consistency with respect to the products and standards provided as input to that phase	7, 12.7	Plan for the verification of SIS for each phase	Results of the verification of the SIS for each phase
SIS functional safety assessment	To investigate and arrive at a judgment on the functional safety achieved by the SIS	5	Planning for SIS functional safety assessment, SIS safety requirement	Results of SIS functional safety assessment

Appendix II: Collection of PSFs levels, adapted from (Gertman et al., 2005)

SPAR-H PSFs	SPAR-H PSF levels	SPAR-H Multipliers	HEART Multipliers	CREAM Multipliers	ASEP Multipliers	THERP Multipliers
Available time	Inadequate time	P (failure) = 1	11- EPC 2	-	P(failure) = 1,0 – table 7.2	P (failure) =1,0 – Table 20.1
	Time available = time required	10	1	5- CPC20	10 – Table 7.2	10 – Table 20.1
	Nominal time	1	-	1- CPC 19	1 – Table 7.2	1- Table 20.1
	Time available ≥ 5X time required	0,1	-	-	-	-
	Time available ≥ 50X time required	0,01	-	0,5 – CPC18	0,01 – Table 7.2	0,01 – Table 20.1
Stress/ stressors	Extreme	5	-	-	5- Table 7.3	5,25 – Table 20.16
	High	2	1,3 – EPC 29 1,15- EPC33	1,2 – CPC 22	-	2,5 – Table 20.16
	Nominal	1	-	1-CPC 21	-	-
Complexity	Highly complex	5	5,5- EPC 10	2 – CPC 17	2,5 or 5 (depending on stress)	-
	Moderately complex	2	-	1 – CPC 16	-	-
	Nominal	1	-	1 – CPC 15	-	-
Experience	Low	3	17 – EPC1	2-CPC 25	10 – Table 8.3	2 – Table 20.16

SPAR-H PSFs	**SPAR-H PSF levels**	**SPAR-H Multipliers**	**HEART Multipliers**	**CREAM Multipliers**	**ASEP Multipliers**	**THERP Multipliers**
/training			3 – EPC 15 8- EPC 6 6-EPC 9 4- EPC 12 2,5 – EPC 18 2 –EPC 20 1,6 EPC 24			
	Nominal	1	1	1- CPC 24	1	1
	High	0,5	-	0,8 – CPC 23	0,1 – Table 8.3	-
Procedures	Not available	50	-	-	P(failure) = 1,0 – Table 7.1, Table 8.1	50 – Table 20.7
	Incomplete	20	5 – EPC 11 3 – EPC 16,17 1,4 – EPC 28 1,2 – EPC 32	2 – CPC 14	-	10 – Table 20.7
	Available, but poor	5	5 –EPC 11 3 – EPC 16,17	2 – EPC 14	-	10 – Table 20.7

SPAR-H PSFs	SPAR-H PSF levels	SPAR-H Multipliers	HEART Multipliers	CREAM Multipliers	ASEP Multipliers	THERP Multipliers
			1,4 – EPC 28 1,2 – EPC 32			
	Nominal	1		1 – CPC 13	-	-
Ergonomics / HMI	Missing/ Misleading	50	-	-	P (failure) = 1,0 – Table 7.1, 8.1	100 or 1000 - Table 20.12
	Poor	10	10 – EPC 3 9 – EPC 4 8 – EPC 5,7 4 – EPC 13, 14 2,5 – EPC19 1,6 – EPC 23 1,4 – EPC 26 1,2 – EPC 32	5 – CPC 11 2 – CPC7	-	6 – Tables 20.9,11,12 10 – Tables 20.10,13,14
	Nominal	1	-	1 – CPC 9, 10,6	-	-
	Good	0,5	-	0,8 – CPC5 0,5 - CPC8	-	-
Fitness for duty	Unfit	P(failure) = 1.0	-	-	-	-

SPAR-H PSFs	**SPAR-H PSF levels**	**SPAR-H Multipliers**	**HEART Multipliers**	**CREAM Multipliers**	**ASEP Multipliers**	**THERP Multipliers**
	Degraded fitness	5	1,8 – EPC 22 1,2 – EPC 30 1,1 – EPC 35	-	-	-
	Nominal	1	-	-	-	-
Work processes	Poor	2	2 - EPC 21 1,6 – EPC 25 1,4 – EPC 27 1,2 – EPC 31 1,06 – EPC 36	5 – CPC 29 2 – CPC4 1,2 – CPC 3 1 – CPC 28	-	-
	Nominal	1	-	1 – CPC 2.27	-	-
	Good	0,8	-	0,8 – CPC 1 0,5 – CPC 26	-	-

Appendix III: Criteria for the notification of an accident to the European Commission, adapted from "Seveso Directive" (EC, 2012)

I. Any accident covered by paragraph 1 or having at least one of the consequences described in paragraphs 2,3,4 and 5 must be notified to the Commission.

1. **Substances involved**

   Any fire or explosion or accident discharge of a dangerous substance involving, a quantity of at least 5% of the qualifying quantity laid den in column 3 of Annex I of the Seveso Directive (2012/18/EU).

2. **Injury to persons and damage to real estate**

   An accident directly involving a dangerous substances and giving rise to one of the following events:

   - a death,
   - Six persons injured within the establishment and hospitalized for at least 24 hours,
   - One person outside the establishment hospitalized for at least 24 hours,
   - Dwelling(s) outside the establishment damaged and unusable as a result of the accidents,
   - The evacuation or confinement of persons for more than 2 hours (persons × hours): the value is at least 500,
   - The interruption of drinking water, electricity, gas or telephone services for more than 2 hours (persons × hours): the value is at least 1000.

3. **Immediate damage to the environment**

   - Permanent or long-term damage to terrestrial habitats:
     - 0.5 hectares (ha) or more of a habitat of environmental or conservation importance protected by legislation,
     - 10 or more hectares of more widespread habitat, including agricultural land,
   - Significant or long-term damage to freshwater and marine habitats
     - 10 Km or more of river or canal,
     - 1 ha or more of a lake or pond,
     - 2 ha or more of a delta,
     - 2 ha or more of a coastline or open sea,
   - Significant damage to an aquifer or underground water
     - 1 ha or more.

4. **Damage to property**

   - Damage to property in the establishment: at least ECU 2 million,

   - Damage to property outside the establishment at least ECU 0.5 million.

5. **Cross-border damage**

   - Any accident directly involving a dangerous substance giving rise to effects outside the territory of the Member State concerned.

II. Accidents or “near misses” which Member States regard as being of particular technical interest for preventing major accidents and limiting their consequences and which do not meet the quantitative criteria above should be notified to the Commission.

Appendix IV: EMARS accident reporting structure: available to extract the data from accident report, adapted from (Emars, n.d.).

Accident profile

Date/Time of major occurrence

Accident tile

Accident type	Reporting under	Seveso II status
Major accident	EU Seveso I Directive	
Near miss	EU Seveso II Directive	
Near miss	EU Seveso II Directive + OECD	
Other event	EU Seveso II Directive + UN/ECE	
	OECD	
	UN/ECE	

Industrial type

Reason for reporting

☐	Substances involved: greater than 5% of quantity in Column 3 of Annex I (Seveso Directive)
☐	Injury to persons: ≥ 1 fatalities, ≥ 6 hospitalizing injuries etc
☐	Immediate damage to environment (according to Annex VI)
☐	Damage to property: on-site > 2M €, off-site > 0.5M €
☐	Cross-border damage: transboundary accidents
☐	Interesting for lessons learned

Accident report

Accident description:

Accident involved:

Domino effects

Natech events

Transboundary effects

Contractors

Release

Major occurrences

□	Fluid release to ground
□	Fluid release to water
□	Gas/vapour/ mist / etc release to air
□	Not known / not applicable
□	Solid release to air
□	Solid release to ground
□	Solid release to water

Initiating events

□	Fluid release to ground
□	Fluid release to water
□	Gas/vapour/ mist / etc release to air
□	Not known / not applicable
□	Solid release to air
□	Solid release to ground
□	Solid release to water

Fire

Major occurrences

□	Conflagration (a general engulfment fire)
□	Fireball (burning mass rising in air, often after BLEVE)
□	Flash fire (burning vapour cloud, subsonic flame front)
□	Jet flame (burning jet of fluid from orifice)
□	Not known / not applicable
□	Pool fire (burning pool of liquid, contained or uncontained)

Initiating events

□	Conflagration (a general engulfment fire)
□	Fireball (burning mass rising in air, often after BLEVE)
□	Flash fire (burning vapour cloud, subsonic flame front)
□	Jet flame (burning jet of fluid from orifice)
□	Not known / not applicable
□	Pool fire (burning pool of liquid, contained or uncontained)

Explosion

Major occurrences

Initiating events

□	BLEVE (boiling liquid expanding vapour explosion)
□	Dust explosion
□	Explosive decomposition (of unstable material)
□	Not known / not applicable
□	Pressure burst (rupture of pressure system)
□	Rapid phase-transition explosion (rapid change of state)
□	Runaway reaction explosion (usually exothermic)
□	VCE (Vapour Cloud Explosion; supersonic wave front)

□	BLEVE (boiling liquid expanding vapour explosion)
□	Dust explosion
□	Explosive decomposition (of unstable material)
□	Not known / not applicable
□	Pressure burst (rupture of pressure system)
□	Rapid phase-transition explosion (rapid change of state)
□	Runaway reaction explosion (usually exothermic)
□	VCE (Vapour Cloud Explosion; supersonic wave front)

Transport

Major occurrences

□	Air
□	Rail
□	Road
□	Water (sea. river, etc)

Initiating events

□	Air
□	Rail
□	Road
□	Water (sea. river, etc)

Others

Site description

Installation / unit description

Storage

Major occurrences		Equipment type
□	Distribution-associated (not on-site of manufacture)	
□	Not known / not applicable	
□	Other	
□	Process-associated (stockholding, etc. on-site of manufacture)	

Initiating Events		Equipment type
□	Distribution-associated (not on-site of manufacture)	
□	Not known / not applicable	
□	Other	
□	Process-associated (stockholding, etc. on-site of manufacture)	

Process

Major occurrences		Equipment type
□	Chemical batch reaction	
□	Chemical continuous reaction	
□	Disposal activities (incinerating, buying, etc)	
□	Electrochemical operations	
□	Heat exchanger (boiler, refrigerator, heating coils, etc)	
□	Not known / not applicable	
□	Others	
□	Physical operations (mixing,	

	melting, crystallizing, etc)	
□	Power generation (burning fuel etc.)	
□	Treating /use for treatment (stanching, preserving etc.)	

