Combining empirical knowledge and first principles qualitative and quantitative models in HAZOP

Part I. HAZOP Review

Wu, Jing; Lind, Morten

Publication date:
2017

Document Version
Publisher's PDF, also known as Version of record

Technical University of Denmark

Combining empirical knowledge and first principles qualitative and quantitative models in HAZOP

Part I. HAZOP Review

February, 2017

DTU Electrical Engineering
Department of Electrical Engineering

Combining empirical knowledge and first principles qualitative and quantitative models in HAZOP, Part I. HAZOP Review

Author(s):

Jing Wu, Morten Lind

Department of Electrical Engineering
Ørsteds Plads
Building 348
DK-2800 Kgs. Lyngby
Denmark

Sponsored by:

Danish Hydrocarbon Research and Technology Center (DHRTC)
Technical University of Denmark
Anker Engelunds Vej 1
2800 Kgs. Lyngby
Denmark

TABLE OF CONTENT

ACKNOWLEDGEMENTS

We would like to express our appreciation to all those who provided us the possibility to conduct this project. A special gratitude we give to Danish Hydrocarbon Research and Technology Center which funded the project.

We appreciate the cooperation among the participants through setting up discussion meetings, Prof. Emeritus Sten Bay Jørgensen DTU Chemical Engineering, Prof. Michael Havbro Faber the Department of Civil Engineering, Aalborg University, Assoc. Prof. Gürkan Sin DTU Chemical Engineering, Senior researcher Thomas Martini Jørgensen DTU Compute, Dr. Niels Jensen Safepark. Thanks to their comment and advice that have improved the quality of report. Furthermore, we would also like to acknowledge the crucial role of the project manager, Mr. Erik Bek-Pedersen, whose contribution in stimulating suggestions and encouragement and providing resources helped us to coordinate our project.

EXECUTIVE SUMMARY

Objectives of the project have been to explore the roles of empirical knowledge, qualitative models and quantitative models in HAZOP. The research bridges the gap between industrial HAZOP practice and academic HAZOP research. It gives insight on dealing with system complexity from a HAZOP study perspective.

The project reviews HAZOP where empirical knowledge, qualitative models, and quantitative models play key roles in facilitating in different tasks of HAZOP. Based on the review, an integrated qualitative and quantitative framework based on methods of Multilevel Flow Modeling, risk matrix and dynamic simulation is illustrated with an offshore three-phase separation process case study demonstrating the feasibility and applicability of the proposed framework.

The research results indicate that the challenges of HAZOP are management knowledge i.e. dealing with system complexity, uncertainty, vagueness, and requirement of completeness, and efficiency. The encoding empirical knowledge in the form of qualitative models, and quantitative models are the means to overcome those challenges. Therefore, the conclusion is to integrate these means by making use of their features to serve as a framework to prepare for HAZOP study meetings. In this way one can maximize the complementary advantages of the means and come up to better HAZOP quality.

The research can enlighten the importance of understanding system complexity for personnel in oil and gas industry and thereby gradually to change old-fashioned HAZOP industrial practice and improve safety performance in oil and gas industry. Methods in the framework and potential tools can improve HAZOP quality and efficiency with low manpower cost and help with decision making. The oil and gas industry can implement the framework for HAZOP study on real plants to test its usefulness.

The research is carried out by Jing Wu and Morten Lind in DTU Electrical Department and funded by Danish Hydrocarbon Research and Technology Center (DHRTC). Research partners in the project include Prof. Emeritus Sten Bay Jørgensen, Assoc. Prof. Gürkan Sin in DTU Chemical Engineering, Prof. Michael Havbro Faber in the Department of Civil Engineering, Aalborg University.

1 INTRODUCTION

1.1 Background

The Chinese scientist Qian [1] proposed an architecture for modern system and technology based on system science. Vertically, each subject contains three levels of knowledge: Application technology (Engineering technology) directly used for transformation of objective world; Technical science intended as theoretical and methodology foundation for application technology; Basic theory (science) for revealing the laws of the objective world. Therefore, to solve a problem of safety engineering science, it is necessary to research the three levels of knowledge, especially basic foundation research.

Although considerable development has taken place in the safety of processing industries, yet accidents do increasingly occur. Given the accident in the Gulf of Mexico (USA) in 2010 at BP-operated Macondo well and its huge political, social, economic and environmental consequences, indeed the significance of ensuring process safety cannot be emphasized more. Surely this event has already fundamentally changed the process safety practice in especially Offshore Oil and Gas industry, which will have ramifications on how process safety is managed and audited across the board[2]. This and other accidents (e.g. Fukushima nuclear disaster in the aftermath of a tsunami triggered by the Tohoku earthquake in 2011) have stressed the importance of treating safety with due consideration at all levels from academic research (e.g. safety at early stage process development) to the top of the executive management of the industries (e.g. self-commitment and provision of adequate resources for safety among others). Ensuring safety of complex systems that provides vital services to the modern society (from energy, electricity to chemicals, drugs, food and others) is a minimum requirement from societal, political and environmental points of view. Hence the development of systematic methods and techniques for ensuring safety across the life cycle of complex systems is an important challenge for the systems engineering community.

HAZOP (Hazard and Operability study) is among these systematic methods and techniques, which is dominantly embraced by oil and gas industry to identify hazards and operability problems. After several decades of its application from 1974, very little focus has been on the dimensions of system complexity dealt with in HAZOP implemented in the different stages of life cycle of a plant project. Recent accidents in advanced industrial processes and technological infrastructures also have demonstrated that system complexity is a major challenge in the management of process safety. Based on different understandings of system complexity, different system modeling methodologies has been developed. There are three understandings of complexity: physical-chemical self-organizing system complexity, system connectivity complexity and system semantic complexity represented by system goals and functions. The first two kinds of complexity have been dealt properly [3]. However, analysis of system semantic complexity requires a new modeling methodology to systematically represent system properties. Understanding the nature of system complexity and how to deal with it and manage the associated risks are the focus aspects of system designers as well as operators, and also the focus of science-based safety engineering research.

Plant design documents, operating procedures, online data are in different forms to display the system complexity. As always, these are necessary sources to carry out HAZOP. Proper integration of these sources of information and methods require the fundamental knowledge of the relations between e.g. quantitative and qualitative models and knowledge of how to combine models based on first principles, operating experience, and on-line data. The motivation of the project is exactly to try to clarify it better.

Furthermore, there is a lack of a computer-aided HAZOP- based communication tool between designers and operators in phases of designing and operation/maintenance for supporting plant-wide life cycle engineering activities to boost productivity, quality, and safety. Previously, a preliminary framework for integration of qualitative and quantitative knowledge for such tool to develop has been proposed by partners of this project. The project points out the research needs and directions for extending the framework to develop such potential tool.

1.2 Research Theme

1.2.1 What is risk management in oil and gas industry?

The Chinese word for risk, “Wei-Ji”, combines the words for “danger” and “opportunity” to describe the balance between loss and profit. The “management” of “danger” (hazards) and “opportunity” (reduced down-time) is a critical strategy to keep such balance in any industry including oil and gas industry. Therefore, the risk management in oil and gas industry can be interpreted as a dynamic process for kicking out “danger” and improving “opportunity” at some cost such as time, money and manpower to a certain safety level.

By means of techniques and methods fulfilling such strategy, a certain safety level is achieved. Normally, the certain safety level is called “as low as reasonably practicable” (ALARP) [4]. Because obviously, some “danger” in oil and gas industry is inherent, one cannot be eliminated completely. For example, the raw processing mediums are oil and gas which is flammable and cannot be replaced, however, where also lies in “opportunity”- the opportunity to have better innovative and advanced techniques to make more profit out of it more safely. It is supposed to be our striving for putting forth the new instead of sticking to established practice in old-fashions.

Technically, risk management in oil and gas industry covers all stages before and after accident occurrence, although the emphasis is a preventative risk management rather than post-accident risk management. This is also why it makes the task of risk management more difficult because it is urgent to predict what possibly can go wrong and in which way the failure can be preventive or mitigated. Specifically, risk management mainly focuses on safety in design and consequence analysis.

The objectives of safety in design are to in all industry:

1. Prevent, or minimize the likelihood of loss of containment of hazardous inventories;

2. Control the risk of ignition;

3. Control& mitigate the potential consequences of loss of containment of flammable inventories (fire, explosion, pollution etc.);

4. Control the risks from non-hydrocarbon events e.g. structural failure, dropped objects, helicopter crash, ship collision, vehicle impact, etc.;

5. Limit escalations;

6. Ensure that means of escape and evacuation are in place and that adequate emergency response facilities will be provided.

To meet such objectives, prevention, detection, control and protection techniques and methods are adopted. Among them, Process Safety Review [5-6] is needed, where also HAZOP technique arises. Consequence analysis [7] is to identify magnitude such as a release scenario in order to design of safety systems and input it into risk assessment, where also involves the use of models to predict the effect of a particular event of concern. The technique of Quantified Risk Assessment (QRA) [8] was originated from.

However, if the protection layers[9] of preventing, detect, control and mitigate all fail (See in Figure 1), an accident investigation is applied to find out what has gone wrong and why, and take action to reinforce weak controls to prevent reoccurrence.

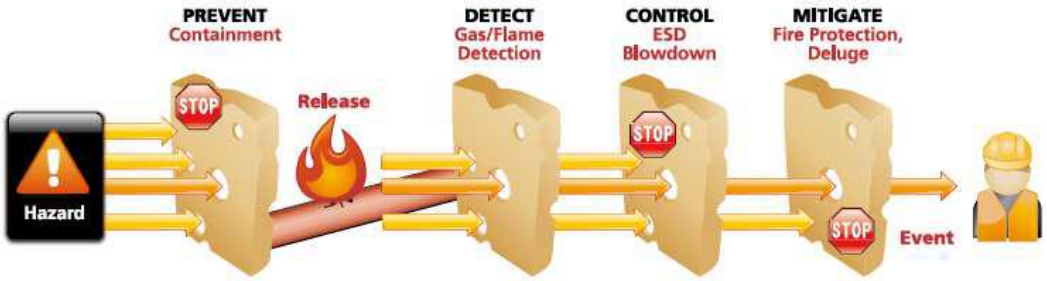


Figure 1. Application of the “Swiss cheese” model

In summary, risk management in oil and gas industry deals with what goes wrong, why goes wrong, and in which way we can control it. However, to achieve this, it is necessary to acquire associated knowledge and modeling of the system to represent a real world to analyze.

1.2.2 What are empirical knowledge and first principle qualitative and quantitative models?

To perform a HAZOP study, empirical data and knowledge of the system and its operation is required including and how deviations from design intents of a system may cause hazards and operability problems. An advantage of empirical techniques is a certain independence of detailed knowledge of plant behaviour. However, a disadvantage of the empirical approach is that risk scenarios are defined by patterns of observed plant variables values or historical accident data. It may accordingly be difficult to identify hazards which have not been encountered before. A significant problem with empirical methods is that hazards are defined by expert judgments i.e. there is no systematic basis for defining hazards and thereby to ensure completeness or consistency of the analysis. Expert judgment on the possibility of causes, the severity of consequences and risk criteria come from empirical sense as well.

According to Venkatasubramanian[10], model-based approaches used in engineering (Figure 2) can be classified into qualitative and quantitative. However, such classification of model-based approaches is problematic. For example, causal models can be qualitative or quantitative. Qualitative models and qualitative reasoning are the abstraction of the system's behaviour in qualitative numerical description. The causality between variables is a qualitative relation between states or events. For example, the high outlet flowrate from a water container causes low level of the water in container. The qualitative reasoning uses the causual relation to make infererences from evidences. If a quantitative simulation data can generate a quantitative causal relation between variables, such as the outlet flowrate and level and represented in a quantitative differential equation, then the model becomes a quantitative model and the reasoning accordingly is quantitative.

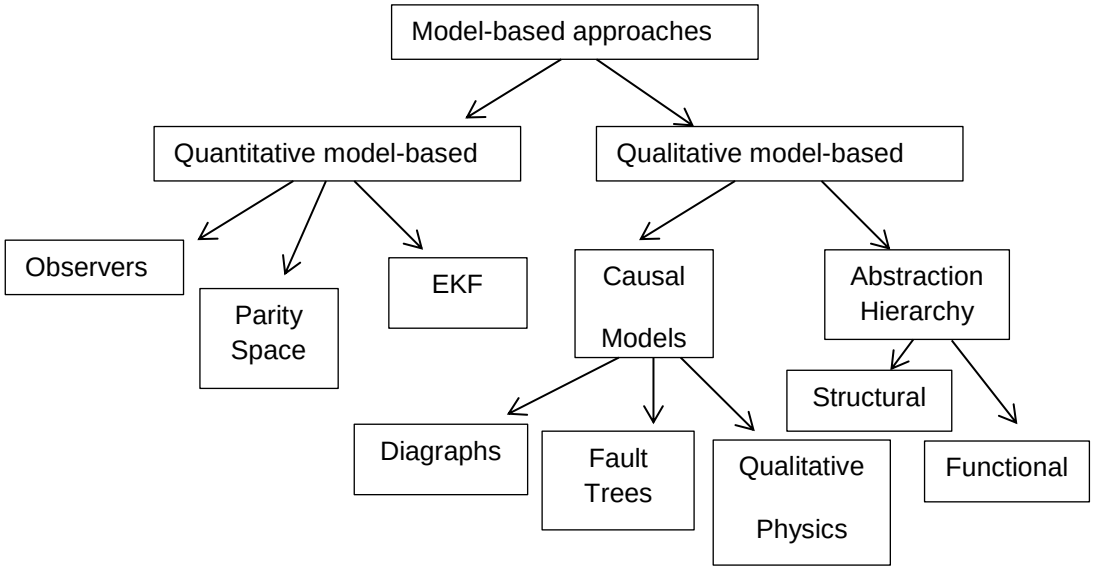


Figure 2. Classification of model-based approaches by Venkatasubramanian [11]

We find out the classification proposed by Venkatasubramanian is not adequate because it confuses several aspects which should be separated. We believe that the distinctions between qualitative models from quantitative models involve two dimensions: Classifications and scales. Classifications define the concepts used to build the model. For example, outlets and containments are classifications. Scales is about measurement of values (e.g. flowrate and level). Scales [12] are categorized into four groups: nominal, ordinal, interval, and ratio. Nominal scale is classification, ordinal scale allows for ranking order. Interval scale allow for the degree of difference between items, but not the ratio between them and ratio scale is the estimation of the ratio between a magnitude of a continuous quantity and a unit magnitude of the same kind. The nominal scale and ordinal scale are qualitative, in contrast, Interval scale and ratio scale are quantitative. We believe that one should have a qualitative model of the system, and then with the increasing scale, the quantitative models are obtained. In another word, quantitative models (e.g. differential and algebraic equations, DAEs) [13] can be developed from knowledge of physical, chemical, and biological mechanisms (i.e., first engineering principles modeling or mechanistic modeling) which are convenient for detailed calculations but require a large amount of

background data which often is quantitative but are not available.