Initiating events		Equipment type
□	Loading /unloading activities (transfer interfaces)	
□	Mechanical transfer (conveyors etc)	
□	Not known / not applicable	
□	Others	
□	Pipeline / pipework treatment	
□	Vehicular transport	

Transfer

Major occurrences		Equipment type
□	Loading /unloading activities (transfer interfaces)	
□	Mechanical transfer (conveyors etc)	
□	Not known / not applicable	
□	Others	
□	Pipeline / pipework treatment	
□	Vehicular transport	

Initiating events		Equipment type
□	Chemical batch reaction	

□	Chemical continuous reaction	
□	Disposal activities (incinerating, buying, etc)	
□	Electrochemical operations	
□	Heat exchanger (boiler, refrigerator, heating coils, etc)	
□	Not known / not applicable	
□	Others	
□	Physical operations (mixing, melting, crystallizing, etc)	
□	Power generation (burning fuel etc.)	
□	Treating /use for treatment (stanching, preserving etc.)	

Transport

Major occurrences		Equipment type
□	Not known / not applicable	
□	Others	
□	Packing (bagging, cylinder filling, drum filling etc)	

Initiating events		Equipment type
□	Not known / not applicable	
□	Others	
□	Packing (bagging, cylinder filling, drum filling etc)	

Others

Substances involved

Substances Classification

□	Named substance
□	Very toxic
□	Toxic
□	Oxidizing
□	Explosive
□	Flammable
□	Highly Flammable
□	Extremely Flammable
□	Dangerous for the environment
□	Any classification

Substance Involved

Substances	CAS Number	Directly Involved (tonnes)	Potential Quantity (tons)

Causes of the accidents

The reason for the accident (potentially un-wanted event)

Organizational

Causative Factor		Type
□	Blockage	

□	Component / machinery failure / malfunction	
□	Corrosion / fatigue	
□	Electrostatic accumulation	
□	Instrument / control / monitoring-device failure	
□	Loss of process control	
□	Not identified	
□	Not known / not applicable	
□	Others	
□	Runaway reaction	
□	Unexpected reaction / phase-transaction	
□	Vessel / container / containment-equipment failure	

Plant / Equipment

Causative Factor		Type
□	Malicious intervention	
□	Not identified	
□	Not known / not applicable	
□	Operator error	
□	Operator health (includes ailments, intoxication, death, etc)	
□	Others	
□	Wilful disobedience / failure to carry out duties	

Human

Causative Factor		Type
□	Design of plant / equipment/ system	
□	Installation	
□	Isolation of equipment / system	

□	Maintenance / repair	
□	Management attitude problem	
□	Management organization inadequate	
□	Manufacture / construction	
□	Not identified	
□	Not known / not applicable	
□	Organized procedures	
□	Others	
□	Process analysis	
□	Staffing	
□	Supervision	
□	Testing/ inspection/ recording	
□	User-unfriendly (apparatus, system etc)	

External

Causative Factor		Type
□	Domino-effect from other accident	
□	Establishment safeguards / security deficiency	
□	Natural events (weather, temperature, earthquake, etc)	
□	Not identified	
□	Not known / not applicable	
□	Others	
□	Struck by object	
□	Transport accident	
□	Utilities failure (electricity, gas, water, steam air, etc)	

Others

Consequences

Human

On site		Quantity	Quantity / Effect
□	At risk		
□	Fatalities		
□	Injuries		
□	Others		

Off site		Quantity	Quantity / Effect
□	At risk		
□	Fatalities		
□	Injuries		
□	Others		

Environment

On site		Quantity	Quantity / Effect
□	Freshwater: freshwater reservoir		
□	Freshwater: pond/lake		
□	Freshwater: river		
□	Freshwater: stream/tributary		
□	Inland: arable land/ crops/ vineyards/ orchards		
□	Inland: grassland/ pasture/ meadow		
□	Inland: marsh/ reedbeds		
□	Inland: metropolitan development		
□	Inland: moor/ heathland/ upland vegetation		

□	Inland: Parkland/ common land		
□	Inland: Rural development		
□	Inland: Urban development		
□	Inland: Woodland; predominantly or totally natural		
□	Inland: Woodland; predominantly or totally plantation		
□	Offshore: Estuary		
□	Offshore: Saline lagoon		
□	Offshore: Sea/ seabed		
□	Others		
□	Shore: Rocky shore		
□	Shore: Salt-marsh / mud-flats		
□	Shore: Sand / dunes/ dune slacks		
□	Shore: Shingle beach		

Off site		Quantity	Quantity / Effect
□	Freshwater: freshwater reservoir		
□	Freshwater: pond/lake		
□	Freshwater: river		
□	Freshwater: stream/tributary		
□	Inland: arable land/ crops/ vineyards/ orchards		
□	Inland: grassland/ pasture/ meadow		
□	Inland: marsh/ reedbeds		
□	Inland: metropolitan development		
□	Inland: moor/ heathland/ upland vegetation		

□	Inland: Parkland/ common land		
□	Inland: Rural development		
□	Inland: Urban development		
□	Inland: Woodland; predominantly or totally natural		
□	Inland: Woodland; predominantly or totally plantation		
□	Offshore: Estuary		
□	Offshore: Saline lagoon		
□	Offshore: Sea/ seabed		
□	Others		
□	Shore: Rocky shore		
□	Shore: Salt-marsh / mud-flats		
□	Shore: Sand / dunes/ dune slacks		
□	Shore: Shingle beach		

Cost

On site		Cost in Euro	Quantity / Effects
□	Material losses		
□	Others		
□	Response, cleanup, restoration costs		

Off site		Cost in Euro	Quantity / Effects
□	Material losses		
□	Others		
□	Response, cleanup, restoration costs		

Disruption

On site		Quantity	Quantity / Effects
□	Infrastructure (telecommunication, roads, railways, waterways, air transport etc)		
□	Nearby factories, offices, small shops		
□	Nearby residence, hotels		
□	Others		
□	Other places of public assembly		
□	School, hospitals, instaurations		
□	Utilities (gas, water, electricity etc)		

Off site		Quantity	Quantity / Effects
□	Infrastructure (telecommunication, roads, railways, waterways, air transport etc)		
□	Nearby factories, offices, small shops		
□	Nearby residence, hotels		
□	Others		
□	Other places of public assembly		
□	School, hospitals, instaurations		
□	Utilities (gas, water, electricity etc)		

Emergency response

Emergency response	Quantity	Quantity / Effects

□	Evacuation		
□	Off-site external services		
□	On-site external services		
□	Others		
□	Sheltering		

Remedial measure		Quantity	Quantity / Effects
□	Decontamination		
□	Other		
□	Restoration		

Theme of lessons learned

□	Causes – External
□	Causes - Human
□	Causes – Organizational
□	Causes – Plant/ equipment
□	Emergency response
□	Others

Lessons Learned

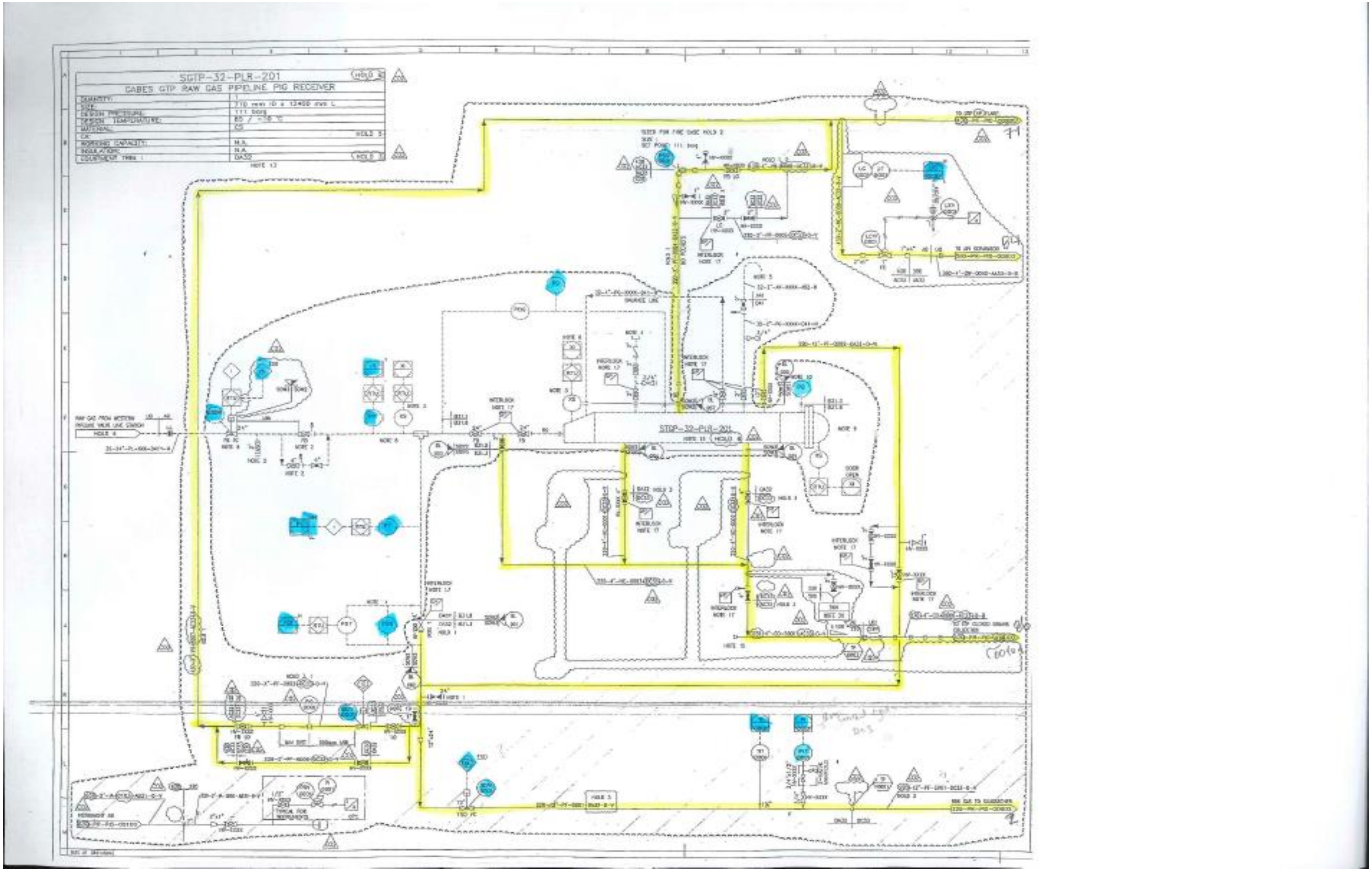
Attachment Section

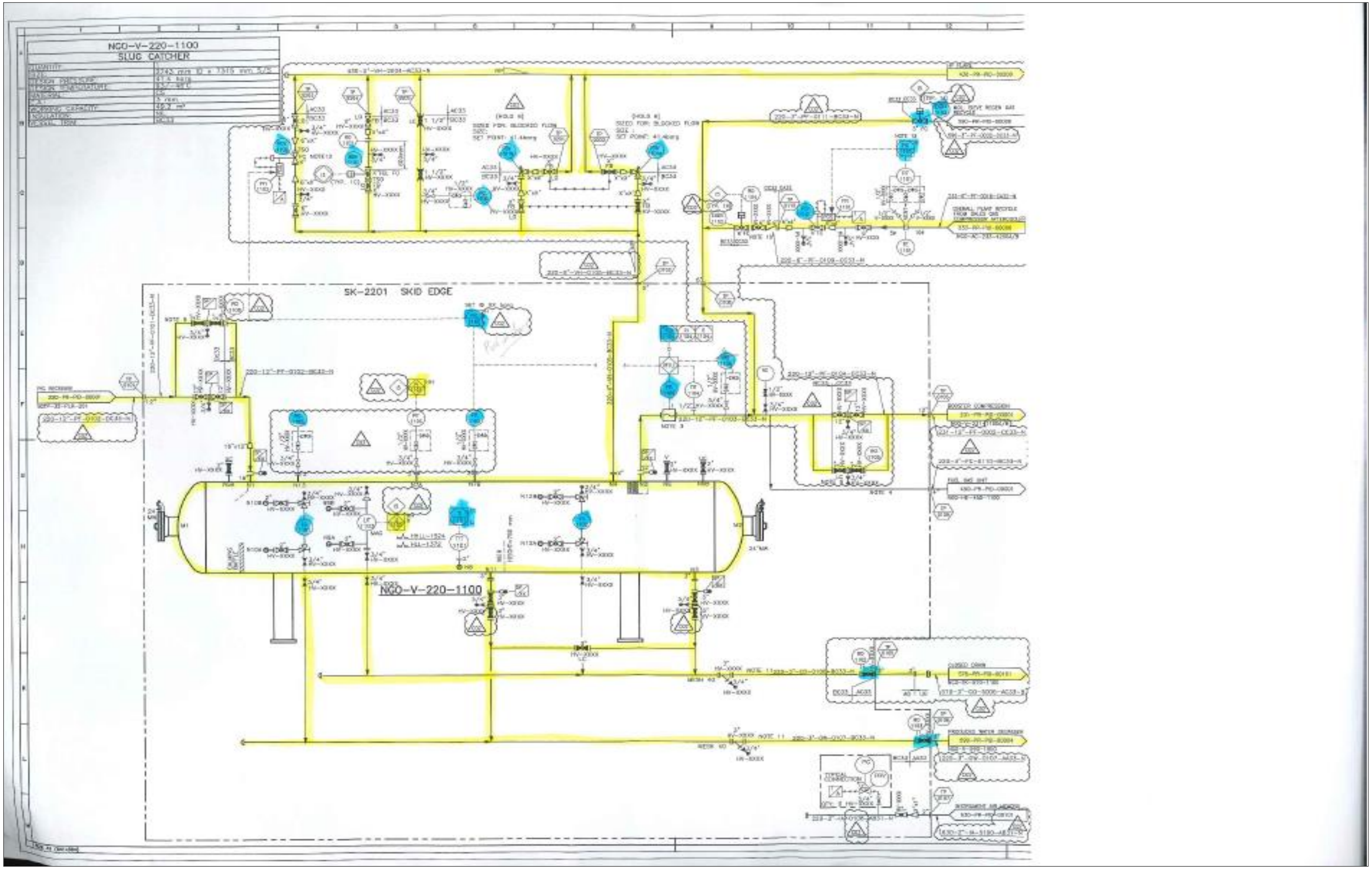
Appendix V: Selection criteria for THERP tables

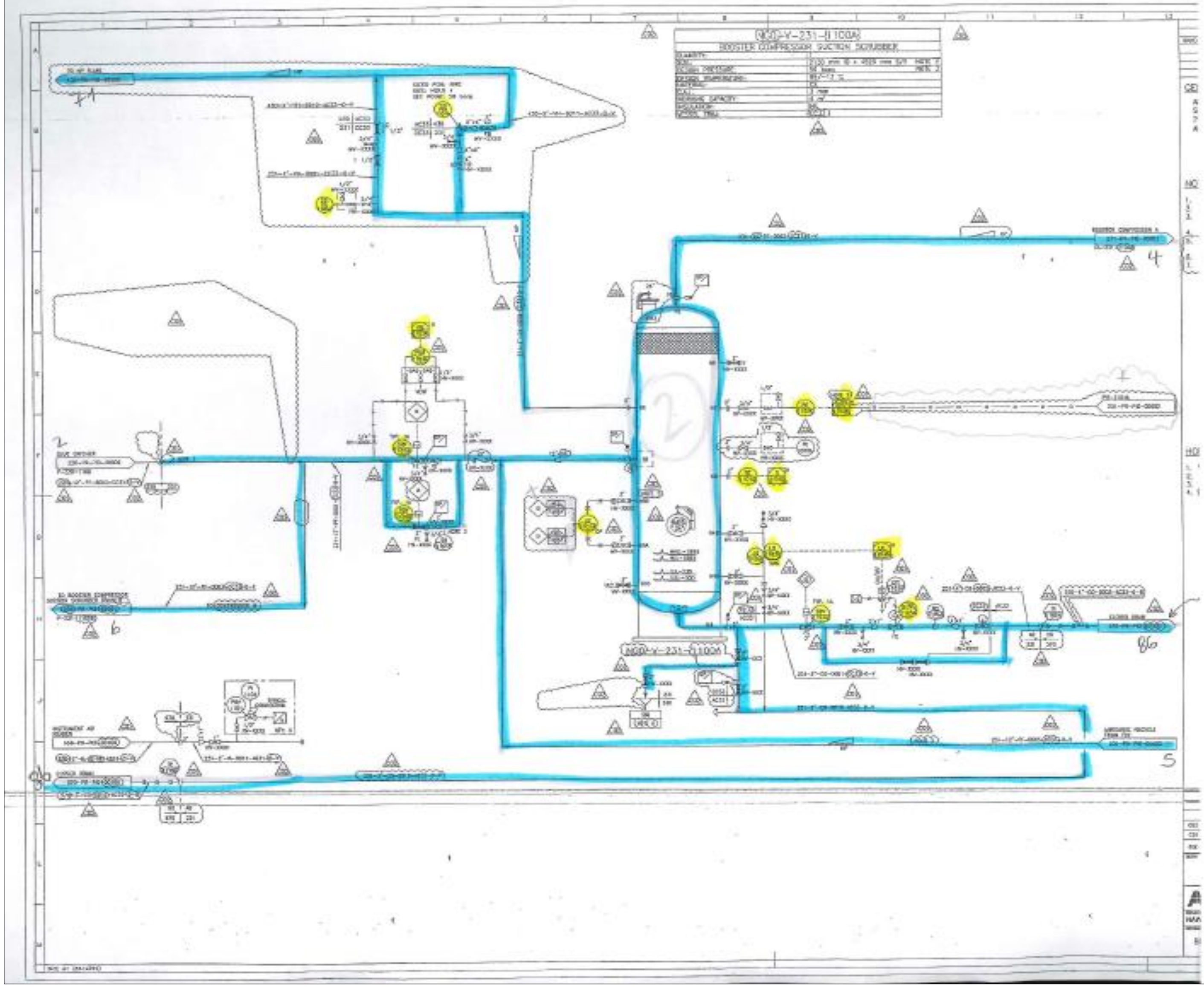
Action type	Corresponding THERP tables	THERP description	Rationale for selection
Monitoring equipment from field (M)	Table 20-27, item (4)	Table to estimate the probabilities that the basic walk-around inspection (after 4 days) will fail to detect a particular deviant indication of equipment outside the control room within 30 days, given one inspection per shift for three shifts per day. Assumed that no written procedures are used.	Basic walk around table has been selected since monitoring in chemical process industry is usually performed by a walk-around carried out by an operator. Item (4) has been selected based on expert judgment.
Monitoring/ operating equipment from control room (A)	Table 20-11, item (1) & item (2)	Table to estimate the probabilities for errors of commission in check-reading displays. Item (1) is related to digital indicators and item (2) is for analog meters with easily seen limit marks.	The specific table has been selected because operations are related to control room and corresponding table can provide the closest estimate to the actions considered in this action type.
Communication (C)	Table 20-7, item (2) & item (3)	Table to estimate the probability of errors of omission per item of instruction when use of written procedures is specified. Item (2) corresponds to when procedures with checkoff provision are correctly used for long list > 10 items. Item (3) when procedures without checkoff provisions are used for short list < 10 items.	Procedures without check off provisions for short list < 10 items has been selected to represent the communication errors in chemical process industry.
Manual tasks on-field (F)	Table 20-13, item (4)	Table to estimate the failure probability for selection errors of locally operated valves. Item (4) represents the unclearly, ambiguously labelled, part of group of a group of two or more that are similar in one of the following: size and shape, state or presence of tags.	The selection errors table has been selected to represent the manual tasks on-field tasks since number of times selection errors have been observed during this action class. Furthermore, valves are usually grouped together in process industry for certain operations. Hence, corresponding table and item can provide the required correspondence.