Qualitative models and associated methods [14] based on logical inference is under development for safety and risk analysis and can with advantage be combined with quantitative methods. Functional modeling (FM) [15] can be considered as a type of first principles model as well as a qualitative method. But the first principles are not given by laws of nature, but by necessary logical constraints between deviations, goals, tasks and plant functions and execution of actions. These first principles reflect conditions for successful action can be called *first principles of operation* [16]. Therefore, first principles include first engineering principles and first operational principles. First engineering principles are principles based on the knowledge of how to use physical, chemical, and biological laws in design. And, first operational principles are actions following the action sequences to achieve a target. From another point of view, FM is a representation of combined intent model and causal model. FM represents the objectives/goals of a system as well as the causal relations between functions.

1.2.3 Why and how the qualitative and quantitative models are combined?

No single model can capture all the system aspects which are important for prediction of threats and evaluation of risks. Qualitative models are suitable for studies on the level of the whole system including its purpose orientation where quantitative models fail. Conversely, quantitative models are suitable for studies of the detailed behaviour of subsystems where qualitative models are not adequate. Hybrid modeling comprising qualitative and quantitative methods for safety assessment is, therefore, necessary.

Specifically, obtaining the necessary information to formulate a quantitative model with required fidelity may be difficult, in particular without a well-developed understanding and accurate knowledge about the system and its internal processes. When fundamental theories and mathematical equations are not available, empirical equations can be developed to fit a hypothetical mathematical model, but such a possibility requires the availability of measurements, that is, a data-driven modeling approach. However, for safety critical systems, the data-driven methods may not be applicable due to the low accident occurrence rate of safety critical situations. There may not be enough accident event data to be obtained from plant operation. Accordingly, empirical data are insufficient to enable proper modeling and validation for this specific purpose. Hence at the moment, the available computer-aided tools [17-18] are mostly used for simulations and analysis of failure scenarios as a means to support training and education in safety critical systems.

However, a quantitative model does not contain an explicit representation of (sub-) system intention and purpose. To achieve the purpose of preventing or mitigating significant hazards, good hazard identification practices are, therefore, highly dependent on understanding the qualitative nature of the system. Quantitative methods can therefore with advantage be combined analyses based on qualitative models, which are effective for global analyses and require less background data. System models must represent system features and capture system knowledge about design intention.

1.3 Research Contribution

The purpose of the report is to survey existing HAZOP methods as well as formulating the scientific

challenges in HAZOP studies in the life cycle of a system, e.g. an oil and gas plant and possible methods based on empirical knowledge, qualitative models and quantitative models to deal with them. The results of the report will provide a theoretical baseline for the DHRTC Water Management project. The main research contributions include:

1. The advantages and disadvantages relevant of existing HAZOP method and those disadvantages can be dealt with by an integrated qualitative and quantitative model-based framework.

2. Challenges faced by HAZOP, especially in management of system complexity are identified.

3. Computer-aided methods for HAZOP based on empirical knowledge, qualitative models, and quantitative models are reviewed.

4. A principle or procedure for using the qualitative and quantitative models could be used during the life cycle of a HAZOP.

5. Future work to advance in modelling techniques, consistency of analysis, and reasoning capacities to produce a better quality of HAZOPs is summarized.

1.4 Report structure

The major contents of the report are summarized in Figure 3. It includes two parts: 1) HAZOP literature review and 2) An integrated qualitative and quantitative HAZOP framework. Part I (highlighted by green colour) can be viewed as a theoretical foundation for an integrated qualitative and quantitative HAZOP framework proposed in Part II. Part II (highlighted by yellow colour) is to elaborately how qualitative models and quantitative models play their roles in HAZOP study.

In part I, firstly, a comprehensive Process Hazard Analysis (PHA) and associated techniques review in oil and gas industry is given. Then the HAZOP is selected as one of representative PHA technique is introduced in details in terms of its method, procedures, pros and cons. In order to differentiate the HAZOP industrial practice and fundamental research interest in computer-aided methods, the emphasis is made on its implementation in plant-wide life cycle engineering and challenges and methods based on qualitative models and quantitative models for dealing with those challenges in aspects of knowledge management of system complexity, uncertainty, vagueness, completeness and efficiency, respectively.

In part II, the complementary strengths of qualitative and quantitative models are analysed, a summary of a proposed integrated qualitative and quantitative HAZOP framework is illustrated with a case study of HAZOP for an offshore three-phase separation production process. Finally a to-do list for developing a potential tool called “MFM-HAZOP” is presented.

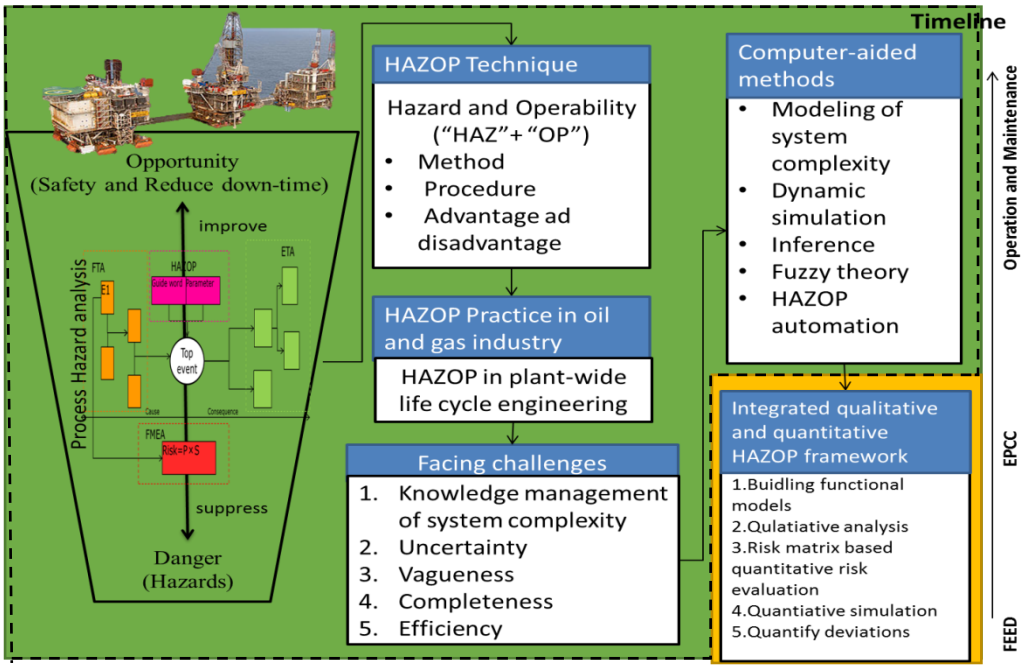


Figure 3. Report contents overview

2 MOTIVATIONS

The purpose of part I is to explore the roles of empirical knowledge, qualitative models and quantitative models in HAZOP by doing literature review mostly regarding the challenges faced by HAZOP and computer-aided methods based on empirical knowledge, qualitative models and quantitative models aiming at dealing with those challenges. The process hazard analysis methods, HAZOP technique and its industrial practice in a life cycle of a plant project are introduced as well in order to serve better understanding basis for readers who are not much familiar with HAZOP. The context of HAZOP implementation is allocated in oil and gas industry. However, HAZOP method itself is generic, so the explored results are fit into varieties of the process industry. Part I can be viewed as a theoretical foundation for the integrated qualitative and quantitative HAZOP framework proposed in Part II.

3 PROCESS HAZARD ANALYSIS (PHA) IN OIL AND GAS INDUSTRY

3.1 Risk background in oil and gas industry

The Oil and Gas industry includes the processes of exploration, extraction, refining, transporting (often by oil tankers and pipelines), and marketing oil and gas products. It dates back into 19th century. However, the exploitation of oil and natural gas in Northern Europe is a comparatively new activity which is important for economy development. For example, the first oil production in Denmark began in 1972 from the Dan Field. However, with the passage of time, aging fields increases the risk of production downtime. Besides upstream production, the hazardous operation of downstream production and services should not be ignored. Their operation should also pay attention to achieving continuing future production safely.

Also, flammable hydrocarbons are handled in large quantities in oil and gas industry which makes the risk is inherently threatening employees who have their workplace on an offshore platform or in onshore installations. Accidents occur continuingly, such as the Macondo explosion and fire in the Gulf of Mexico leading to eleven dead, the sinking of the drilling rig and over a period of three months the release of more than 4 million barrels of oil into the Gulf of Mexico[19]. According to safety performance indicators-2015 data [20] (Figure 4), the overall fatal accident rate (FAR) of 2015 is even 41% relative higher than that of 2014, especially FAR in offshore is more than that in onshore. The OGP statistics show that there is still a long way to go before the safety performance keeps in good profile in oil and gas industry.

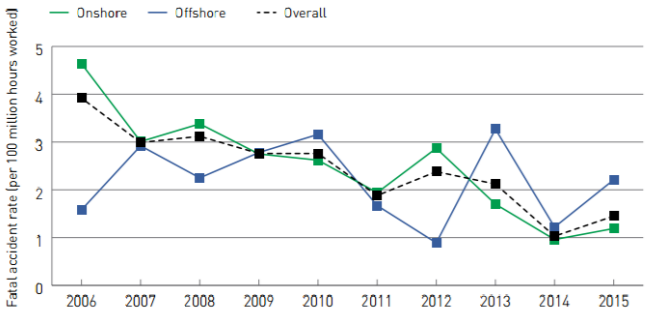


Figure 4. Fatal accident rate by onshore & offshore operations (2006–2015) [2]

In order to control risk in oil and gas industry, the authorities [21] (Danish Energy Agency, Petroleum Safety Authority Norway etc.) and insurance companies require and monitor operating companies to carry out hazard identification and risk assessment during a facility design, as well as prior to construction and how often during operation using a lifecycle approach to safety. Studies by regulatory bodies indicate that the dominant factors in system failures are in the specification (44.1%), changes

after commissioning (20.6%), operations and maintenance (14.7%), installation & commissioning (5.9%), and design and implementation (14.7%)[22], see in Figure 5. The authorities require that the Process Hazard Analysis (PHA) studies be recorded and acted-upon and that they are subject to management audit and approval. For example, Safety Reports are required for major accident installations in compliance with the European Seveso Directive III. The Major Accident Hazard Identification and Evaluation must be covered in the Safety Reports [23].

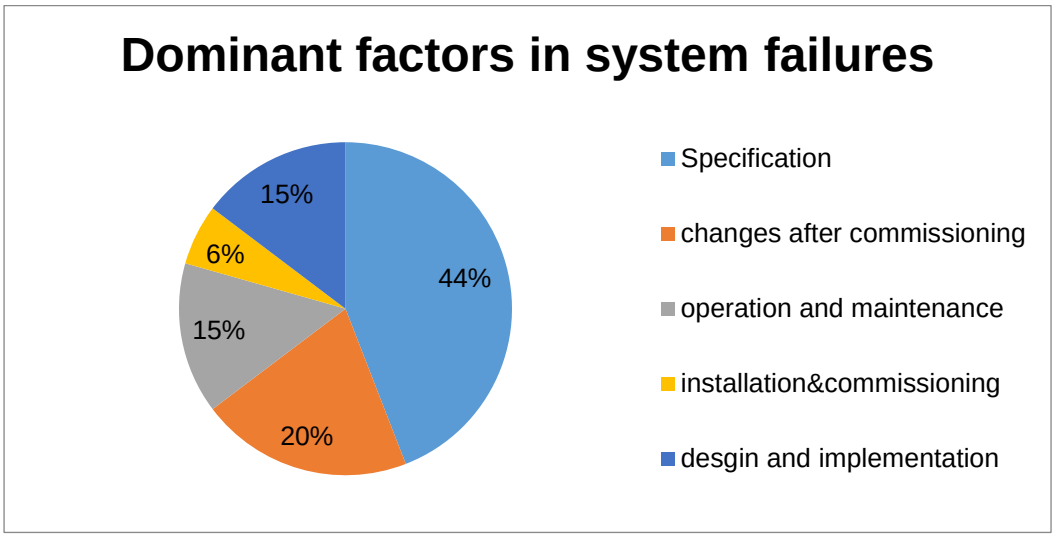


Figure 5. Dominant factors in system failures

3.2 PHA techniques

To meet the above demands, comprehensive hazard identification is the cornerstone of effective risk management since if a hazard has not been identified then measures cannot be put in place to mitigate the risk. However, where do the hazards originate?

An early attempt by Haddon to define a system-oriented taxonomy of hazards [24] was based on an exclusive classification of forms of energy that could be harmful to people. However, it was argued that such an approach for categorizing hazards was not easily recognized and applicable to solving problems so it is difficult to identify hazards, and let alone put forward the protective measures for controlling them. Given this, the categories of hazard sources were more pragmatically proposed by Rasmussen [25], that is, energy accumulations, accumulation of toxic substances, structural integrity and stability, and the mixed. Hazards in the form of energy accumulations typically can be monitored by measurements of process variables, such as flow rate, temperature, or pressure. Hazards in form of accumulation of toxic substances are released by the critical event 'loss of containment' of toxic material, leading to release of toxic fumes, a leak of chemicals. Structural integrity and stability are conditionally dependent on the ability of a structure to support a designed load. The mixed hazards include the damage from interaction with sharp edges, rotating machinery, bad weather, which needs to be derived from epidemiological analysis of accident reports by regulators and communicated to users by means of standards and guidelines.

After knowing the taxonomy of hazards, it needs an action to analyze each hazard type. Process Hazard Analysis (PHA) is a tool commonly used in the process industry, such as oil and gas, to

describe the tasks of identification of hazards and the evaluation of risks as well. It consists of two stages: hazard identification and risk assessment. Hazard analysis is a more generic term to cover the two stages', whose results are to provide actions so as to prevent accidents.

Hazard analysis can be divided into two categories: qualitative analysis and quantitative analysis. The qualitative analysis aims to identify the existing hazard factors, identify the risk scenarios and their effects on system safety, and finally to propose the safety functions to control the risk. Based on the results of a qualitative analysis, a quantitative analysis can be carried out to evaluate the risk for cases where the qualitative analysis indicates unacceptable uncertainty, based on the quantitative relations between the cause and effect leading to the quantitative results indicated by process parameters, safety, and reliability data. A summary of hazard identification techniques are found in[26,27], which include approaches such as Preliminary Process Hazard Analysis(PrHA), Fault Tree Analysis (FTA), Event Tree Analysis(ETA),Failure Mode and Effects Analysis/Failure Mode and Effects Critical Analysis (FMEA/FMECA) ,What-If Analysis, Checklists, Hazard and Operability Studies(HAZOP), Functional Hazard Assessment(FHA)[28].

In this section, the report is reviewing the above methods for hazard analysis based on events leading to hazards driven by a failure of functions, components, and parameters (See in Table 1). An outcome of the review is to illustrate whether the techniques are suitable to be applied in a safety lifecycle [29]. Figure 6 also represents the relations among methods of HAZOP, FTA, ETA, and FMEA. By using HAZOP, the top event of a scenario can be identified. If the top event is propagated to upstream, FTA is used to identify the causes. If the top event is viewed as the initial event in ETA, then it can be propagated to downstream to examine the consequences. If a bottom event (E1) represents the failure of equipment, then FMEA can be adopted to analyze the risk of the event by considering the combination of P (probability) and S(severity), see in Figure 6. More comparison of PHA techniques and supplements with each other can be read in references [30-32].

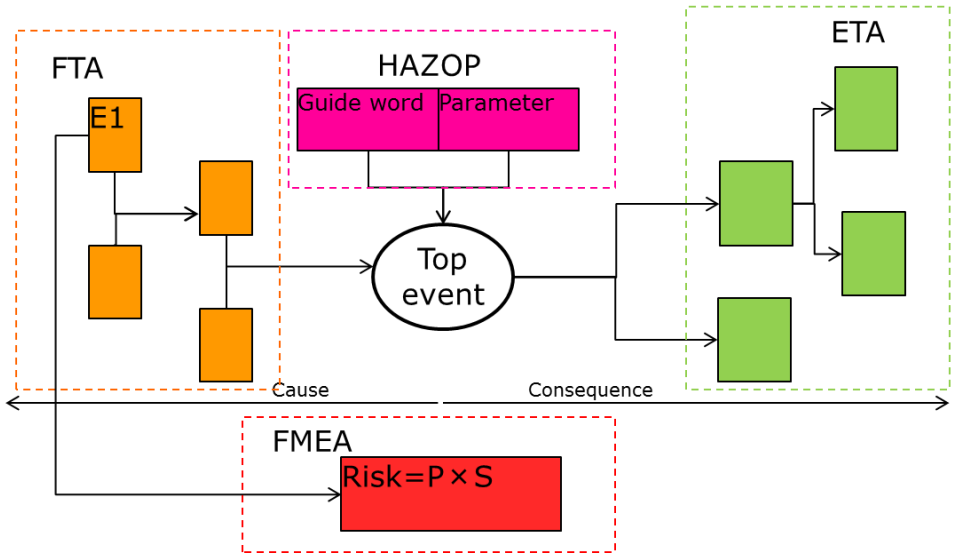


Figure 6. Relations of PHA methods

Table 1. Summary of hazard identification techniques based on Wells' book

Driven by failure types	Name of techniques	Procedures	Scale of techniques		When to use
			Qualitative	quantitative	
Event	PrHA	Define and describe the system to be analyzed, collect risk information from previous and similar systems (e.g.from accident data bases), to identify all possible hazards and events , rank the identified accidental events according to their risk(consequence and frequency estimation), identify required hazard controls and follow-up actions. All the results are filled in a PHA worksheet.	√		New designs at the conceptual stage in order to assist with layouts, etc. and for existing facilities where some level of prioritization is needed prior to more detailed hazards analysis, e.g., HAZOPs
	What-if Analysis	Simply a brainstorming technique that asks a variety of questions related to situations that can occur. An analysis of this situation then follows. The answer should provide a description of the resulting consequence. Recommendations then follow, if required, on the measures taken to prevent an accident.	√		The what-if analysis approach is useful throughout the entire lifecycle of a process and is frequently used in conjunction with the checklist approach.
	Checklist	By taking the applicable standards and practices and	√		The Checklist approach is useful throughout the entire lifecycle of a process

		using them to generate a list of questions that seek to identify any differences or deficiencies. If a checklist for a process does not exist, an experienced person must develop one based on standards, practices, and facility or equipment experience.			
	FTA	By top-down strategy, to select a particular failure of event, using Boolean logic to combine a series of lower-level events to generate a tree-alike failure paths of the selected event	√		Detailed design, operation, modification, decommissioning
	ETA	Define the system, identify the accident scenarios, identify the initiating events, build the event tree diagram, obtain event failure probabilities, identify the outcome risk, evaluate the outcome risk, recommend corrective action, document the ETA		√	Detailed design, operation, modification, decommissioning
Function	FHA	From a suitable representation, select functions in turn, define purpose and behavior of function, consider hypothetical failure modes, determine effects, determine	√		All stages of a life-cycle of a system. Ref. to the Aerospace Recommended Practice - ARP 4754 [SAE94]

		and record associatd risk factors(i.e.severity and probability budget) and fill in a FHA record.			
Component	FMEA	Select system or component and split into subsystems or subcomponents, and postulate a failure mode of the subsystem or subcomponent, list the effects of the failure, safeguards or controls and recommended remedial actions are following.	√		Analyzing specific systems or items of equipment that are best handled as objects rather than by the use of parameters or operations. A new cycle begins (new product/process);Changes are made to the operating conditions; A change is made in the design; New regulations are instituted; Customer feedback indicates a problem
	FMECA	FMECA extends FMEA by including a criticality analysis, which is used to chart the probability of failure modes against the severity of their consequences	√	√	The same as above
Parameter /Operations	HAZOP	The system is divided into “nodes”, and “guide-words” combined with “parameters”(called as “deviation”) are applied to examine possible causes and consequences for each deviation in each ”node”, to consider safeguards and recommendation for action.	√		Conceptual design, detailed design, approved for construction, ‘as-built’, proposed modifications, regulatory requirements.

Among the PHA techniques, HAZOP has been well-accepted by oil and gas industry. The HAZOP method originated in the chemical industry and has been extended to various industries for carrying out a hazard analysis. For different problem-solving purposes, HAZOP is classified into Process HAZOP, Human HAZOP, Social HAZOP, Procedure HAZOP and Software HAZOP.

1. A Process HAZOP represents a conventional or classical HAZOP which is original to assess plants and process systems [33]. This is quite a common type that is being practiced in oil and gas industries.

2. A Human HAZOP is a group of specialized HAZOPs with more focus on human errors than on technical failures. In order to systematically identify human errors factors by borrowing the basic principles of HAZOP, it is based on the changing guide words themselves (some by changing the interpretation of guide words) and changing parameters/operations into different descriptions of human actions. Those changed guide words together with human actions are deviation of human actions, which categorized into different human error types such as psychological errors, cognitive errors, violation errors[34-35].In general, Human HAZOP studies identify the potential for human failures during safety critical operating or maintenance activities and make recommendations to optimize the factors influencing human performance. Usually, it is conducted only on violations of work permits or report of a bulk of near-miss events. A practical application of Human HAZOP can be found in [36].

3. Social HAZOP: If the wrong human actions are more concerned with broader ranges including organization management activities as well, it is called as Social HAZOP [37].

4. A Procedure HAZOP is the review of procedures or operational sequences. Such HAZOP involves a step by step review of the procedure with consideration given to the sequencing, delay, or missing of steps involved in the procedure [38]. An example is given for HAZOP on start-up/shut down procedure and the guidelines, procedures, and templates that are necessary to perform this HAZOP is studied [39]. Procedure HAZOP is usually carried out while a major deviation in the process line is proposed.

5. A Software HAZOP identifies possible errors in the development of software [40]. It is modified form of HAZOP to characterize likely failure modes of software components. It may also be called as SHARD (Software Hazard Analysis and Resolution in Design) [41]. Reference [39] pointed out the special benefit of HAZOP for software analysis which is identifying the interaction effects between the software, its computer environment and the real world in which it is used. A review of the HAZOP method and specific experience related to software assessment can be found in [40]. This is useful to analyze the hazards that may arise from the failure of automated control systems. It is essential for all electric and electronic control systems. It is often practiced in oil and gas industries.

The present report is concerned with a survey of Process HAZOP in the context of oil and gas industry, especially in offshore. Because offshore oil and gas process operations undergo frequent HAZOP analysis. However, the approaches for Process HAZOP in other industries, mainly in the chemical industry are also reviewed so that it can reflect inspirations and the lessons learned from other industries. Hydrocarbon processing mainly is a continuous process, so Process HAZOP for continuous process rather than for batch process is our concern. Because plant operators generally play a larger part in batch operations, more consideration has to be given to human operator reliability.

4 HAZOP TECHNIQUE

4.1 HAZOP method

In the 1960s, an improved form of what-if analysis emerged within Imperial Chemical Industries (ICI), and its application first became known as operability and hazard studies. Later, to emphasize the importance of process safety, the name HAZOP (HAZard and OPerability) was coined. HAZOP study is a well-accepted and worthy method [42] for hazard identification of process designs and for planned modifications, which initially was developed for analyzing chemical process hazards [43]. The training of HAZOP is also continuously in education and industry [44] and lessons were learnt [45]. It greatly accelerated after the methyl isocyanate (MIC) release in Bhopal, India, in 1984. A large release of hydrogen fluoride from a Texas City, Texas, refinery in 1987 prompted the oil and gas industry to embrace HAZOP studies.

The approach is a structured brainstorming using guidewords and is performed by a multidisciplinary team during a set of meetings to derive the records of causes and consequences of deviations [46]. An effective HAZOP ensures that all potential deviations from design intentions are identified and process hazards are revealed. Based on the brainstorming sessions, mitigating actions can be planned against unacceptable process consequences or actions for improvement of the system safety integrity level. It is important that records of the brainstorming sessions and documentation of planned actions are available for review by management and authorities [47].

For those are interested in details of HAZOP can find in most recent guidelines, such as Guidelines for Hazard Evaluation Procedures, IEC61882:2016 Hazard and operability studies (HAZOP studies)-Application Guide, ISO 17776.Guidelines on tools and techniques for hazard identification and risk assessment [48-50], etc. In oil and gas industry, HAZOP study team members should also be familiar with some technical standards extensively applied, such as API RP 14C Recommend Practice for Analysis, Design, Installation and Testing of Basic Surface Safe Systems for Offshore Production Platforms, API RP 520 Sizing, Selection and Installation of Pressure-Relieving Devices in refineries, API RP 521 Guide for Pressure-Relieving and Depressuring Systems, ISO 10418 Petroleum and natural gas industries-analysis, design, installation and testing of basic surface process safety systems on offshore production, installations-Requirements and guidelines, IEC 61508/61511 Functional safety of electrical/electronic/programmable electronic safety-related systems, etc.

Typical concepts in HAZOP are listed in Table2. HAZOP Guide words and meanings are in Table 3. These guide words are applicable to both the more general parameters (e.g. react, transfer) and to the more specific parameters (e.g. pressure, temperature, flow). With the general parameters, meaningful deviations are usually generated for each guide word. Moreover, it is not unusual to have more than one deviation from the application of one guide word. For example, "more reaction" could mean either that a reaction takes place at a faster rate, or that a greater quantity of product results. With the specific parameters, some modification of the guide words may be necessary.

In addition, it is not unusual to find that some potential deviations are eliminated by physical limitation. For example, if the design intention of a pressure or temperature is being considered, the guide words “more” or "less" may be the only possibilities.

Finally, when dealing with a design intention involving a complex set of interrelated plant parameters (e.g., temperatures, reaction rates, composition, or pressure), it may be better to apply the whole sequence of guide words to each parameter individually than to apply each guide word across all of the parameters as a group. Also, when applying the guide words to a sentence it may be more useful to apply the sequence of guide words to each word or phrase separately, starting with the key part which describes the activity (usually the verbs or adverbs). These parts of the sentence usually are related to some impact on the process parameters.

Table 2. Typical concepts in HAZOP

Term	Definition
Hazard	A source or situation(event, circumstance or condition)with the potential to harm, including ill health, injury or death, damage to property, plants, product or the environment, production losses for increased liabilities.
Operability	The ability to keep equipment, a system or a whole industrial installation in a safe and reliable functioning condition, according to pre-defined operational requirements
Design intention	Definition of how the plant is expected to operate and the range of operating conditions.
Nodes	Section of equipment with definite boundaries within which process parameters are investigated for deviation.
Guide words	Simple words that are used to quantify the design intention and to guide and stimulate the brainstorming process for identifying process hazards
Process parameter	Physical or chemical property associated with the process. Includes general terms such as reaction, mixing, concentration, PH and specific items such as temperature, pressure, phase and flow.
Deviations	Departures from the design intention that are discovered by systematically applying the guide words to process parameters for each process section.
Causes	Reasons why deviations might occur. Once a deviation has been shown to have a credible cause, it can be treated as a meaningful deviation.
Consequences	Results of deviations. Normally, the team assumes active protection systems fail to work
Safeguards(Protection)	Engineered systems or administrative controls designed to prevent the causes or mitigate the consequences of deviations.
Actions(or Recommendation)	Suggestion for design changes, procedural changes, or areas for further study.

Table 3. HAZOP Guide words and meanings

Guide words	Meanings
No	Negation of the design intent
Less	Quantitative decrease
More	Quantitative increase
Part of	Only a part of the intention is achieved
As well as	Impurities present, simultaneous execution of another operation/step
Reverse	Logical opposite of the intent
Other than	Complete substitution

4.2 HAZOP procedures

The most important thing in preparing for a Hazop study is to define the purpose, objectives, and scope of the study. The more precisely this is done, the more focused and relevant the committee discussions can be. The next step is to collect all relevant information on the process under consideration. This includes flow diagrams, process equipment specifications, nominal flows, etc as noted previously. The procedure is highly dependent on the reliability of this information. Efforts expended here are worthwhile. Many committees use the flow sheet as the central structure to organize their discussions.

The Hazop procedure is illustrated as follows, see in Figure 7:

(1) Prior to the commencement of a HAZOP study, the process plant or the portion identified for the study is to be divided into “nodes.” A node is i.e. vessel, line.

Nodes are small, manageable and logical portions into which the process is divided. Consider the following guidelines for the identification/selection of nodes on a P&ID:

Input streams to the equipment

Output streams from the equipment

Utility connections to/from the equipment

Vent lines, drain lines, overflow lines

Equipment, such as a reactor, tank, heat exchanger, dryer, centrifuge, etc.

Each node from each input/output stream should be marked in the P&ID, preferably with different color codes. These nodes are normally identified by a HAZOP study team leader, with assistance from the process engineer, well before the HAZOP study session. If time does not permit, this identification exercise can be done at the beginning of the first HAZOP study session. Long nodes running into two or more P&IDs, consisting of a number of lines and equipment within the same node, are sometimes identified by team leaders. This should be avoided, as a HAZOP study is likely to miss some probable causes and consequences, decreasing the study's overall effectiveness.

(2) The node's design intention, i.e. flow, cooling, etc., is described

(3) A process parameter such as temperature, pressure, pH, component, viscosity, etc., is chosen

(4) A guide word to determine a possible deviation is applied. One purpose of the guide words is to ensure that all relevant deviations of process parameters are evaluated. Sometimes, teams consider a fairly large number of deviations (i.e. up to 10 – 20) for each section or step and identify their potential causes and consequences. Normally, all of the deviations for a given section or step are analyzed before proceeding further.

(5) If the deviation is applicable, the possible causes should be determined and any protective systems noted

(6)The consequences of the deviation should be evaluated

(7) Specific action should be recommended when spelling out what, when, and by whom

(8) All information should be recorded on HAZOP worksheets.