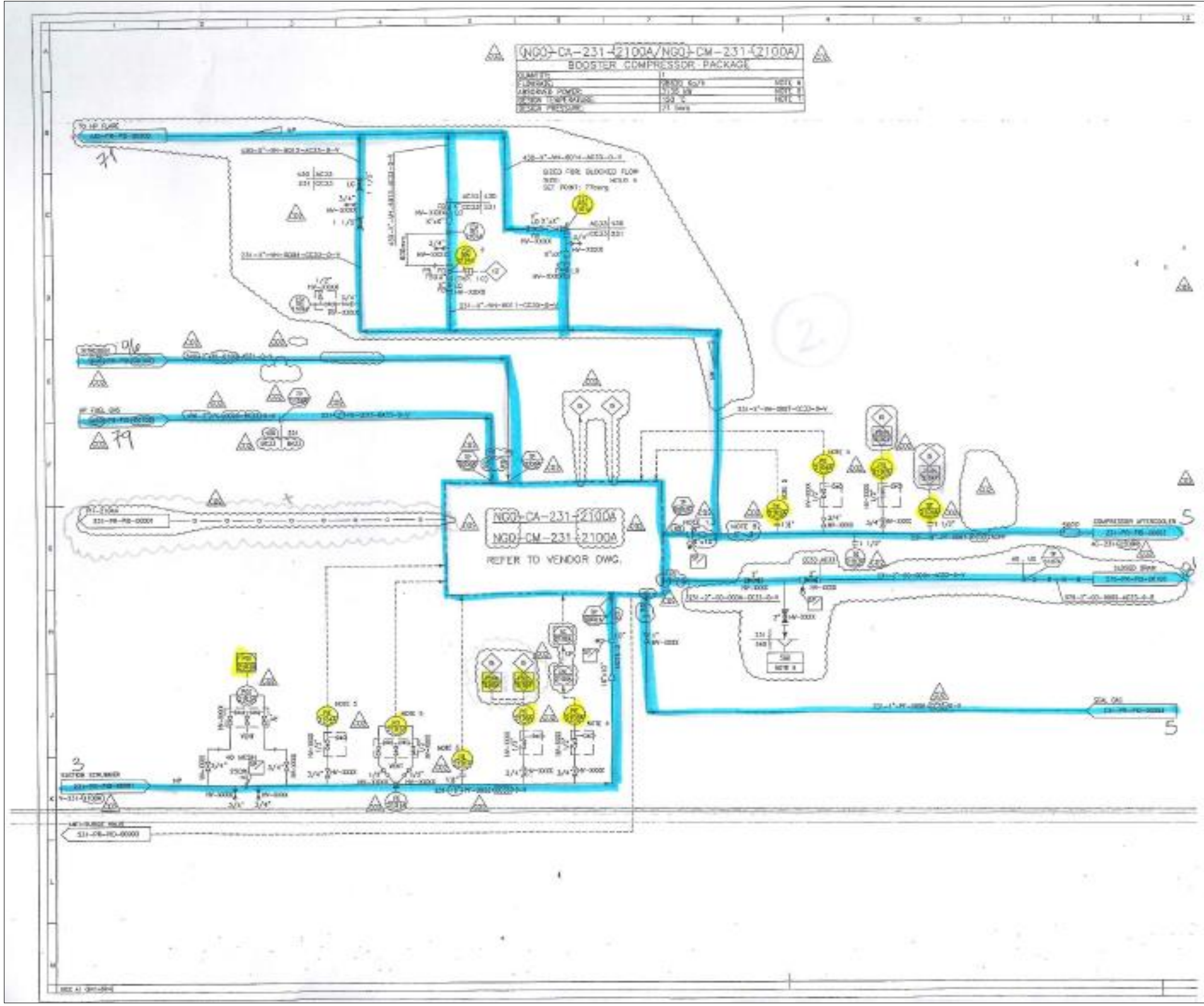
Reporting (R)	Table 20-22, item (9)	Table to estimate the probability that a checker will fail to detect errors made by others. Item (9) represent the checking status of equipment if that status affects one’s safety when performing the tasks.	This table has been selected to represent the reporting based on the assumption that whenever checker/ operator detects the problem, he will certainly report the problem.
Diagnostic: Monitoring (M)	Table 20-22, item (4)	Table to estimate that a checker will fail to detect errors made by others. Item (4) representing those checking operations that involve active participation, such as special measurements. This table applies to cases during the normal operations.	This table has been selected to represent the supervisor’s failure probability in the process industry. Due to possible complexity of supervisor’s tasks item (4) has been selected.
Diagnostic: Control room action (A)	Table 20-2, item (2)	Table to estimate the failure probabilities for rule-based actions by control room personnel after diagnosis of an abnormal events. This is for the CR crew rather than one individual.	The corresponding action class is representing the failure during CR actions following an abnormal situation therefore the considered THERP table and the item can provide a high relevance.
Diagnostic: Manual tasks on-field (F)	Table 20-16 item (6)	Table to modify the error probabilities for the effects of stress and experience levels. Item (6) corresponds to the step-by-step tasks for a novice operator.	In order to select this table, it has been assumed that following an abnormal situation, stress level is also increase. Therefore, corresponding table multiplier (i.e. ×10) has been used for maximum affect to modify probability of normal manual tasks on- field. The conservative multiplier has been used which is for a novice operator.

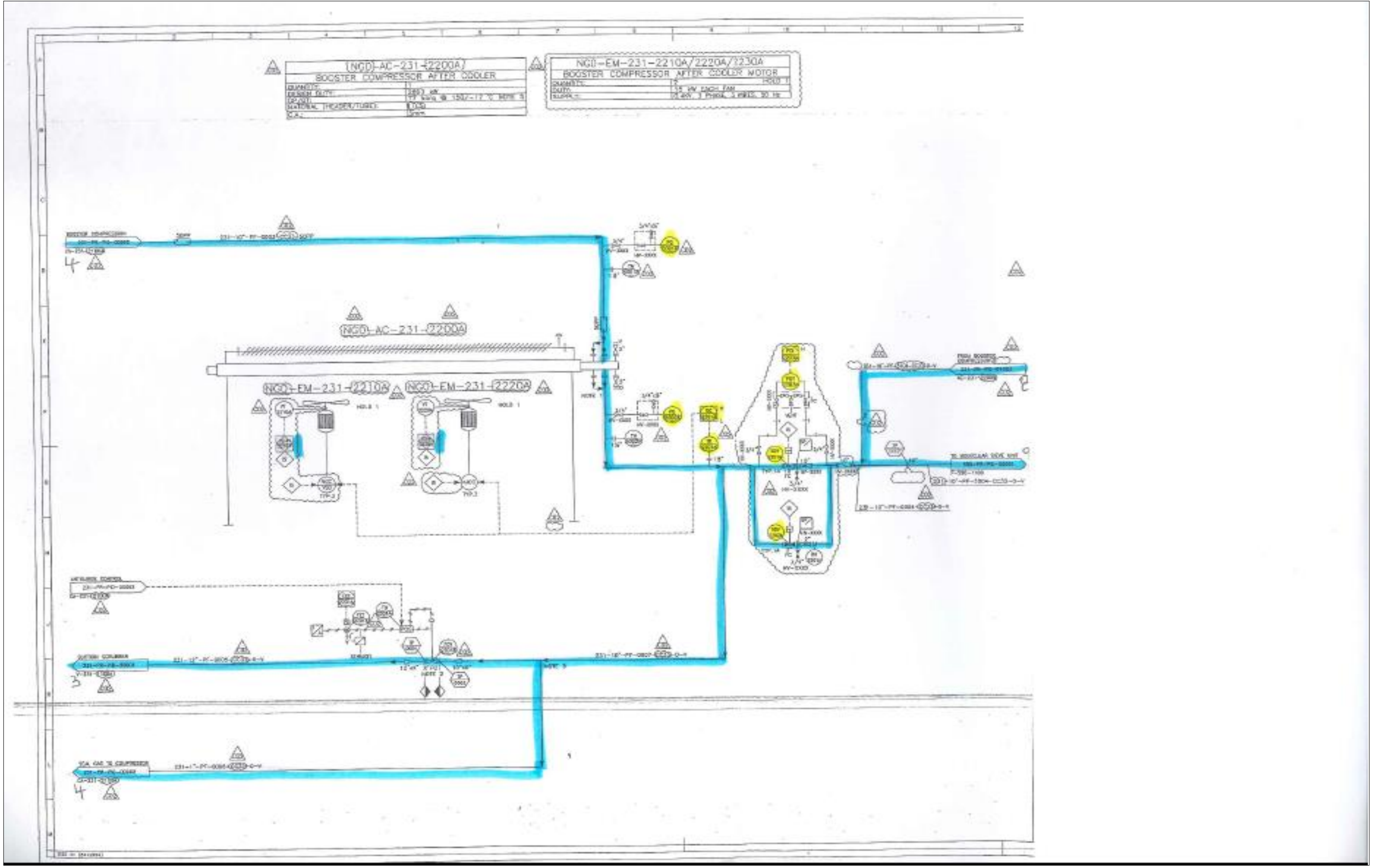
Appendix VI: Piping and instrumentation diagrams, used in case study

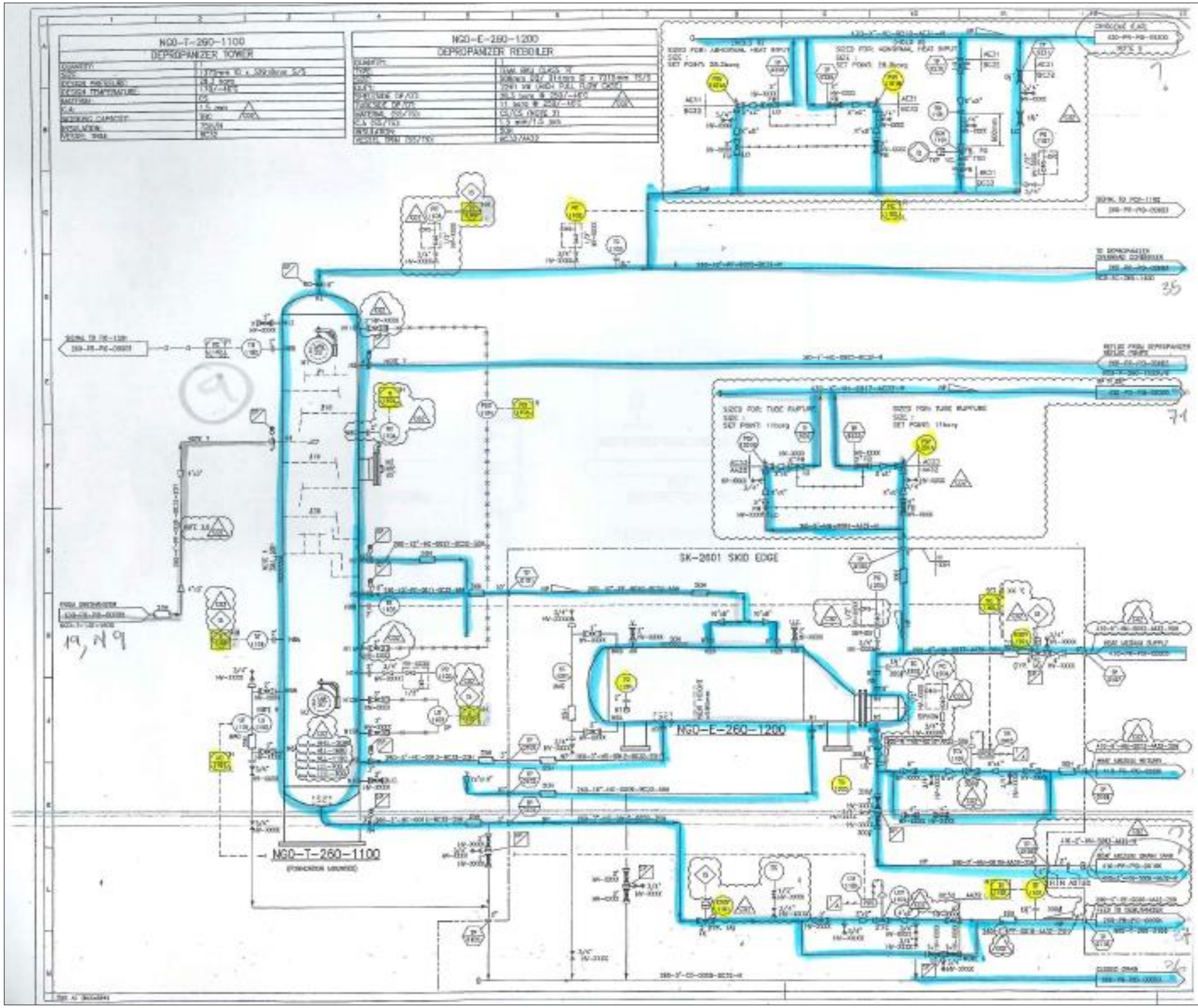


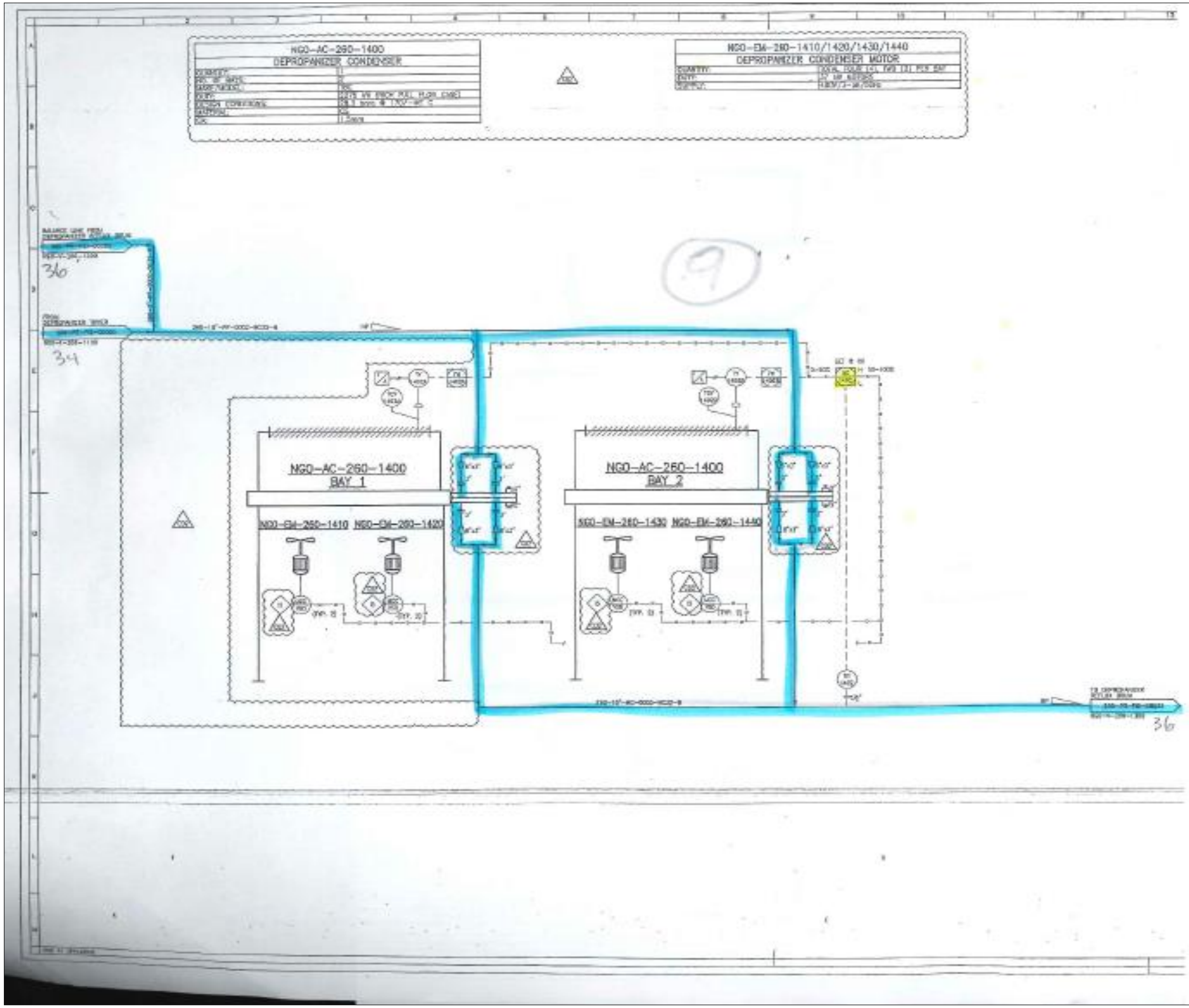

NGO-V-220-1100
SLUG CATCHER
SK-2201 SKID EDGE
NGO-V-220-1100
BOOSTER COMPRESSION
CLOSED DRAIN
PRODUCED WATER DEGASSER
TYPICAL CONNECTION

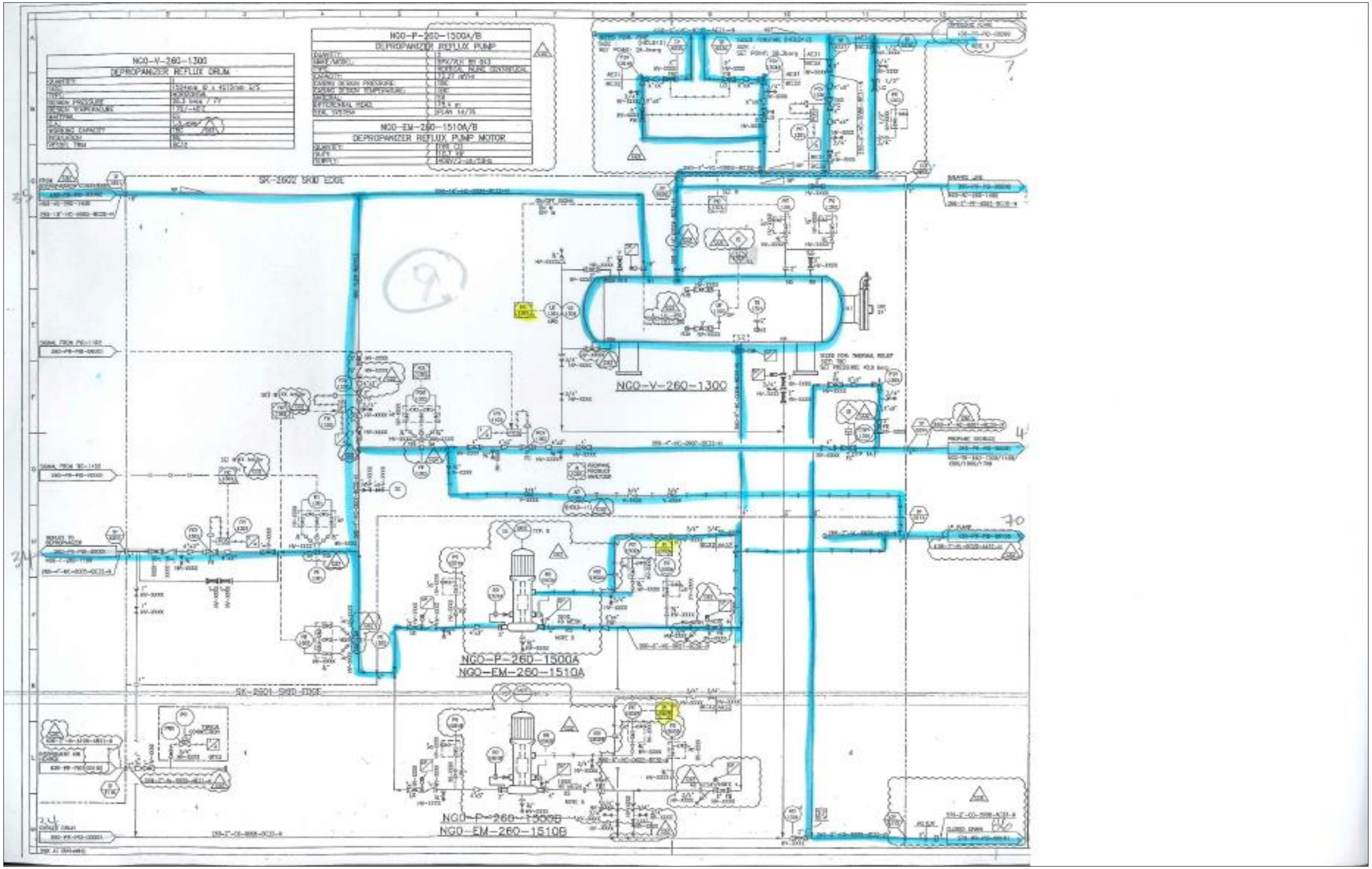

V-231-[illegible]100A
BOOSTER COMPRESSOR SUCTION SCRUBBER
1
2
4
5
6

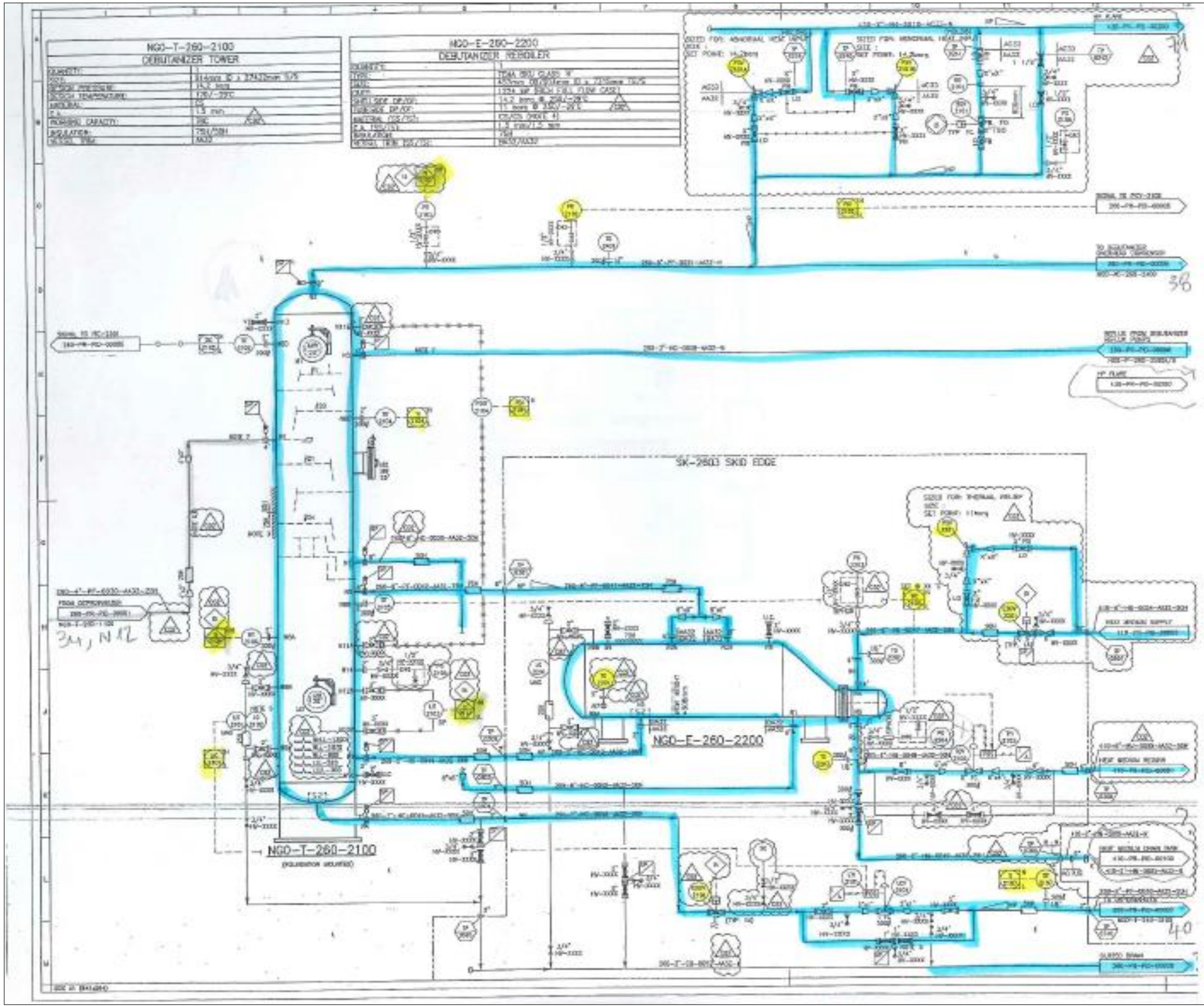

NGO-CA-231-2100A/NGO-CM-231-2100A
BOOSTER COMPRESSOR PACKAGE
NGO-CA-231-2100A
NGO-CM-231-2100A
REFER TO VENDOR DWG.
TO HP FLARE
71
96
79
3
5
5
2