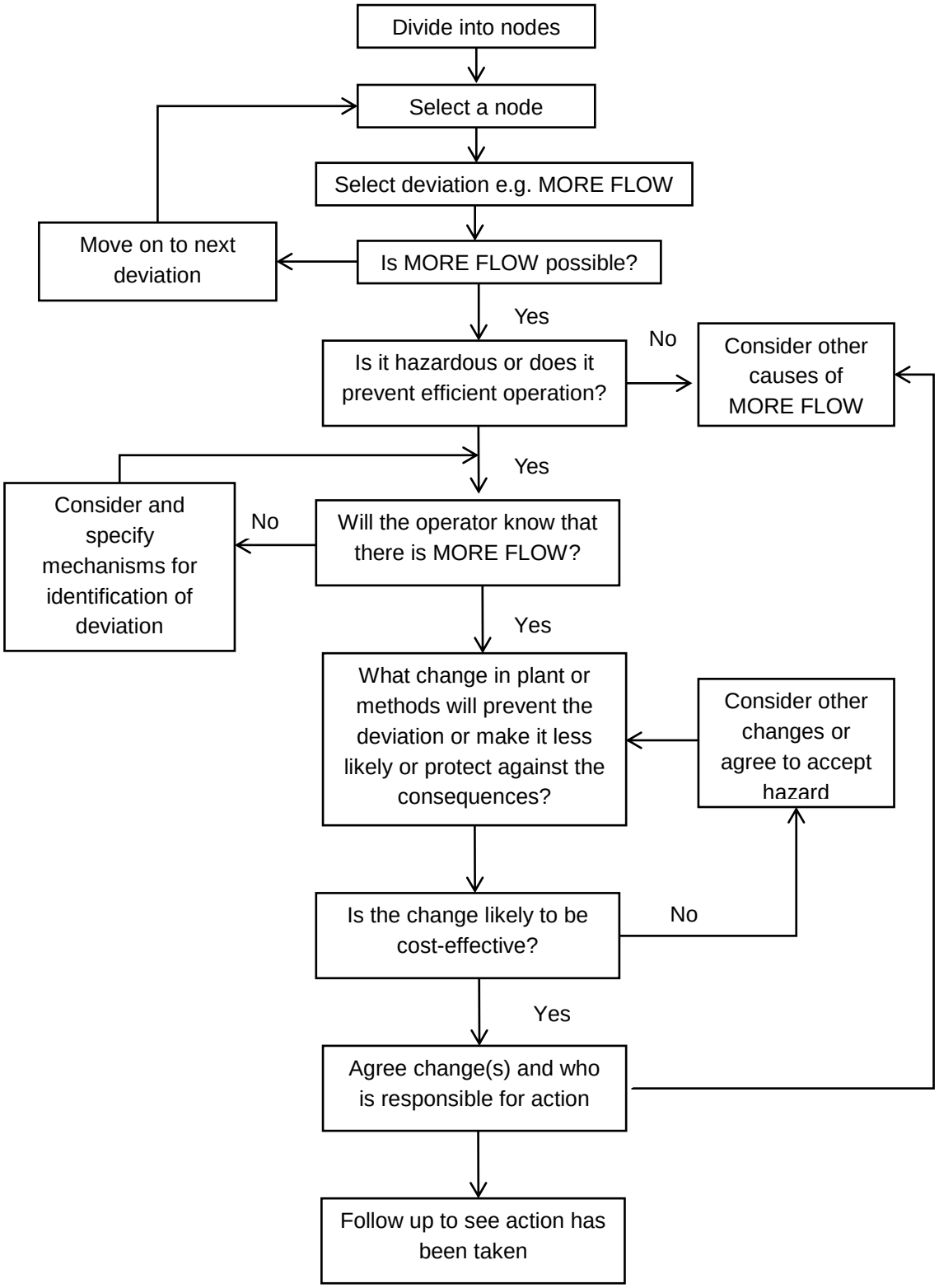


Figure 7. HAZOP procedure extracted from Figure 2.1"HAZOP and HAZAN", 4th Ed, P.11

4.3 HAZOP advantages and disadvantages

4.3.1 HAZOP advantages

1. It is a well-defined risk analysis approach to identify the dangerous scenarios and covers all systems in a P&ID draw.

2. It is possible to assess the impact of one process deviation in other subsystems. Following a systematic procedure allows HAZOP team to find new dangerous situations that may occur.

3. The big benefit for conducting a HAZOP study comes when the study recommendations are implemented and this is easier given a strong linkage to management processes for safety improvement, energy efficiency and investment appraisal.

4. One of the applications is to assist plant operators and safety managers in an online process monitoring and fault diagnosis of abnormal situations.

4.3.2 HAZOP disadvantages

Some limitations have been pointed out by Crawly [51], Tyler and Simmons [52]. A more comprehensive critique of the method by Baybutt [53] was provided very recently. Here, some points are addressed relevant for the nature of the method and those can be dealt with by an integrated qualitative and quantitative model-based framework.

1. HAZOP highly demands on the knowledge and skills of HAZOP study participants, without good HAZOP team and HAZOP leader good HAZOP study can't be done. It also influences the HAZOP study time required. Knowledge of how the process works are totally different from the knowledge of how the process may fail. The HAZOP study participant, knowledge holder of the process may not be able to access the failure knowledge. Some researchers suggest the knowledge representation of the process should be adopted to support the brain-storming section of the HAZOP meeting.

2. Another limitation of HAZOP is that this approach is inherently qualitative (a "diagnostic tool"). Moreover, there is the difficulty in estimating the time required for a complete HAZOP study.

3. Another negative aspect of the traditional HAZOP is the lack of risk acceptability levels and international standards. Furthermore, the work done by Labovsky [54] points out other negative characteristics of HAZOP. These include the possibility that some risks are neglected due to the qualitative nature of the method and recommendations or mitigating actions may not be implemented. In some cases, many recommendations cannot be implemented because of some factors, such as technical feasibility, risk reduction benefit, the total cost of implementation, availability of alternative solutions and it is not clear how much impact on process risk will have.

4. Also, it does not give priority to terms of recommendation implementation. Many recommendations require further investigation or other actions to complete the task, alleviate or

minimize the hazard and close out the action item based upon the recommendation. Without action sequence evaluation, it is not possible to recognize high risks in need of prompt attention. Assessment of severity and probability of each scenario allows selecting the most important preventive recommendations for implementation. Aiming to solve these problems, the adoption of the method associated with mathematical models may be needed.

5. Last but not least, possible causes of each scenario are identified, but it does not have any implications from where those causes are resulted by and explain more in detail if equipment failures and therefore it does not define a specific action for the equipment. This requires the failure modes analysis of equipment supported by some other available techniques to analyze the local failure cause and effect.

5 HAZOP PRACTICE IN OIL AND GAS INDUSTRY

5.1 *Plant-wide life cycle engineering (Plant wide-LCE)*

In general, the engineers design a plant in the form of a Block Flow Diagrams (BFDs), Process Flow Diagrams (PFDs) and Piping and Instrumentation Diagrams (P&IDs). Meanwhile, designers also generate operation procedures (OPs) for guiding operators to run the plant properly. However, there is a lack of a communication tool between designers and operators in phases of designing and operation/maintenance for supporting plant life cycle engineering (Plant-LCE) activities to boost productivity, quality.

Life-cycle in MIL-STD-882E defined as “All phases of the system’s life, including design, research, development, test and evaluation, production, deployment (inventory), operations and support, and disposal. LCE is an approach for engineering people to deal with environmental issues at first. A definition for LCE in [55] is “engineering activities which include the application of technological and scientific principles to manufacturing products with the goal of protecting the environment, conserving resources, encouraging economic progress, keeping in mind social concerns, and the need for sustainability, while optimizing the product life cycle and minimizing pollution and waste.”

Later on, researchers bring up the importance of Process safety management (PSM) [56-57] based on Plant wide-LCE for chemical processes, which is from process development to process safety design, plant construction, production, and plant maintenance[58], see in Figure 8. It is most effective when conducted during the conceptual design phase where recommendations affecting the general design may be made.

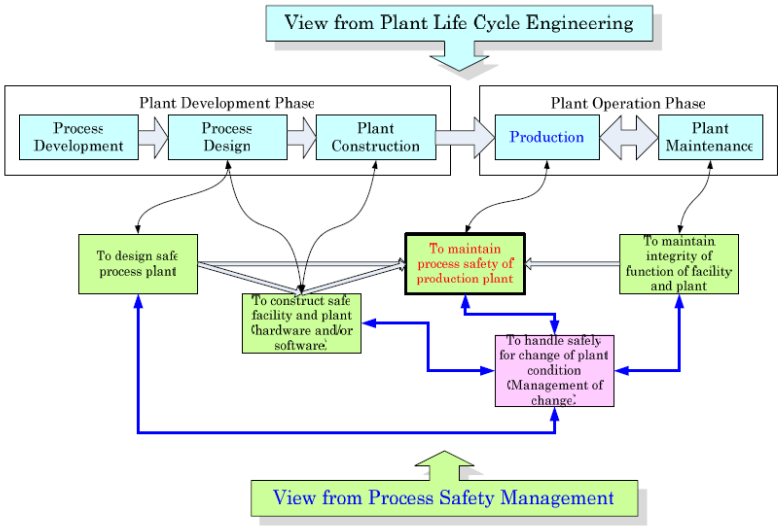


Figure 8. Views from Plant-LCE and PSM refers to reference [30]

Safety life cycle (SLC) generally refers as a concept for optimizing the design of a safety instrumented system (SIS) and to increase safety, see in Figure 9. It has been incorporated into many national and international standards, such as ANSI/ISA-84.00.01-2004), IEC 61508 and IEC 61511.

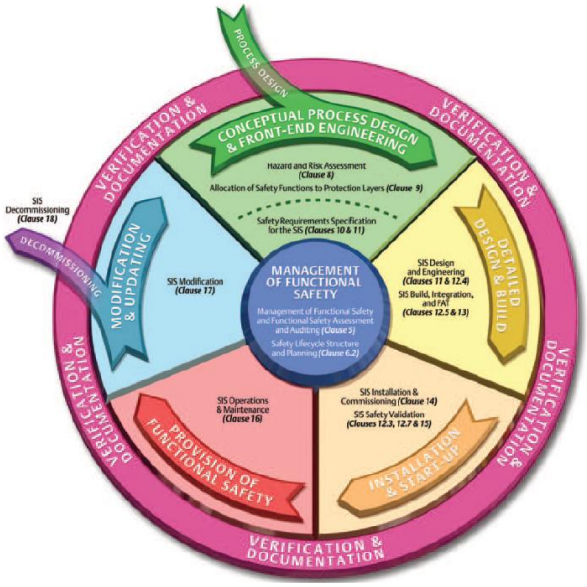


Figure 9. SLC for increasing safety of SIS

The SLC consists of three stages, see in Figure 10. The first is the analysis phase, which focuses on identifying hazards and hazardous events, the likelihood these hazardous events will occur, potential consequences, and the availability of a layer of protection, as well as the need for any SISs and the allocated SIL. The second phase is the realization, which focuses on design and fabrication of the SIS; and the final phase is the operation, which covers startup, operation, maintenance, modification and eventual decommissioning of the SIS. These phases encompass the entire life-cycle process of the safety system from concept through decommissioning. Figure 7 is an example in IEC 61508.

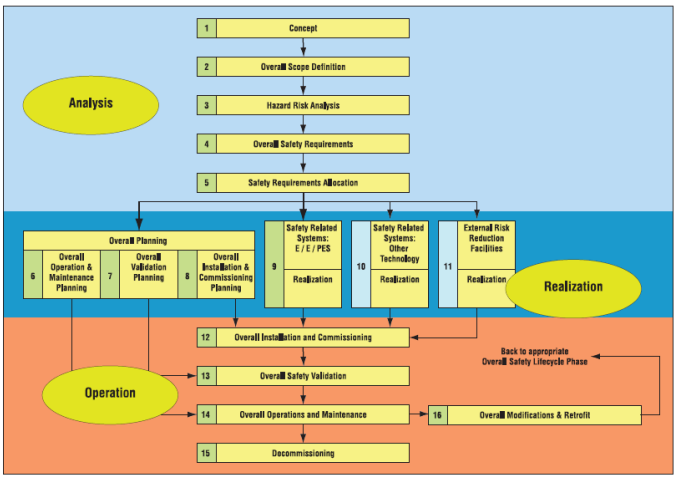


Figure 10. SLC described in IEC 61508

Ensuring safety to an acceptable risk level is vital for a life cycle of a plant. To complicate things, with

current PHA approaches engineers lack the means to integrate BFDs, PFDs, P&IDs, and OPs with process behaviour information[59]. Therefore, it is necessary to establish a framework to provide an assistant in performing hazard identifications using PHA approaches, such as HAZOP, in a process (such as oil and gas process) life cycle. Some preliminary studies [60] for implementing HAZOP in project life cycle in different types of process, such as railroad transportation, were examined. However, the framework of information sharing in stages for HAZOP is still missing.

5.2 HAZOP position in Plant wide-LCE

HAZOP was originally applied to finalized plant design drawings. However, changes arising at this stage can be costly and the technique has been modified or progressive stages of application in Plant wide-LCE [61]. From the inherent safety analysis point of view, the largest payoffs can be achieved by conducting HAZOPs early in the sense that the inherent safety principles are considered early as well as claimed by Khan[62]. From the cost of changes vs. project life cycle perspective, HAZOPs are also best to be done early in the project, shown in Figure 11. The intersection of the ability to influence changes curve and cost of changes curve probably suggests the point at which a change in scope changes from a constructive opportunity into a destructive intervention.

As well as being a design tool HAZOP can be equally successfully applied to existing plant and can lead to worthwhile modifications to the maintenance procedures. As discussed in Table 1, HAZOP are most suitable in the later stages of detailed design, for examining operating facilities and when changes to existing facilities are made. Cui also argued that in the design stage, the operation stage and the modification stage, the computer-aided method for HAZOP might provide a more reliable lifelong guarantee of process safety, see in Figure 12.

HAZOP studies may also be used more extensively, including: at the initial concept stage when design drawings are available, when the final piping and instrumentation diagrams(P&ID) are available, during construction and installation to ensure that recommendations are implemented, during commissioning, during operation to ensure that plant emergency and operating procedures are regularly reviewed and updated as required[63]. In general speaking, HAZOP should be applied during all stages in plant wide-LCE [64].

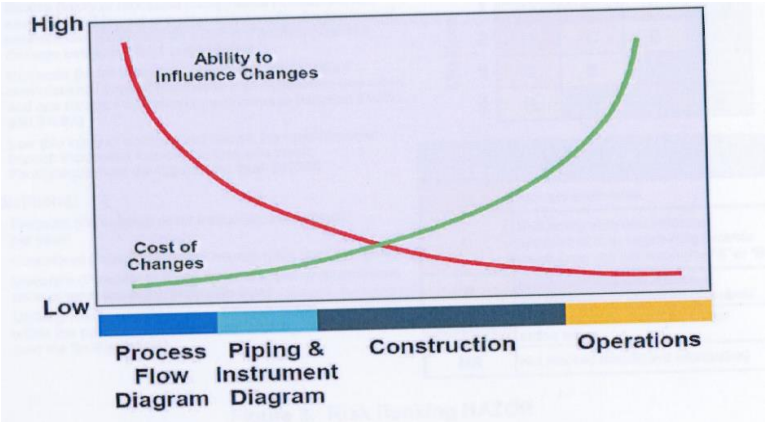


Figure 11. Cost of changes vs. Project life cycle in [65]

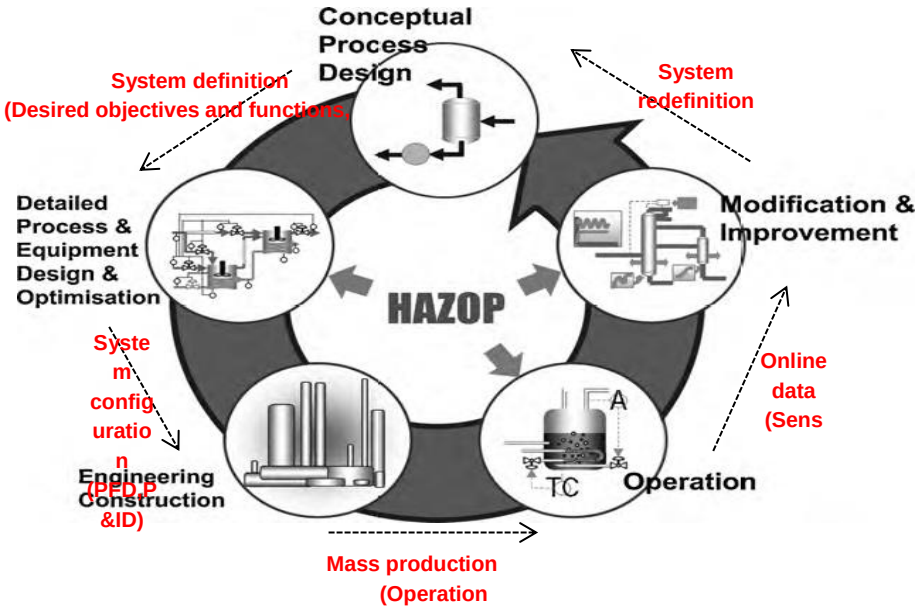


Figure 12. Information flow for HAZOP studies in plant wide-LCE

(Adapted from Cui et al.[66])

5.2.1 Implementation of HAZOP in FEED

Front-End Engineering Design (FEED) is the basic engineering which comes after the Conceptual design and before completing the detailed design. It focuses on the technical requirements as well as rough investment cost for the project and it is used as the design basis.

In FEED [67], the design concept and major system parts are decided, although the detailed design and documentation required to conduct the HAZOP do not exist. The information can be plant site information, plant objectives, required functions and Block Flow Diagrams (BFD). BFD represents unit operations. Blocks are connected by straight lines representing process flow streams. Process flow streams may be mixtures of liquids, gasses, and solids flowing in pipes or ducts.

It is necessary to identify site major hazards and site specific safety requirements at this stage to facilitate the future HAZOP analysis. Here, it is called as Preliminary Hazard Identification. This can refer to the Hazard study 1 in reference [68].To carry out the analysis, PrHA, What-if analysis and Checklist can be used as reviewed in PHA techniques section.

In the Preliminary FEED, the preliminary plot plan, Process Flow Diagram (PFD) and basic process data are available. PFD indicates the general flow of plant processes and equipment. The PFD displays the relationship between major equipment of a plant facility and does not show minor details such as piping details and designations. Usually, it includes the process piping, major equipment items, control valves and other major valves, connections with other systems, major bypass and recirculation streams, operational data(temperature, pressure, mass flow rate, density etc.), often by stream references to a mass balance, process stream names. A variety of software tools is available for accomplishing the PFD task, such as K-Spice®, Unisim, HYSYS, Aspen, and PRO II.

At the stage in a project where the PFD has been generated, a majority of the future plant costs and safety/environmental risks are locked in. Therefore, it is necessary to identify major process hazards and basic process safety requirements by using HAZOP. To implement the results of HAZOP analysis, the final FEED package is achieved. Implementation of HAZOP in FEED is illustrated in Figure 13.

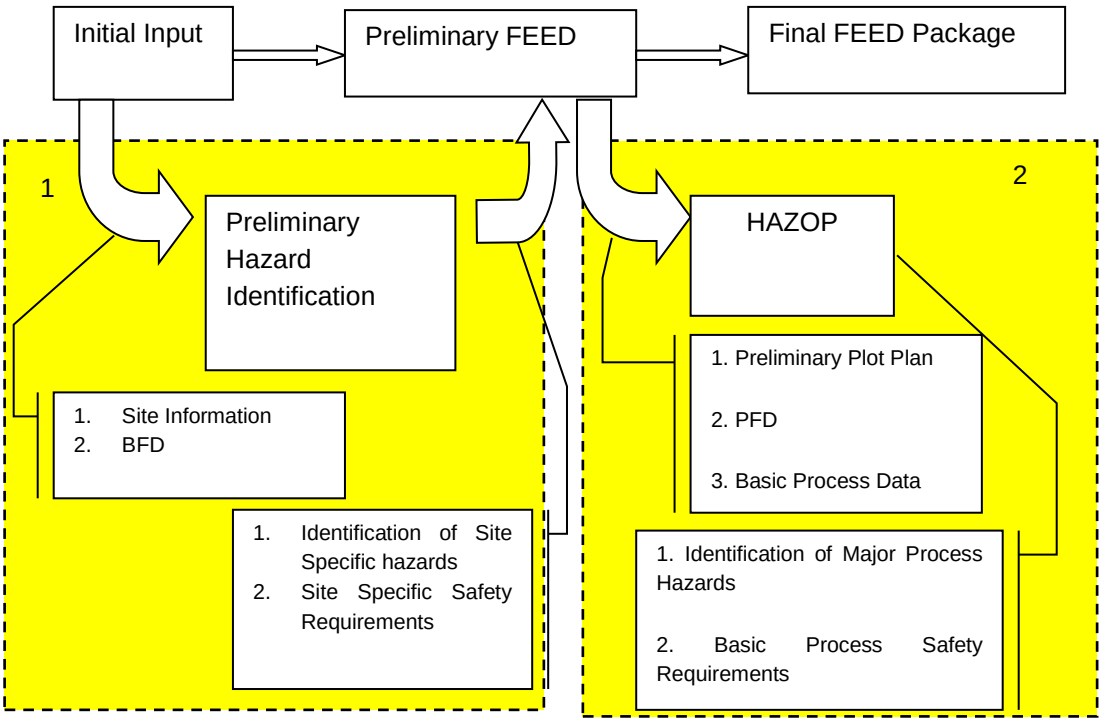


Figure 13. Implementation of HAZOP in FEED

5.2.2 Implementation of HAZOP in EPCC

Engineering Procurement Construction Commissioning (EPCC) is covering all the activities from design, procurement, construction, to commissioning, which is a stage before a project is handed over to the end-user or owner.

There are three stages to develop a 'frozen' P&ID, especially when going from one design phase to another: Approved for Plan(AFP) P&ID, Approved for design(AFD) P&ID, Approved for Construction(AFC) P&ID. P&ID is a diagram which shows the interconnection of process equipment and the instrumentation used to control the process. AFP P&ID provides detailed plot plan, P&ID, detailed process data to facilitate the HAZOP studies. The HAZOP studies in this stage identify process hazards and operability problems, detailed process safety requirements, and requirements for operating procedures. These required actions for mitigating hazards in the HAZOP will be implemented in the AFD P&ID. As claimed in IEC 61882, it is the best time to carry out a HAZOP study just before the design is frozen. And what is more, it is also important to have a system that enables assessment of the implications of any changes made in the AFD P&ID.

Then the AFC P&ID will be developed which will be going into construction stage. An "as-built" HAZOP

is often carried out after construction and immediately before commissioning a new plant, if commissioning and operation of the system can be hazardous and proper operating sequences and instructions are critical, or when there has been a substantial change of intent in a late stage. The "as-built" HAZOP should also review all actions raised during earlier studies to ensure that these have been resolved. Implementation of HAZOP in EPCC is illustrated in Figure 14.

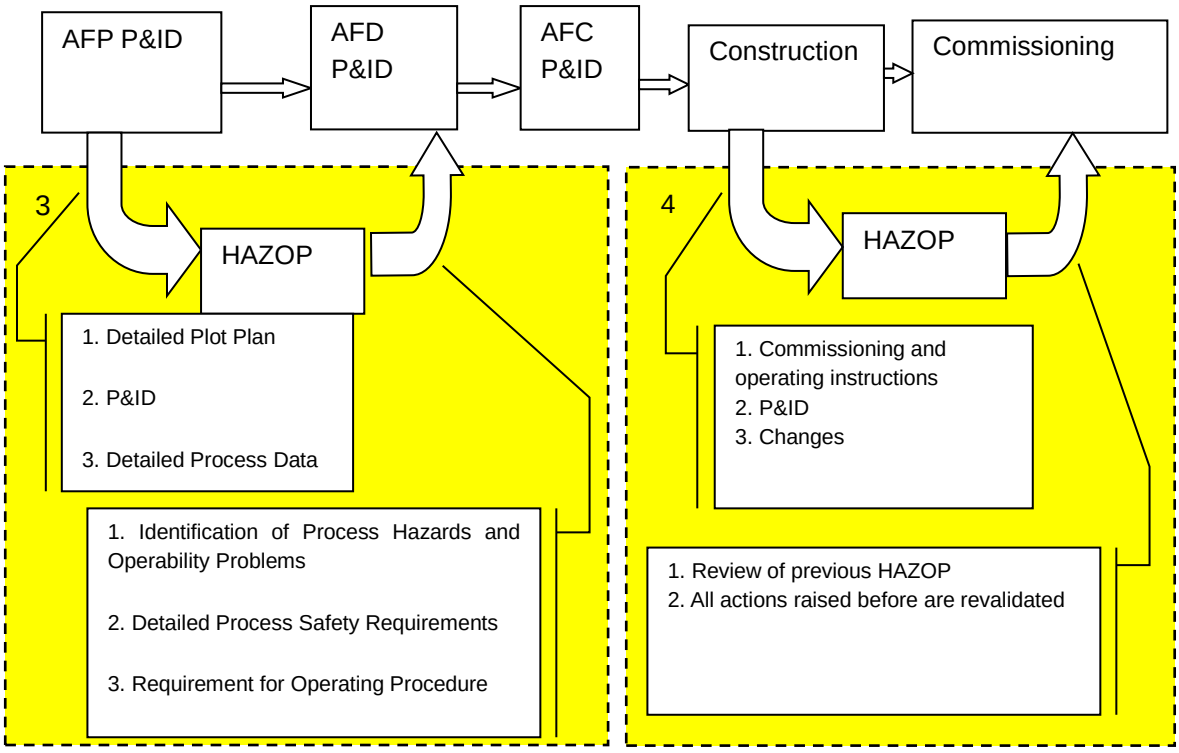


Figure 14. Implementation of HAZOP in EPCC

5.2.3 Implementation of HAZOP in Operation and Maintenance stages

The implementation of HAZOP should be considered before implementing any changes that could affect the safety or operability of a system or have environmental effects, see in Figure 15 and Figure 16. A procedure should also be put in place for periodic reviews of a system to counteract the effects of "creeping change" [69]. It is important that the design documentation and operating instructions used in a study are up to date.