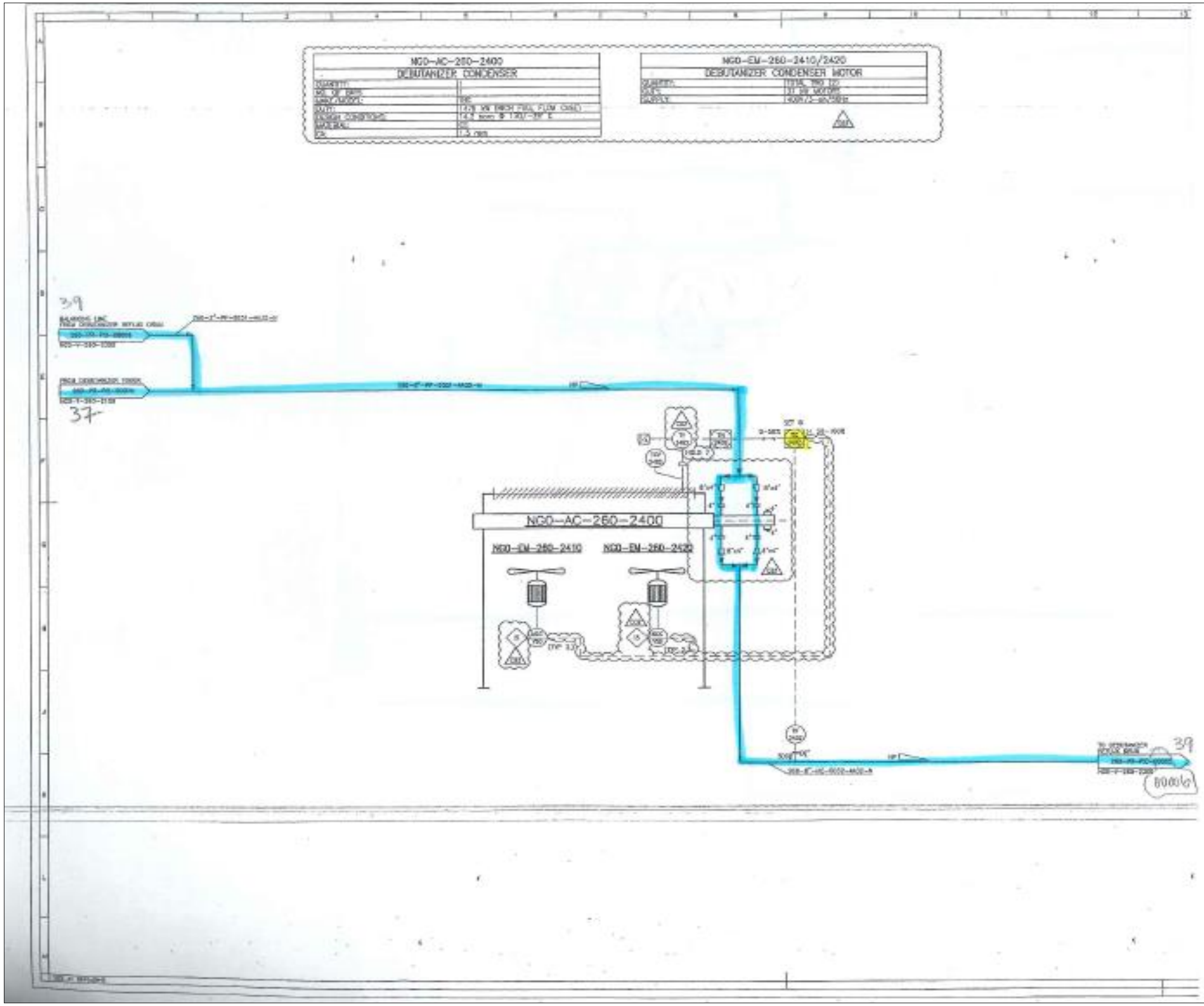

NGD-AC-231-2200A
BOOSTER COMPRESSOR AFTER COOLER
QUANTITY:
DESIGN DUTY:
MATERIAL (HEADER/TUBE):
C.A.:
NGD-EM-231-2210A/2220A/2230A
BOOSTER COMPRESSOR AFTER COOLER MOTOR
QUANTITY:
DUTY:
SUPPLY:
NGD-AC-231-2200A
NGD-EM-231-2210A
NGD-EM-231-2220A
HOLD 1
4
3
4

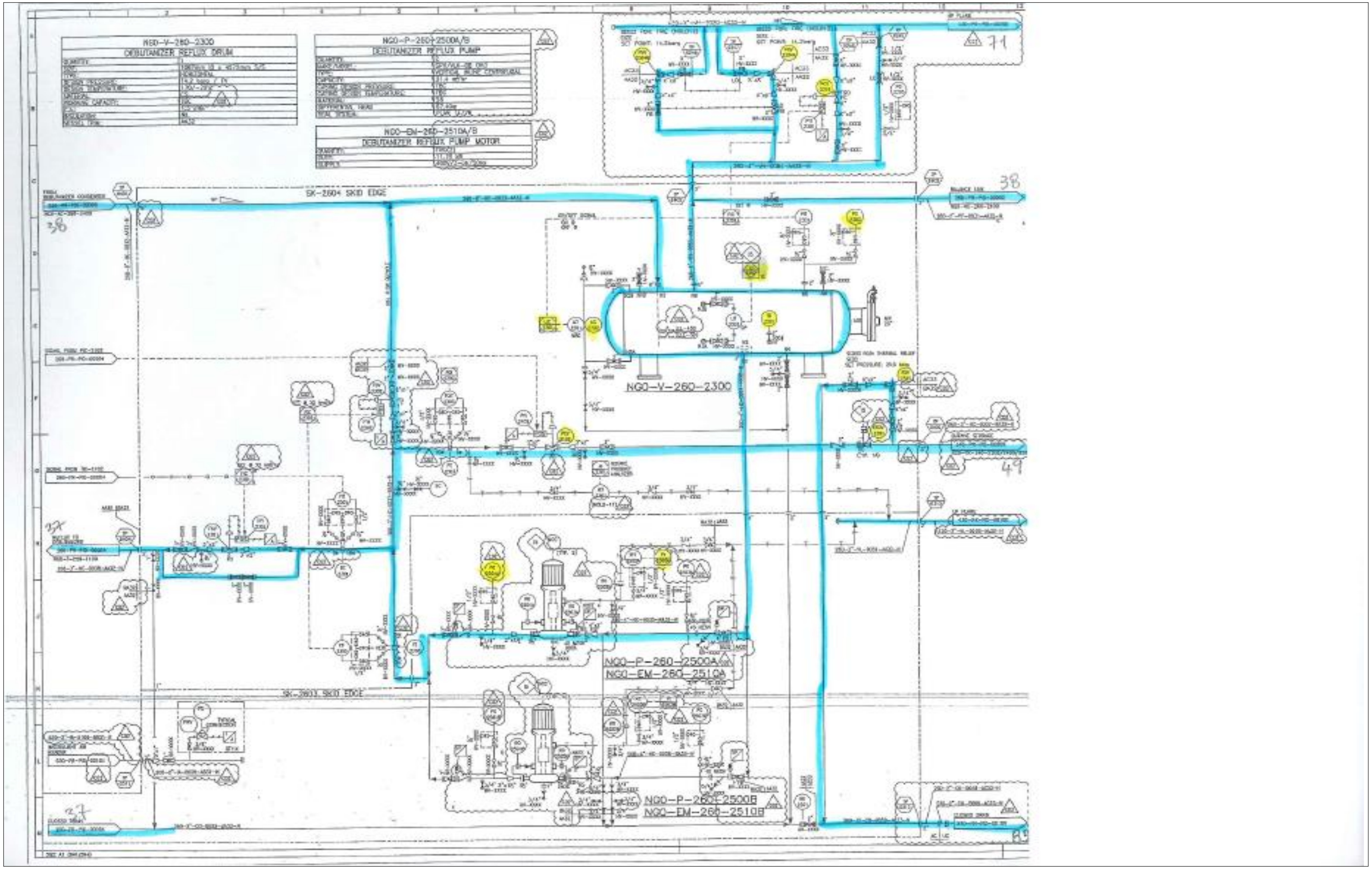

NGO-T-260-1100
DEPROPANIZER TOWER
NGO-E-260-1200
DEPROPANIZER REBOILER
SK-2601 SKID EDGE
NGO-E-260-1200
NGO-T-260-1100
9
19, 49
7
35
71
26