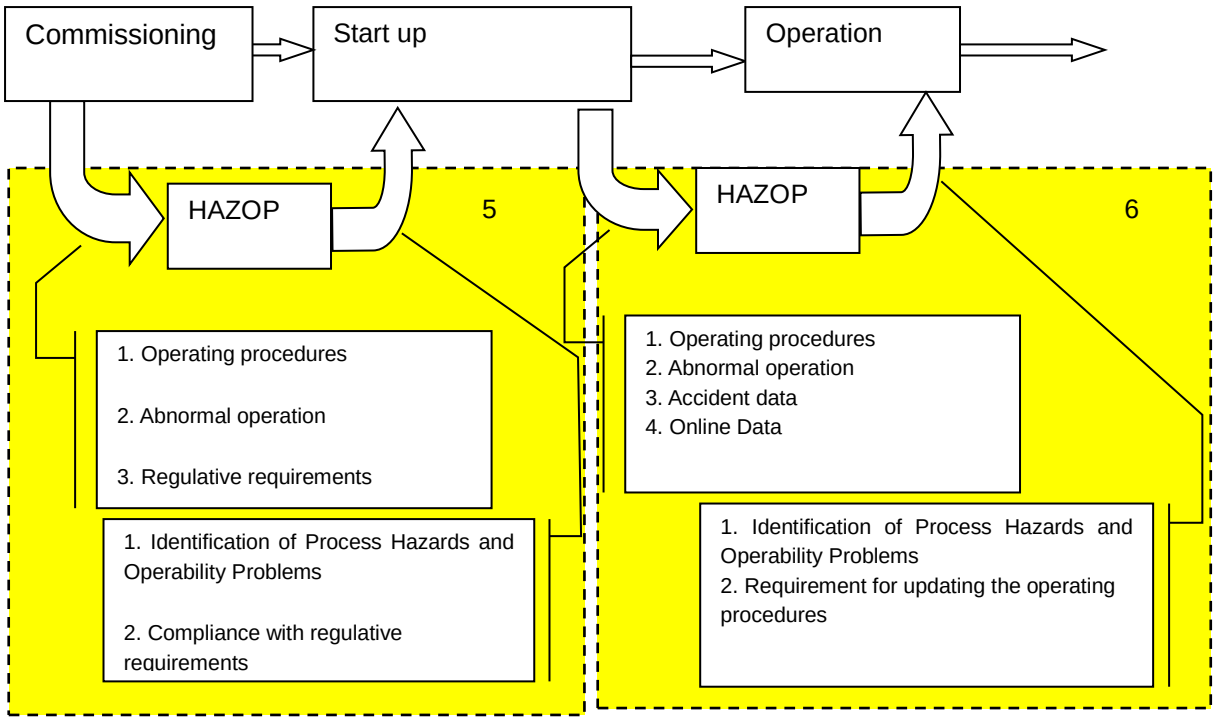


Figure 15. Implementation of HAZOP in Operation stage

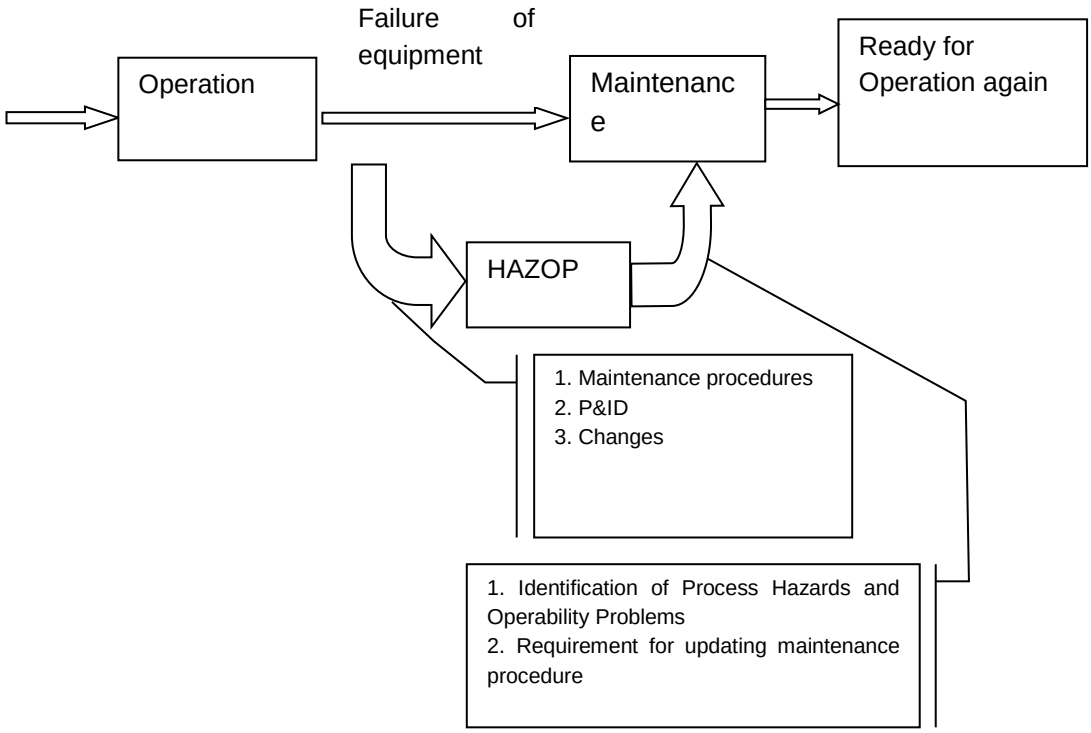


Figure 16. Implementation of HAZOP during Maintenance stage

5.2.4 Implementation of HAZOP in Decommissioning and Disposal stages

A study of this phase may be required, due to hazards that may not be present during normal operation. If records from previous studies exist, this study can be carried out expeditiously. Records should be kept throughout the life of the system in order to ensure that the decommissioning issues can be dealt with expeditiously.

6 CHALLENGES OF HAZOP AND COMPUTER-AIDED METHODS

6.1 HAZOP facing challenges

HAZOP mainly faces 5 challenges as follows: (1) Knowledge management of system complexity; (2) Uncertainty; (3) Vagueness; (4) levels of completeness; (5) Efficiency. The challenges pyramid is shown in Figure 17. The following sections address and illustrate each challenge in detail.

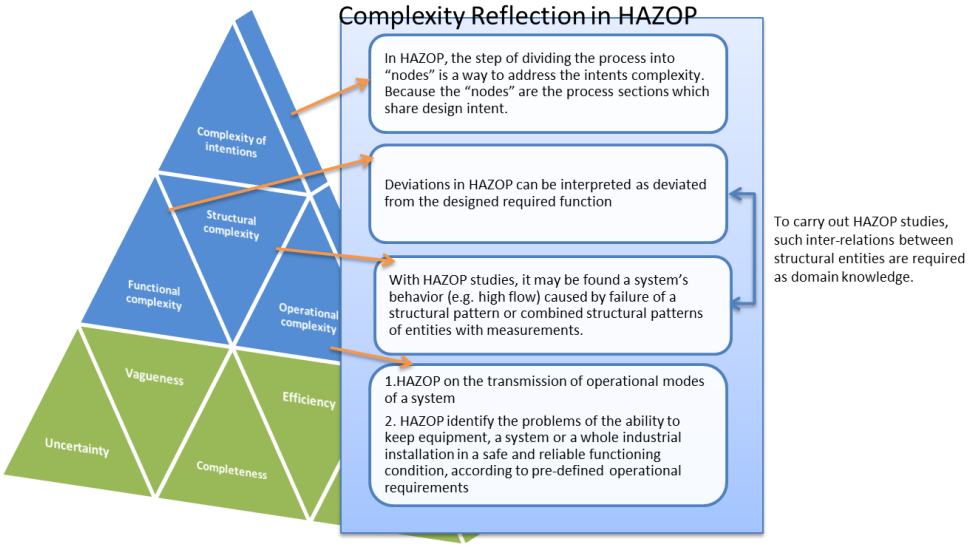


Figure 17. HAZOP challenges pyramid

6.1.1 Knowledge management of system complexity in HAZOP

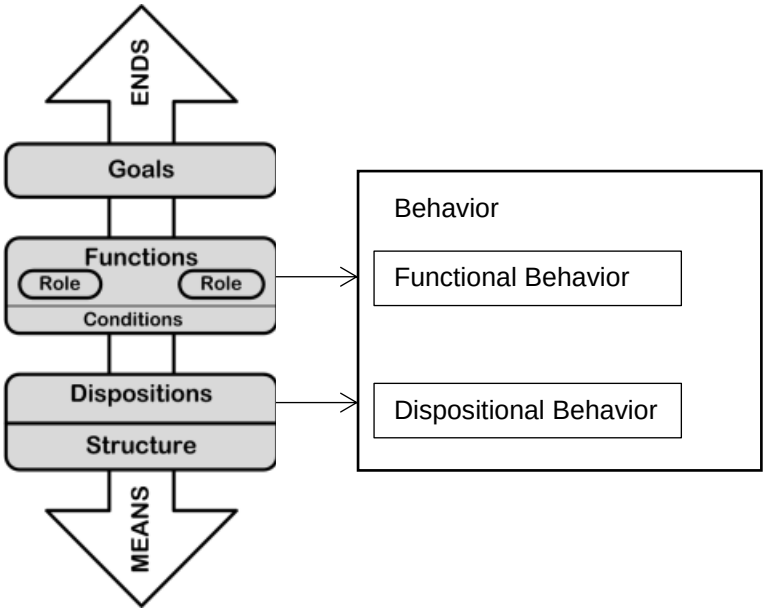
HAZOP is a tool or process to identify potential hazard and operability problems. It is not a design review, a re-design session or a battle of wills between designers and operators. It is used to provide management with knowledge of where potential hazards may exist and to provide an information on mitigation recommendations for plant design modifications prior to construction, on mitigation recommendations for providing specific details for administrative controls, on hazard information communication. The mean of knowledge for carrying out HAZOP comes from the complexity in a system. In addition, HAZOP itself is a structured method to cope with complexity.

Complexity in system engineering can be expressed by the multilayer levels of subsystems, their connections and the number of system elements and their interrelations [70], for example casual relation in one layer. In terms of functions, the function of entire complex systems is the aggregation

and convergence of the functions of the sub-parts [71].

Several different measures defining complexity have been proposed within different scientific disciplines, such as engineering design [72], physics [73], and computational science [74]. Such measures of complexity are generally context dependent [75]. Thirty two complexity types in twelve different disciplines and domains such as projects, structural, technical, computational, functional, and operational complexity are defined by Colwell[76].

Before we look into the complexity of an engineered system, the distinction between three types (structure, function and behaviour) of description of a mechanism is illustrated.



The essence of a functional description is teleology or intention, the relation of the structure and behaviour of a mechanism to its larger context. For example, pumps have two generic functions: one function of a pump is to transport fluids under specific conditions and another function of a pump contains all fluids under all pertinent design conditions. Semantic analysis reveals that the verb *transport* represents a relation between an element of structure (the pump) and a possible behaviour (fluids are not vaporized). However, simulation of the working equipment does not include vaporization among its possible behaviours. The vaporization referred to appears in the design process for the equipment, prior to the addition of the pump. The fluids are able to maintain in liquid phase under design conditions. The structure and dispositions are the means to action. Functions are the potentials and opportunities available for action. The behaviour in two aspects are functional behaviour and dispositional behaviour.

Different dimensions of complexity of a system are elaborated below.

6.1.1.1 Complexity of intentions

At the highest level of a design process, the designer develops the design intent. Through the design process, the designer transforms the design intent into realizable design details. However, what are

intents? In action theory, intents can be seen as precursors to planned action, parts of action plans. Intents complexity comes from human mind and relations of desired intents / undesired intents (goals/ threats). So the intents complexity is inter-subjective.

The intents complexity can be expressed by a goal tree (GT) [77]. The GT is concerned with the goals and objectives which must be achieved by the SYSTEM. Both safety and process objectives are represented in the GT. The customary usage is to start the GT with a single top objective which is achieved if all safety and process objectives are met. All objectives are then described in terms of sub-objectives which may also be further refined, continuing to any level of detail required. In general, at the upper levels which comprise the GT, this decomposition is found to form a conjunctive hierarchy, in that, at these levels of abstract description, objectives decompose into sub-objectives all of which must be achieved.

In HAZOP, the step of dividing the process into “nodes” is a way to address the intents complexity. Because the “nodes” are the process sections which share design intent. Dojuno et al. [78] proposed a criterion for selecting and sizing nodes.

5.1.1.2 Functional complexity

In engineering, a function is interpreted as a specific process, action or task that a system is designed to perform [79]. System functions are facts such as that all knowledge shared by engineers is agreed upon in the community [80]. These for two interwoven principles, namely as machine-like functions and ‘regulation’ functions, then machine-like functions are ideally defined by precise operational principles, while the correctness of a regulative achievement can be expressed only in gestalt-like terms. Therefore, the functional complexity is inter-subjective [81].

Suh’s measure of complexity [82,83] in the functional domain is built on the concept and framework of axiomatic approach of design. In his complexity theory, complexity is defined as a measure of uncertainty in satisfying the functional requirements (FRs) within the specified accuracy. In designing engineered systems, by means of design parameters (DPs) or physical parameters to satisfy the FRs. When a given DP is chosen to satisfy the FR, the uncertainty is characterized by the system’s ability to satisfy the FR within its design range. The FR is satisfied only when the system range is within the design range [84]. HAZOP is used to identify the scenarios when system range is overlapped or completely out of design range.

Four types of complexity: time independent real complexity, time-independent imaginary complexity, time-dependent combinatory complexity and time dependent periodic complexity in the functional domain are described by Suh. However, we do not think it made any contribution to ontology of functions. Accordingly, it is not useful for copying with functional complexity.

5.1.1.3 Structural complexity

Structural complexity deals with multiple connections between component and subsystem of a technical system[85]. Structural Complexity Management is often seen as having evolved out of the first complex engineering projects that were accompanied by the paradigm of Systems Engineering, having itself evolved out of Systems Theory. There is a substantial body of metrics available that is able to assess the structural complexity of a system with a view to different patterns. However, the transfer to the specifics of engineering design processes, i.e., what behavioural aspects relate to what structural characteristic evaluated in a metric, remains unsolved. With HAZOP studies, it may be found a

system's behaviour (e.g. high flow) caused by failure of a structural pattern or combined structural patterns of entities with measurements.

5.1.1.4 Means-end relation links functions and structures

In the context of system objectives, the structural complexity can be expressed by five types of inter-relations between structural entities (e.g. components, energy and material medium) and system functions in means-ends relations, see in Figure 18: (1)Side effect: Although the structural means are dedicated to achieving a particular function, some of them may exert secondary effects on other functions.(2) conditional constraints: in many cases, the use of a structural entity in order to ensure a function may be conditioned on the fulfilment of another structural entity.(3) Technical dependencies: They are generally due to the sharing of technical resources between several structural entities. (4) Sharing dependencies: To achieve a specific function (capacity), it is required to share structural entities or interactions of structural entities. (5) Arbitration: In some cases, alternative structural entities are required to achieve a specific function. To carry out HAZOP studies, such inter-relations between structural entities are required as domain knowledge.

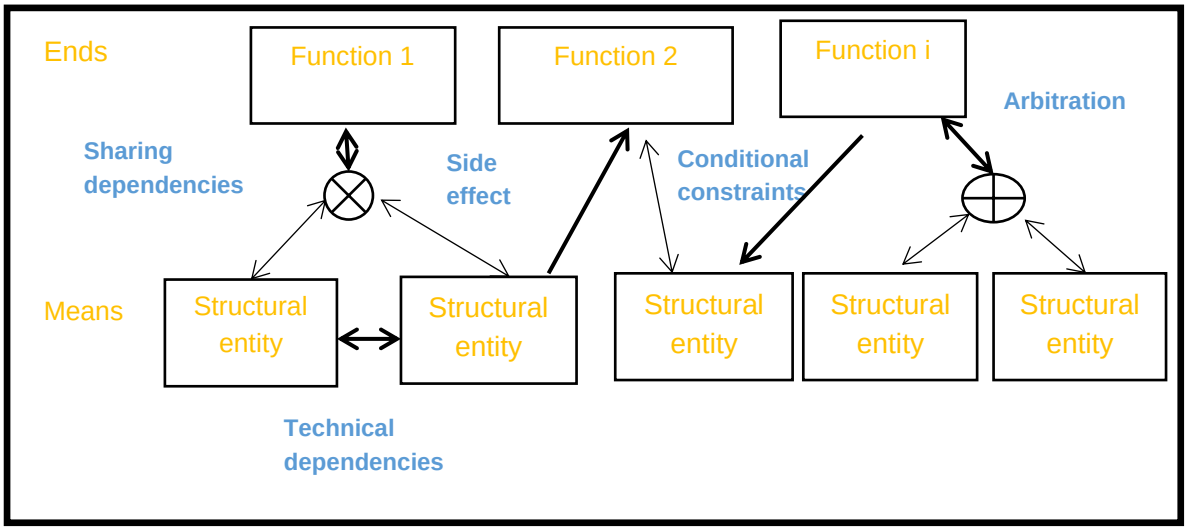


Figure 18. A generic presentation of structural complexity in the context of system objectives

5.1.1.5 Operational complexity

Operability is the ability to keep equipment, a system or a whole industrial installation in a safe and reliable functioning condition, according to pre-defined operational requirements. Accordingly, Operability problems are associated with any operation which under the requirements would cause a shutdown or possibly lead to a violation of HSE (Health, Safety, and Environment) regulations or negatively impact profitability. However, because of the high profile of systems accident, emphasis is too often placed upon the identification of hazards to the neglect of potential operability. The government regulations further emphasized the "HAZ" technique; "OP" was of less interest to the authorities. However, "OP" analyses have the potential to improve quality and productivity, and it is precisely those financial gains that will endear HAZOP to any manager. Hendershot et al. [86] claimed that one HAZOP study of a gas plant incidentally found ways to increase the yield of natural gas liquids by 50%. Many systems are self-organize to operate in a state of optimum performance. However, the

optimal state is potentially a high-risk state that's also why operability problems should be identified.

The operational complexity is different from the operational complexity of human performance which normally dealt with Human HAZOP. The operational complexity in this report presents all the possible states in which a system can be operated and the transitions between them. Process HAZOP examines the scenarios where the system is in malfunction under the pre-defined operational requirements.