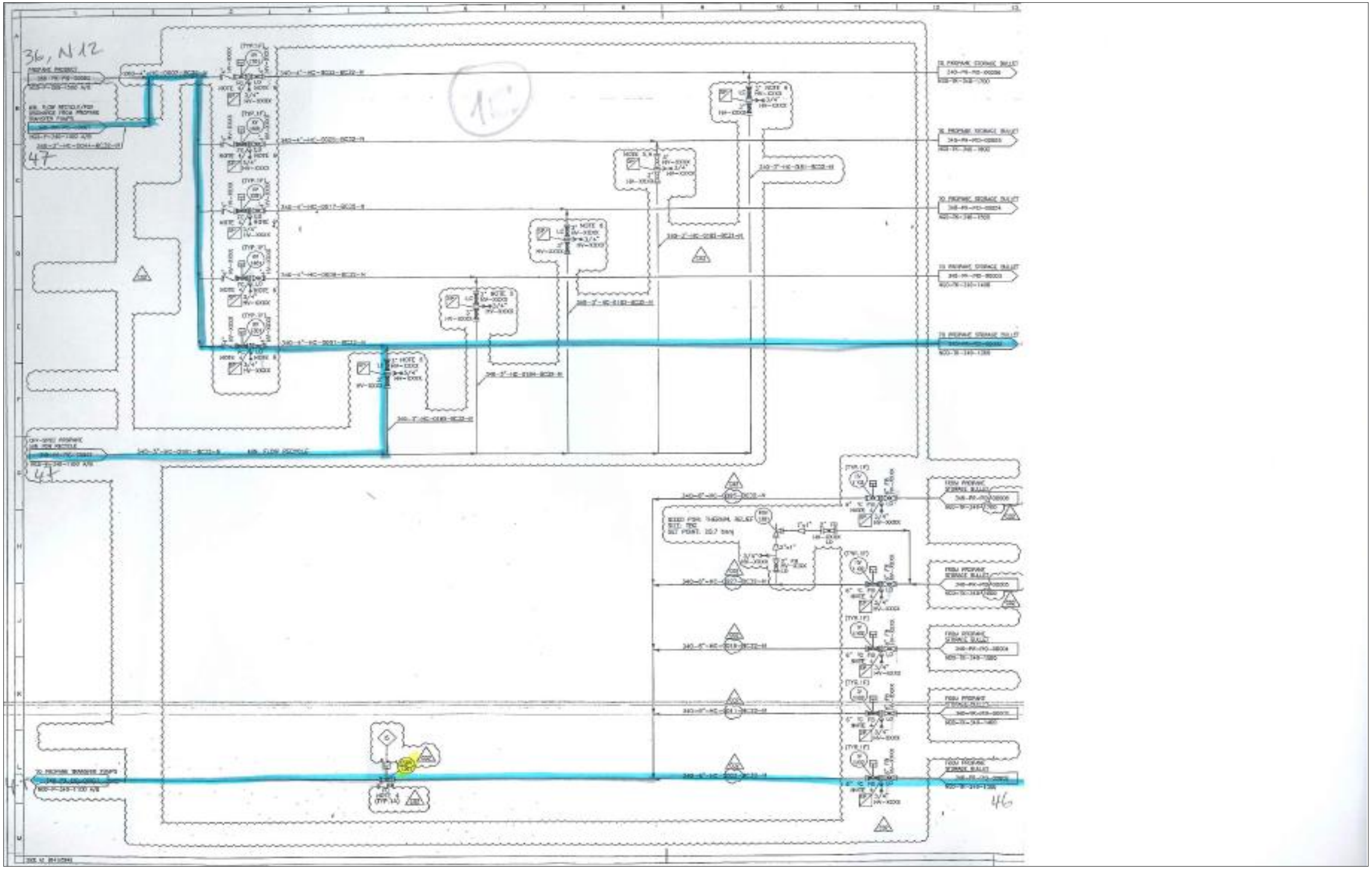

NGO-AC-260-1400
DEPROPANIZER CONDENSER
NGO-EM-260-1410/1420/1430/1440
DEPROPANIZER CONDENSER MOTOR
9
36
34
NGO-AC-260-1400
BAY 1
NGO-AC-260-1400
BAY 2
NGO-EM-260-1410
NGO-EM-260-1420
NGO-EM-260-1430
NGO-EM-260-1440
36

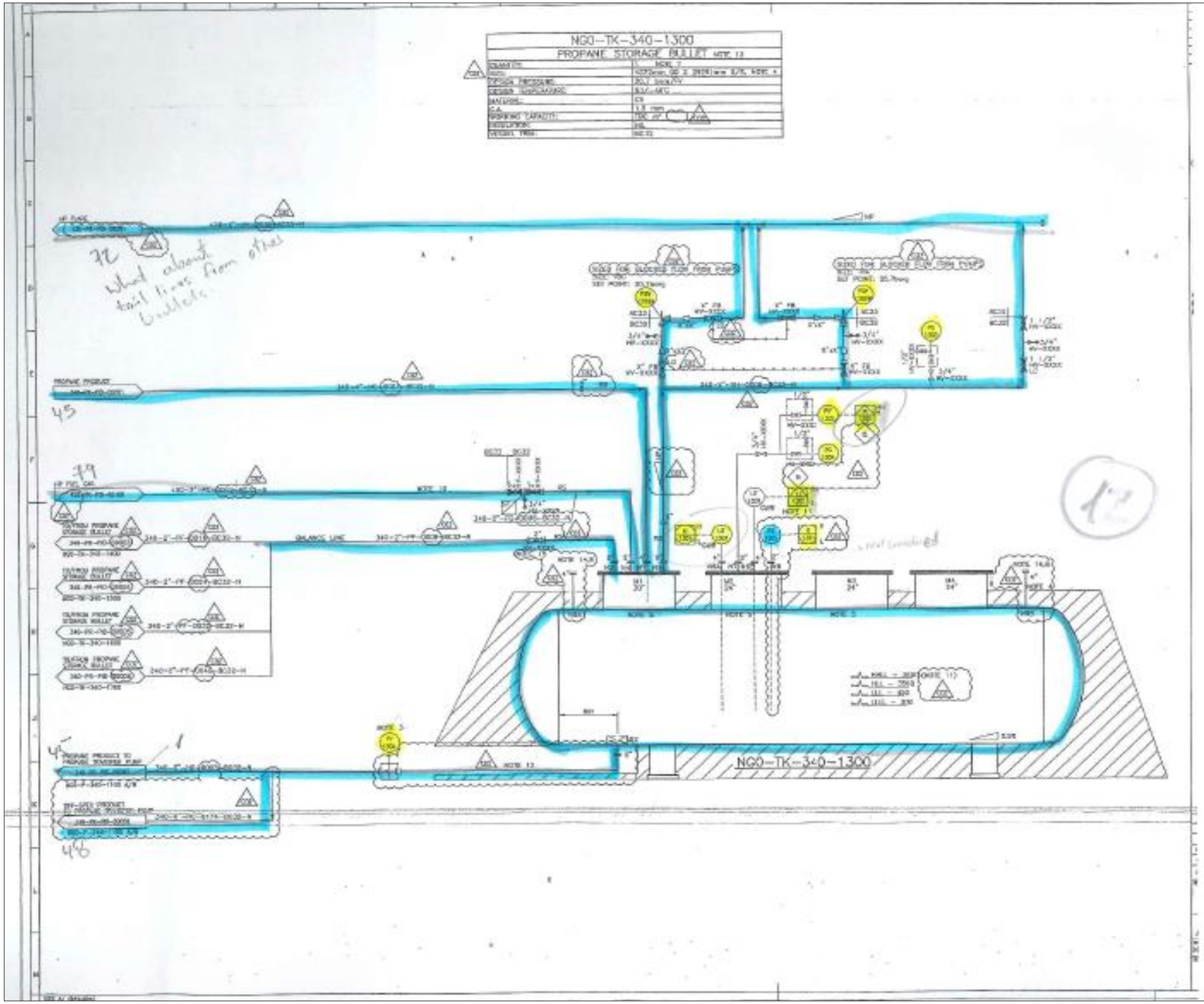

NGO-V-260-1300
DEPROPANIZER REFLUX DRUM
NGO-P-260-1300A/B
DEPROPANIZER REFLUX PUMP
NGO-EM-260-1510A/B
DEPROPANIZER REFLUX PUMP MOTOR
SK-2602 SKID EDGE
SK-2601 SKID EDGE
NGO-V-260-1300
NGO-P-260-1300A
NGO-EM-260-1510A
NGO-P-260-1300B
NGO-EM-260-1510B
PROPANE PRODUCT
CLOSED DRAIN
35
34
9
7
4
70
24

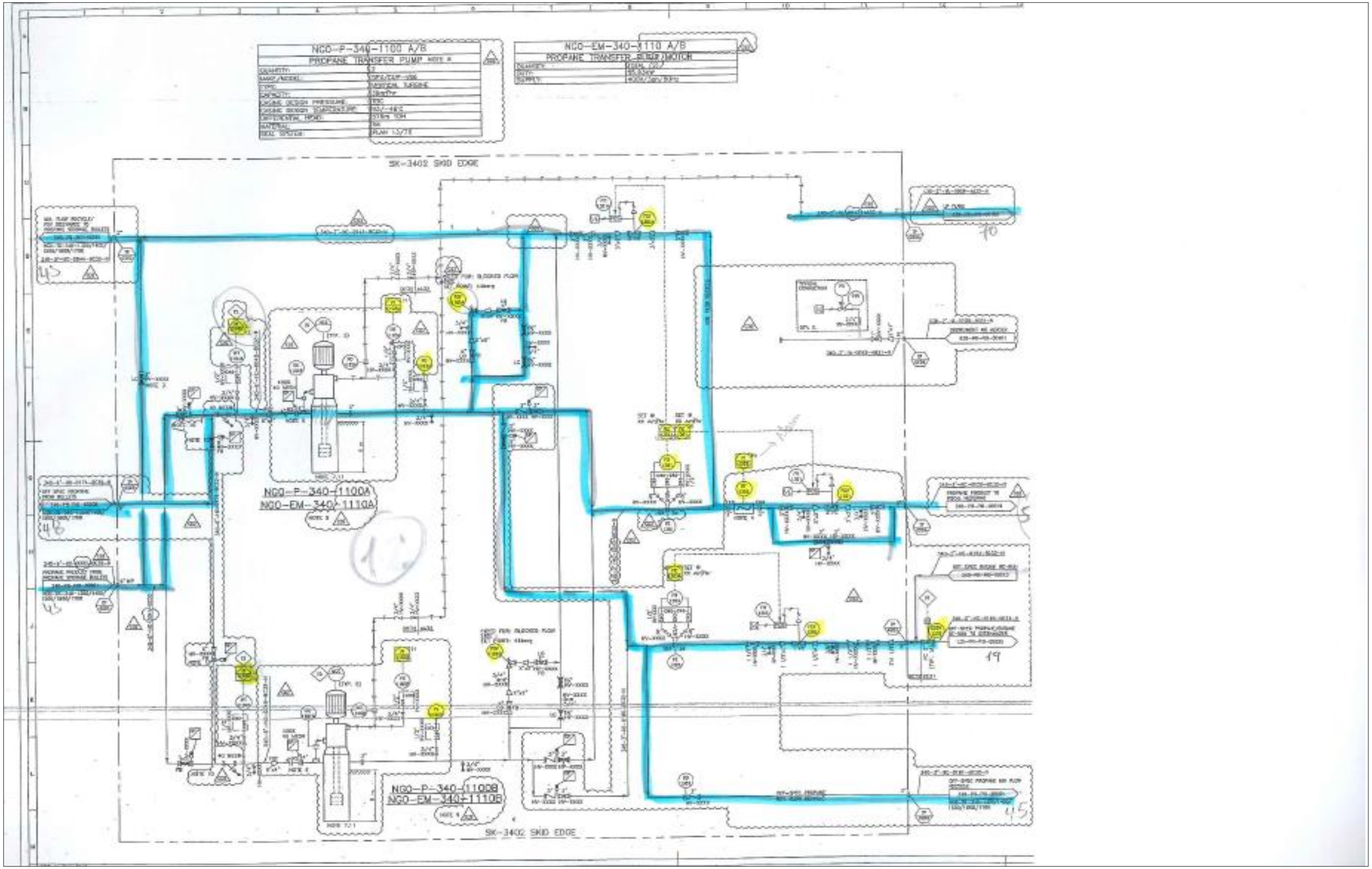

NGO-T-260-2100
DEBUTANIZER TOWER
NGO-E-260-2200
DEBUTANIZER REBOILER
SK-2603 SKID EDGE
NGO-E-260-2200
NGO-T-260-2100
34, N12
38
40

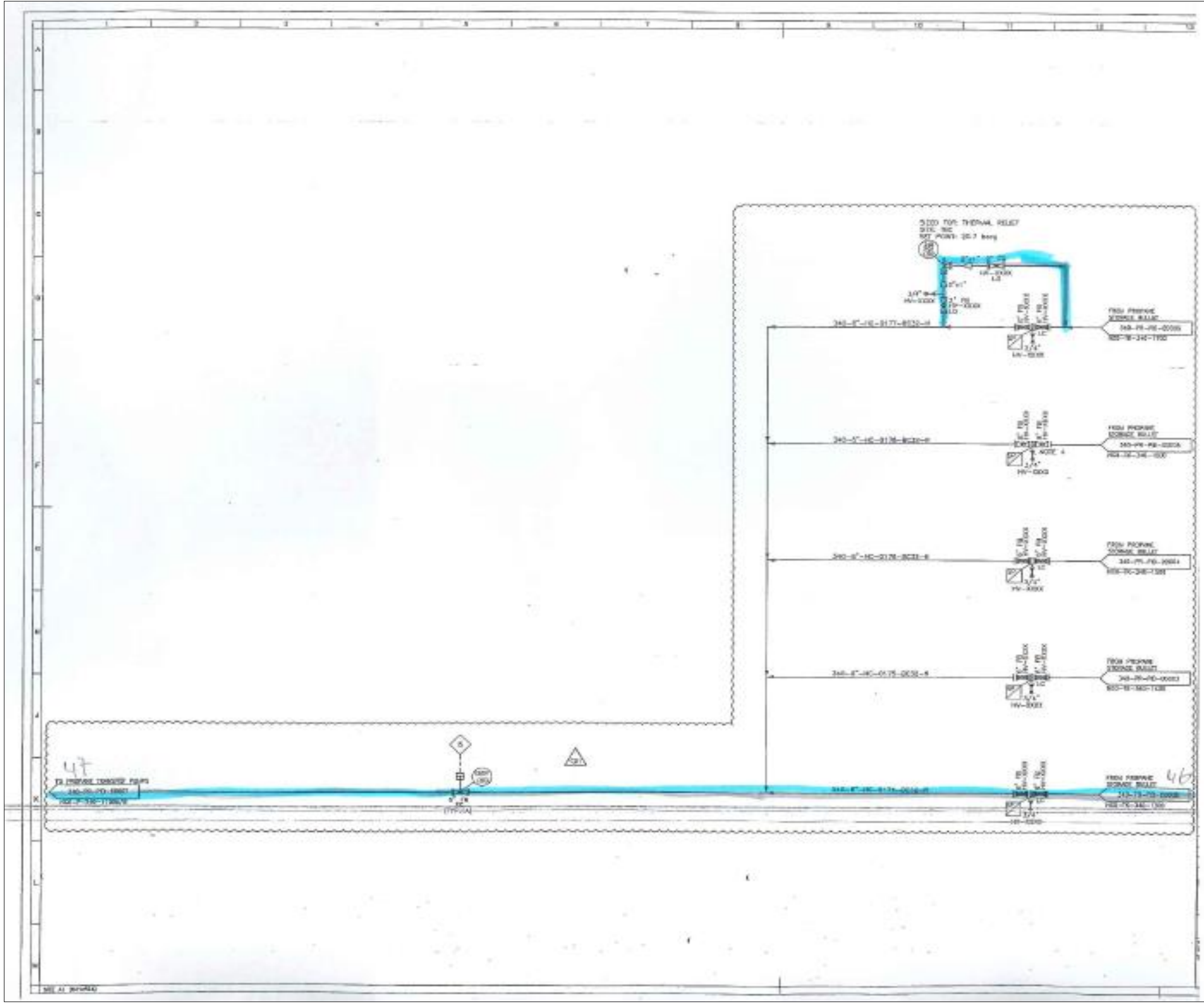

NGD-AC-260-2400
DEBUTANIZER CONDENSER
NGD-EM-260-2410/2420
DEBUTANIZER CONDENSER MOTOR
39
37
NGD-AC-260-2400
NGD-EM-260-2410
NGD-EM-260-2420
HP
39
800016

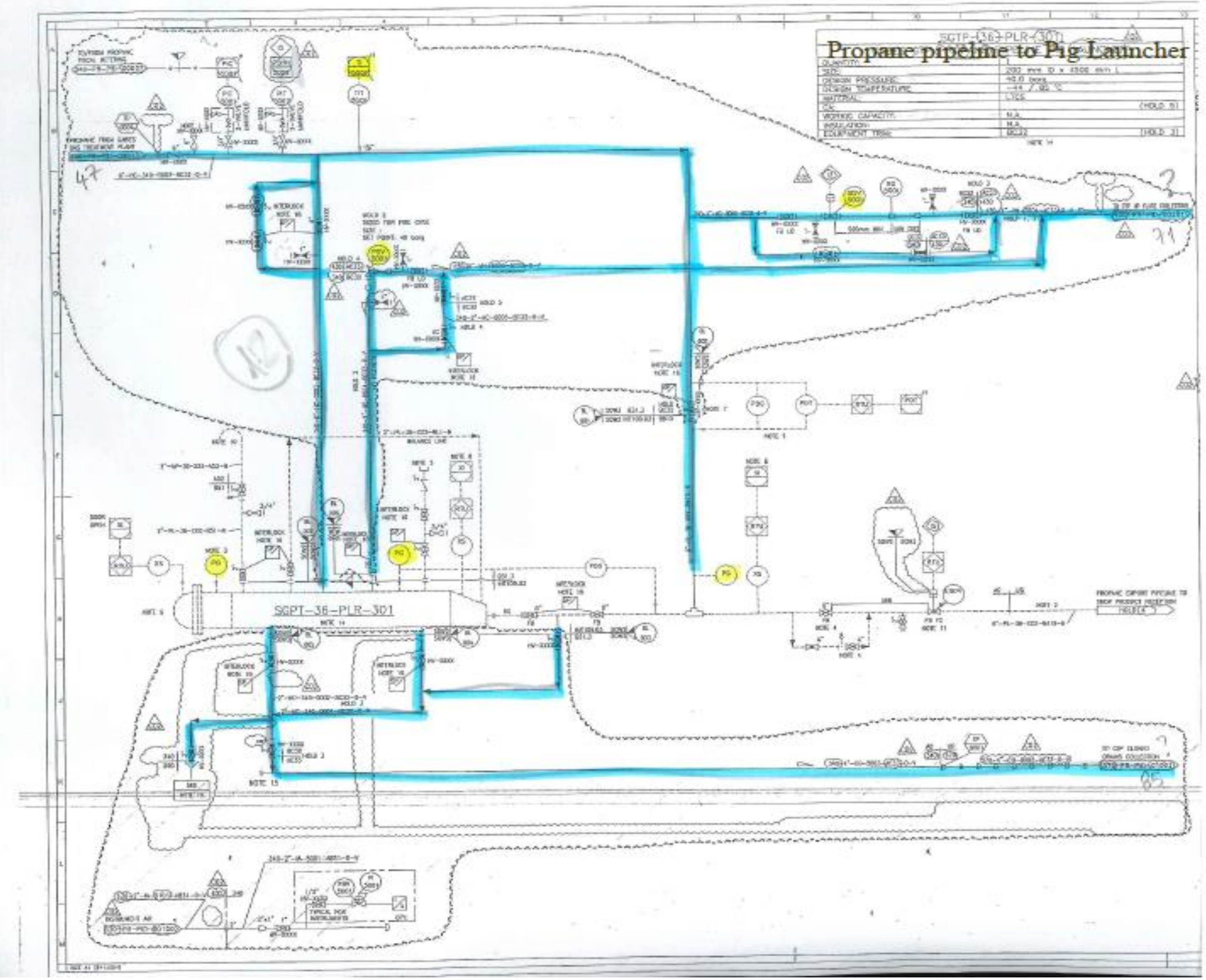

NGO-V-260-2300
DEBUTANIZER REFLUX DRUM
NGO-P-260-2500A/B
DEBUTANIZER REFLUX PUMP
NGO-EM-260-2510A/B
DEBUTANIZER REFLUX PUMP MOTOR
SK-2604 SKID EDGE
NGO-V-260-2300
NGO-P-260-2500A
NGO-EM-260-2510A
SK-2603 SKID EDGE
NGO-P-260-2500B
NGO-EM-260-2510B
71
38
36
49
37
27
85


36, N12
PROPANE PRODUCT
MIN. FLOW RECYCLE/FOR DISCHARGE FROM PROPANE BOOSTER PUMPS
47
(TYP.1F)
NOTE 4
TO PROPANE STORAGE BULLET
TO PROPANE STORAGE BULLET
TO PROPANE STORAGE BULLET
TO PROPANE STORAGE BULLET
TO PROPANE STORAGE BULLET
MIN. FLOW RECYCLE
47
FROM PROPANE STORAGE BULLET
FROM PROPANE STORAGE BULLET
FROM PROPANE STORAGE BULLET
FROM PROPANE STORAGE BULLET
FROM PROPANE STORAGE BULLET
TO PROPANE BOOSTER PUMPS
47
46


NGO-TK-340-1300
PROPANE STORAGE BULLET NOTE 12
DESIGN PRESSURE:
MATERIAL:
C.A.
WORKING CAPACITY:
HP FLARE
72
What about tail lines from other bullets.
PROPANE PRODUCT
45
79
HP FUEL GAS
NOTE 12
BALANCE LINE
4
PROPANE PRODUCT TO PROPANE TRANSFER PUMP
48
NOTE 5
NOTE 11
not combined
NOTE 14,8
NOTE 4
NGO-TK-340-1300
12


NGO-P-340-1100 A/B
PROPANE TRANSFER PUMP NOTE 8
QUANTITY:
MAKE/MODEL:
TYPE:
CAPACITY:
CASING DESIGN PRESSURE:
CASING DESIGN TEMPERATURE:
DIFFERENTIAL HEAD:
MATERIAL:
SEAL SYSTEM:
VERTICAL TURBINE
PLAN 13/75
NGO-EM-340-1110 A/B
PROPANE TRANSFER PUMP MOTOR
QUANTITY:
DUTY:
SUPPLY:
SK-3402 SKID EDGE
NGO-P-340-1100A
NGO-EM-340-1110A
NGO-P-340-1100B
NGO-EM-340-1110B
SK-3402 SKID EDGE
43
48
43
70
5
19
45
12

THERMAL RELIEF
SET POINT: 20.7 barg
FROM PROPANE STORAGE BULLET
FROM PROPANE STORAGE BULLET
FROM PROPANE STORAGE BULLET
FROM PROPANE STORAGE BULLET
FROM PROPANE STORAGE BULLET
NOTE 4
TO PROPANE TRANSFER PUMPS
47
46



Propane pipeline to Pig Launcher