Operational complexity has a perspective, if the operational modes of a system are considered, for example, start-up mode is required to get the system into the nominal operation situation, emergency modes guarantee secure operation when shutting down, or different configurations to comply with varying demands[87]. Process HAZOP needs to pay more attention to the transmission of operational modes of a system.

5.1.1.6 Subjective vs. Objective aspects of complexity in design and operation

Process HAZOP deals with system complexity in design and operation, on the other hand, Human HAZOP examines the subjective process complexity as shown in Figure 19. Both intentional complexity and functional complexity in design are inter-subjective as known in social science [88]. In operation, functional complexity is deemed objective because after the design stage, functions are already selected in terms of the specified properties of structures and their applied context. Static features are the features necessary to describe the state of an engineered system. Dynamic features are the features necessary to describe the state of any engineered system deviating from its design intent due to uncertainty.

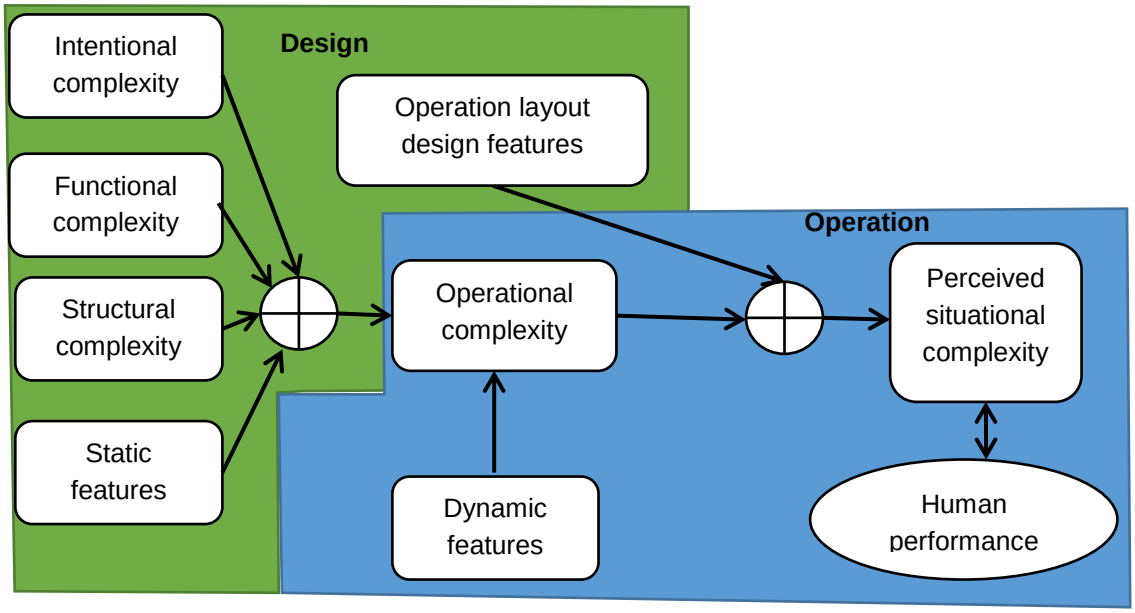


Figure 19. Complexity in design and operation

5.1.1.6 Modeling system complexity

HAZOP is required to relate a system representation to the underlying chain of causality of triggering hazards. There is a need for system models which can reveal complexity aspects relevant for system design and operation, that is, the elements and the relations representing selected features of the

systems relevant for a particular design or operational purpose. Every model has a purpose addressing a specific type of complexity, which should represent the nature of complexity independent on the representation form or tools. It means different models represented eg.by a graphic representation may address the same type of complexity. This aspect of system complexity can accordingly be measured by properties of its graph representation. Complexity is accordingly a property of the system model and can be reduced or increased by aggregation or decomposition of the graph. Therefore, system complexity is relative to the features represented and dependent on the purpose or the model. Another important aspect of system complexity can be measured by the number of system aspects or perspectives which are necessary in order to provide a representation of the system which provides the information relevant for the design or operational problem under consideration. Whereas the complexity measure in the first case is a syntactical property of a particular perspective on the system, it is, in the latter case, related to the content of the representation i.e. semantic relations between the system represented and the model. A complex system would, in this latter view, require many perspectives for its proper representation and, therefore, be semantically complex [89]. Therefore, there is a need for a modeling language with clear syntax and semantics to decompose and aggregate the above mentioned different aspects of complexity in a meaningful way, such as means-ends and whole-part, see in Figure 20.

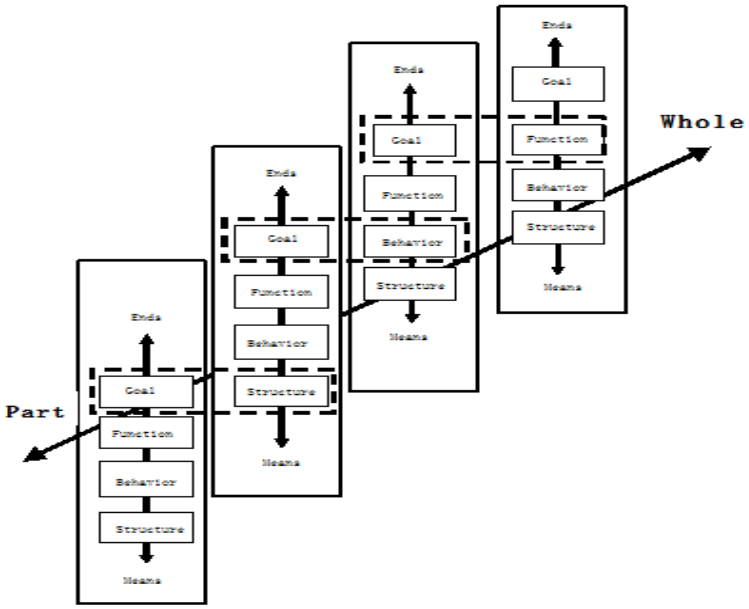


Figure 20. System decomposition and aggregation by means-ends and whole-parts relations

6.1.2 Uncertainty in HAZOP

Particular interest in risk assessment for complex systems is the use of subjective information obtained from experts, which bring up uncertainty aspects of the process hazard analysis. Markowski[90] considers uncertainty in the process risk as an imperfect prediction of risk and points out that there are three types of uncertainty in process safety analysis: completeness uncertainty, modeling uncertainty

and parameter uncertainty. In particular for hazard analysis, e.g. HAZOP, the completeness uncertainty represents inability to identify all risk factors and all representative accident scenarios as well as errors in screening of hazards. Most common practice for screening of hazards is by using risk ranking matrix. The HAZOP consequences are risk rated based on their severity and likelihood. Modeling uncertainty represents inaccurate interaction between different components and variables in accident scenario models. And parameter uncertainty represents imprecision or vagueness in characteristic properties of contributors and variables, for instance, to select appropriate guideword and process parameter. The nature of uncertainty can be lack of knowledge (subjective) and physical variability (objective).

Another uncertainty in HAZOP may come from the inadequate evaluation of recommendations; we call it recommendation uncertainty. Many recommendations require further investigation or other actions to complete the task, alleviate or minimize the hazard, and close out the action item based upon the recommendation. The key to planning implementation activities is a sound method of prioritizing HAZOP recommendations to recognize high risks in need of prompt attention. And the assessment of severity and probability of each scenario allows selecting the most important preventive recommendations for implementation. Such assessment results in recommendation uncertainty.

In this report, we consider how the completeness uncertainty and modeling uncertainty contribute to the quality of HAZOP results. Therefore, the method for dealing with it, we will categorize into computer aided methods for tackling with completeness of HAZOP challenges.

6.1.3 Vagueness in HAZOP

Vagueness in HAZOP can be interpreted in two ways: vagueness in HAZOP records and vagueness in magnitude of causes and consequences. HAZOP results are recorded by the HAZOP team in a worksheet. However, some of the team may not follow the written information because of the vagueness in HAZOP records. In another word, their degree of fidelity is dependent on the particular scribe. This influences the quality of records. Usually, the HAZOP analysis does not consider the duration and magnitude of the deviations generated during the operation. However, what exactly does the deviation of ‘less flow’ mean: 70% or 20% of the usual operation value?

6.1.4 Completeness of HAZOP

Completeness of a HAZOP is determined by the set of possible hazards scenarios in terms of possible causes and consequences. It affects a hazard evaluation in two ways. First, it can never be certain that all hazardous conditions or potential accident scenarios have been identified. Second, for the identified hazards, it can never guarantee that all possible causes and effects of potential accidents have been considered. Moreover, a hazard evaluation is a “snapshot in time” evaluation of a process. Any changes in design, procedures, operation or maintenance (however small) may have a significant impact on the safety of the facility.

Unrecognized hazards were implicated in the BP Texas City disaster, Formosa Plastics explosion, Chevron Richmond Refinery fire and other high profile accidents. HAZOP may fail to identify credible hazard scenarios. A fault tree analysis [91] of the generic HAZOP process was performed to trace the sources of constraints, errors, and omissions. 17 possible sources were identified shown in Table 4. As

we can see the quality of input data (P&ID, equipment specifications, material and safe operating limits, Instrumentation, alarms and interlocks, Process chemistry, utilities, human machine interface, standard operating procedures, history accidents, etc.) for carrying out HAZOP also influences the completeness of HAZOP.

Table 4. Sources of constraints, errors and omissions identified by FTA in Reference [63]

Item No.	**FTA Finding**	**Constraint, Error, or Omission**	**CSB case study documented examples of occurrence**
1	Inherent PHA method limitation	Constraint	None provided
2	Not in scope of work	Constraint	None provided
3	Not enough time or budget	Constraint	None provided
4	Limited Expertise or industry state of knowledge	Constraint	T2 labs [92], BP Amoco [93], process chemistry-reaction hazards not understood or poorly understood.
5	Inappropriate PHA method	Error	None provided
6	Outdated or inaccurate P&ID	Error	Oleum release[94], emergency power supply not included on P&ID
7	Ignored incident history-plant, company or industry	Error	BP Texas City[95], BP Amoco,Formosa Plastics[96], Chevron[97], PHAs and revalidations did not take into account documented plant incidents or company incidents, and/or ignored recommendations from incidents.
8	Took credit for safeguard that is not independent	Error	Oleum, All safeguards required operator attention and action, no engineering controls independent of operator. Chevron PHA only listed qualitative safeguards such as inspection and corrosion allowance.
9	Took credit for safeguard that is not maintained	Error	BP Texas City-raffinate splitter alarm and below down drum high level alarm did not work. Chevron PHA only listed qualitative safeguards such as inspection and corrosion allowance.
10	Mistake in analysis	Error	Chevron Richmond, Did not identify failure mechanism for sulfidation corrosion
11	Incorrect safe operating limits	Omission	BP Amoco Safe operating limits not identified

12	Did not consider human factors	Omission	BP Texas City, Oleum, Formosa Plastics-Human error not taken into account in evaluating safeguards
13	Did not consider external factors like fire or earthquake	Omission	None provided
14	Did not have process safety information or mechanical integrity(MI)data	Omission	Oleum-PHA team lacked information on hazards of transferring oleum using emergency power supply
15	Did not consider non-routine operating modes such as startup and shutdown	Omission	BP Texas City and BP Amoco did not consider startup and shutdown
16	Did not consider valid guide word	Omission	Formosa cited by OSHA[98] for leaving out key guide words for batch processes
17	Did not consider key process variable	Omission	CSB Sterigenics [99] No explosion scenarios evaluated for explosive concentrations

Note: CSB is abbreviation of U.S. Chemical Safety Board

6.1.5 Efficiency of HAZOP

The proper planning and management of HAZOP studies is one of the crucial factors for better effectiveness and good reliability of the results. In practice, the assigned time for HAZOP study is either too short or it is too lengthy. What is more, the manual HAZOP study itself is a time consuming approach. By investigation, for the installation of an oil and gas unit on an existing site, each P&ID (Piping & Instrumentation Diagram) might take 5 or 6 h depending on the scale of the project. For the installation of a major new unit on an existing refinery or of the topsides on an oil platform, 6–8 weeks may be required.

So the balance of time and performance of HAZOP becomes an issue which brought up two questions: How long time devoting for a HAZOP study is the most beneficial and in which way the HAZOP study can be speeded up under the certain devoted time. For effective HAZOP study McKelvey [100] has suggested some key parameters (factors) such as: skill and experience of team leader, proper planning, and availability of information that should be given proper attention. Mulvihil [101] has presented an efficient and effective HAZOP application in studying offshore platform using past experiences of similar case studies and guidelines proposed by McKelvey. The more comprehensive techniques applied to answer the two questions concerning efficiency of HAZOP will be reviewed in computer-aided methods for improving efficiency of HAZOP section. However, the report mainly focuses on HAZOP study itself rather than planning of it, therefore, the HAZOP process management will be summarized in limited space.

6.2 Computer-aided methods for HAZOP

6.2.1 Computer-aided methods for improving knowledge management of system complexity in HAZOP

Developing models of a process system is an effective way for coping with system complexity. Leveson [102] in her *System Safety Engineering: Back To The Future* book also argued that increasing complexity and coupling requires new models. In most of cases, the procedures for developing models can also be computer-aided. There are different methods for modeling of a process system and afterwards, based on those models and run reasoning for conducting HAZOP.

Qualitative and quantitative models built based on first principles are two modelling methods for representing engineering systems. Quantitative approaches are expressed in terms of mathematical relationships such as differential equations. Complex systems such differential equations are hard to set up to represent and reason about knowledge of physical phenomena and systems, In contrast, the qualitative modeling and reasoning techniques that can handle the complexity of large scale dynamic processes. The main reason for this capability is the ability to make qualitative models on several levels of abstraction.

Functional models are one group of qualitative models. It is a combination of functional casual models and models of intentions. *Functional casual models* describe the underlying cause-effects relationships which govern deviations from the normal function of process. Models intent describes knowledge of the process goals. It means that a casual model is placed in a context of intention then it becomes a functional model.

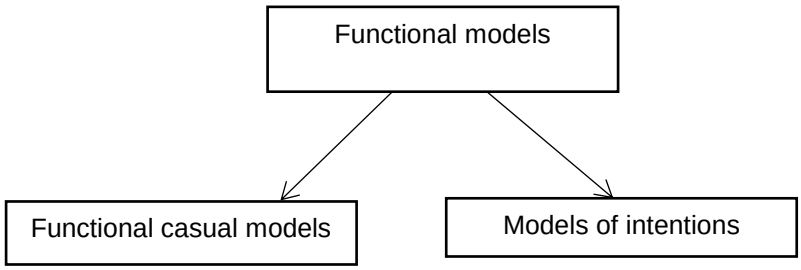


Figure 21. Functional modelling techquie

Functional modeling technique is mainly for modeling of purposes and intentions of a system. However, it also capture different dimensions of system complexity. A functional model in system engineering provides a structured representation of the functionality of the modeled system for an intended application purpose. A functional model is developed from a perspective which focuses on describing the purposes and functional organization of the specific possibly dynamic process. Specifically, a functional model consists of sets of goals, function structures with interrelations and functional elements coupled by causal relations.

The representative functional models and applied for HAZOP studies are D-higraphs[103] and Multilevel Flow Modeling (MFM). The main difference between the two methods is that MFM provides facilities for semantically determinations between different functional abstractions of a system and gives guidelines of how to decompose and aggregate system functions on varying means-ends relations,

whereas D-higraphs do not. It is exactly the reason why MFM seems to be more accurate than D-higraphs because of the much better human intuitive cognitive support for modeling of system complexity.

It should be noted that MFM is a network structured hypergraph, where function nodes are connected constrained by function syntax and the representing connection line depends on their casual relation. The set of function primitives are defined based on a theory of action types applied for process systems. The function node states are defined by possible failure modes of the specific function. An example of energy flow structure of a MFM model of a simple heating system is in shown in Figure 23.

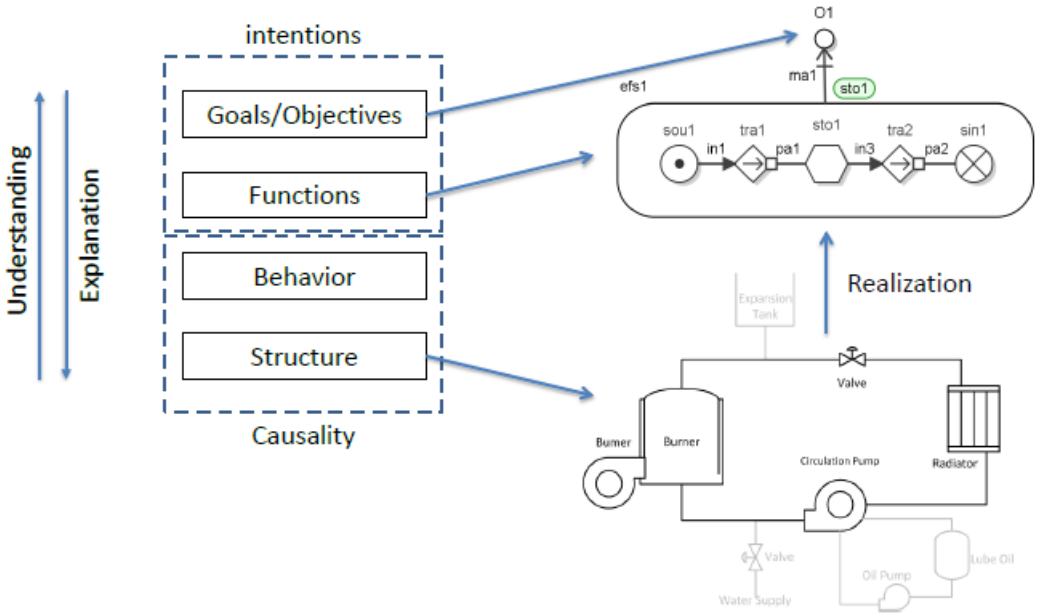


Figure 22. The energy flow structure of a MFM model of a simple heating system from Figure 3.9, P.52 in Zhang, X. (2015). Assessing Operational Situations.

While D-higraphs tries to describe three levels of system knowledge: structure, behavior, and function. Structure knowledge is displayed in a blob assigned as an ACTOR, the device to realize the function and edges attached with the blob at front and at end representing the energy, mass, information flow into and out of the blob. Behavior knowledge is represented and associated with the bi-edges by states of variables and expressed in a set of constraints Z_{Yn}^{Xn}, where variable Xn is directly proportionally to variable Z, and Variable Yn is inversely proportionally to variable Z. Function knowledge is labeled to the blob with text by description of the ACTOR function. The condition in the blob indicates the prerequisite necessary for setting up the function. It is a Boolean variable and is optional property in the blob. The basic blob is shown in Figure 24.

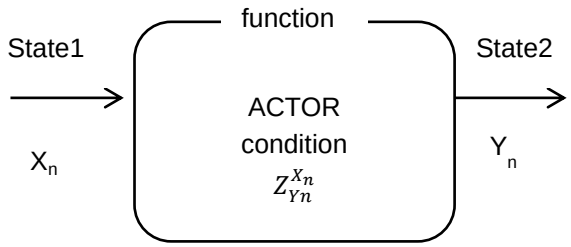


Figure 23. The basic blob in D-higraphs

Although the inventors of D-higraphs claim that D-higraphs is superior to MFM on the basis that D-higraphs integrate functional and structural information, so that the component to realize the related function can be directly refer to. The capability of linking structure information with functions in MFM is also potential, only with preference to formalization of representation to reach semantically consistence. The mapping of function patterns with a component is the key. The manner of linking structure and function in D-higraphs are realized by linguistic language, which obviously does not have to address the same problem. However, meanwhile it does not give insight of process system for designers and operators. In addition, the meaning is explained by linguistic language rather than a formalized modeling language itself.

Table 5. Comparison of D-higraphs and MFM

Method / **Complexity**	**D-higraphs**	**MFM**
Intentions	Implicitly indicated by functions	Explicitly represented as target (achievement or threat) with a round circle
Functions	Described by informal linguistic language	Semantic represented as symbols and a fixed set of functions abstracted from process system
Structures	Displayed in blob as ACTOR By informal linguistic language	In extended MFM, represented realisations of roles
Operations	Control loops are the blobs highlighted in orange colour to differentiate from process blobs. The means to control is explicitly represented	Described as control flow structure and with actuation, the controlled process variables are pointed out

Rodriguez et al.[104] used D-higraphs to perform HAZOP and compared the results obtained by MFM-based HAZOP by Rossing et al. [105] on the same pilot plant, the Indirect Vapor Recompression Distillation pilot Plant (IVaRDiP), at the Department of Chemical and Biochemical Engineering at the Technical University of Denmark (DTU). The results claimed that the D-higraphs HAZOP has a better clear and direct results linked to equipment. However, the study does not really compare the results from both methods for the same scenarios.

In addition to functional causal models, casual models without being placed in a given context include signed directed graphs (SDG), petri-net, layered directed graphs (LDG) are the methods to represent the process behaviour in a graph. However, the purpose of those models is to explore the causal relations among variables. Qualitative reasoning is also based on the variable states. So, these models do not address the problems of system abstraction in hierarchy levels and require prior knowledge. The priori knowledge that is needed for HAZOP studies is a set of failures and the relationship between the observations (symptoms) and the failures. Typical cases studies of HAZOP based on these models can be found in literatures.

In order to get a deeper insight into the difference between the casual models and functional models, we take MFM and SDG as example to compare. SDG model is a network connected by directive lines, also called branches, between nodes. Such node can represent a physical variable, or a kind of event. The influence relationship between SGD nodes with the qualitative way to express, namely each node to other related node is incremental impact or effect reduction. For general qualitative analysis, the state of the node commonly used one of the three states "+" and "-", "0". "+" represents physical variable beyond allowing upper limit, and “-“ represents under allowing lower limit, “0” represents variable is in normal range. Commonly used SGD modeling methods are: based on the mathematical model method and the experience knowledge. An example of SDG model of the regenerator section of FCCU is in Figure 25. The comparison of MFM and SDG models in Table 6.

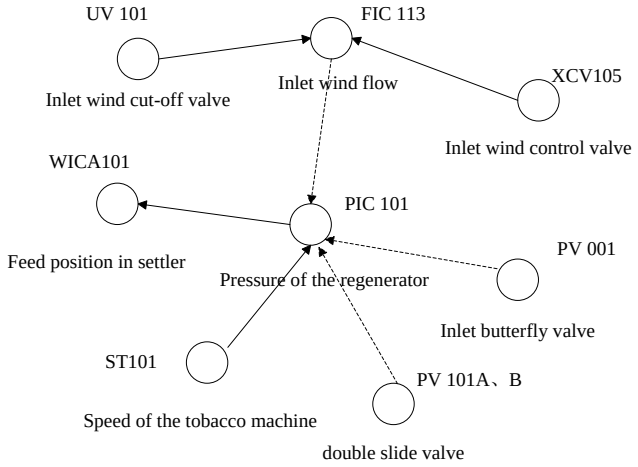


Figure 24. SDG for pressure of the regenerator section of FCCU

Table 6. Comparison of MFM model and SDG model

Property	MFM Model	SDG Model
Type of model	Functional model	Casual model
Type of structure	Network	Graph
Model start	G1	node
Model end	Undefined	Casual knowledge
Goals	Functional goals	Casual goals
Types of relations	Means-end	Cause-effect
Information type	Mass and Energy Flow and Control Information	Deviation influence lines

6.2.2 Computer aided methods for dealing with uncertainty in HAZOP

6.2.2.1. Empirical judgement of risk uncertainty

Risk evaluation of identified hazardous scenarios in HAZOP studies are commonly assessed by subjective judgement of HAZOP team based on their empirical knowledge and historical accident data. Since 1992, several tools have been promoted to give a perception of the loss such as risk matrix, analytic hierarchy process (AHP), risk priority number (RPN). The other specific tools applying for risk management such as facility risk review and uncertainty index can be found in literature [106-107].

Risk matrix can be in a qualitative or semi-quantitative information/knowledge. Two scales on the matrix describe increasing levels of consequence and frequency. Each cell of the matrix is a pair of consequence and frequency, representing a relative risk. However, explicit acceptance risk criteria [108] remains challenging and interesting which can influence the risk scenarios prioritizing process. The tolerable risk depends on the given context based on values of the society.

AHP is a tool developed by Saaty in 1980 that applies for setting priorities in complex, uncertain multi-criteria problems [109]. AHP is the process of dimension that depends on the judgments of professionals to come out with priority scales and pairwise comparisons [110]. According to Saaty, in order to overcome the complexity of the decision making process we need to classify all the unlike factors that influence the decision and put them in a hierarchy structure of homogenous cluster of factors. By comparing these factors in pairs a measurement ratio is obtained. Each factor is compared with the parent factor, which helps us to find the weight of each factor in the hierarchy. By the multiplication of the priority of one factor in each level for the priority of the factor with the parent factor, the weights throughout the hierarchy are obtained. AHP has the ability to synthesize and measure multitude of factors in a hierarchy, which can separate the abstract entity into its constituent element. For example, the hazards can be prioritized.

RPN is an index method proposed by Pillay and Wang [111] in 2003 for risk level assessment applied for FMEA originally, consisting of risk factors occurrence (O), severity(S) and detection (D). Occurrence represents the probability of failure occurrence, severity stands for the failure severity to the system, and detection represents the probability of a failure remains unknown (detectability). RPN is the multiplications of O, S and D. The more likely to happen, the more severe consequence and the more unlikely to detect, the bigger an index number will be assigned.

Some on-going research is carried out using these tools. Gilardi and Gotti[112] have developed a semi-quantitative HAZOP methodology estimating the risk level by using a risk matrix, accordingly, a correct number of barriers was chosen based on the risk level. This suggested a great effort should be exerted to reach an advanced control of risks. Marín[113] developed a local approach called PEMEX based on risk matrix principles for Mexican oil and gas industry and defined risk criteria explicitly for easy use. The risk ranking is made with consideration of safeguards. It can be interpreted as residual risk ranking, where risk remaining after protective measures has been taken. In this way, it is more meaningful for management to make decisions to act on the urgent high risky scenarios.

Othman et al. [114] incorporated a multi-criteria decision-making approach, AHP to prioritize the hazards that may contribute to the undesirable events identified from the HAZOP analysis. The weight assigned to causes and consequences are based on the pair comparison of relative preferable importance of causes rather than likelihood of causes or severity of consequences, so the selected prioritized hazards may not really be the ones that should be paid attention to. However, such thinking is certainly useful for prioritizing any action to plant modification, retrofitting, or construction within the available resources constraints [115].

In 2006, Guimaraes and Lapa [116] have integrated RPN into HAZOP to prioritize of hazards, called as HAZOP$_{\text{-rpn}}$. Additionally, with fuzzy linguistics approach to advance the HAZOP$_{\text{_rnp}}$ by Ilangkumaran and Thamizhselvan [117] to distinguish between the rankings for those hazards with same value of RPN.

6.2.2.2. Dynamic simulation

In the past 40 years, much research effort has been dedicated to the development of dynamic analysis. The dynamic analysis approach for a HAZOP seems the most straightforward procedure which gives quantitative results. The dynamic simulation studies prior to the HAZOP meetings improve the accuracy of the outcome recommendations, reduce the time needed to carry out safety analysis by better focusing the HAZOP meetings, improve design of the process and the possibility for onsite analysis of design changes in view of process safety[118]. Dynamic simulation can serve as a tool [119] for exploring and unfolding the uncertainty in HAZOP in following ways to increase speed, efficiency and reliability:

1. After screening the hazards by different empirical judgement methods, HAZOP team leader may engage a specialist to adopt dynamic simulation to give it more quantitative character for investigating and demonstrating the consequences of deviations from normal operating conditions. Especially, for complex and nonlinear systems, the use of dynamic simulation using deterministic models [120] can be helpful in assessing the effect of faults on the operations and dynamics of the process. In addition, some changes of parameters are more sensitive than others to the effect, there is a need to use sensitivity analysis also called as uncertainty analysis by using dynamic simulation. Multiplicity of steady states in chemical reactions is another situation that requires simulation, where system may have multiple stable steady or dynamic states.

The principle of sensitivity evaluation is to assess factors change in input the influence degree on the output. The bigger influence of certain factors in input, the more sensitive factors they are, where they are called as sensitive factors. Other less influencing factors are called non-sensitive factors. In HAZOP, this principle is applied to analyse the influence sensitivity of multiple causes for the same deviation to the process variable in the deviation. The bigger sensitive value of the cause is, the more priority of the cause is given. For ranking multiple causes for the same deviation in HAZOP, Kang and Guo[121] introduced an approach based on sensitivity evaluation to provide assisting in operator's decision for online fault diagnosis. Dynamic simulation model was established to monitor the dynamic effect of deviation cause on target process variable. The sensitivity value was calculated by departure degree multiplied by correction coefficient. Departure degree is equal to the ratio of the difference of maximum value of the deviation caused by the cause between the normal value of the target process variable divided by the difference of upper and lower alarm threshold of the target process variable. The correction coefficient considers the factors of time and stability degree of the target process variable. The sensitivity analysis algorithm was applied to a depropanization unit in a gas fractionation

plant. For ranking the consequences of the failure scenarios, Rasmussen [122] used sensitivity analysis. The sensitivity value [123] was calculated by the ratio that the difference between the normal operation value at a given position and time in the process and the failure scenario value at the same position and time divided by the difference of input process parameter vector. It applied for an offshore gas re-injection process. The most critical failure scenario was found to be the re-injection control valve failed closed resulting in a pressure peak above design values at the compressor and pressure build-up at gas feed inlet.

2. Generate and quantify the deviation to determine the effect of operational disturbances on the safety of the plant and advise ways to reduce the risk of the consequences. For example, a liquid may become gas upon heating to the boiling point, resulting in an abrupt change in volume. It commonly happens with liquefied material stored under pressure leading to phase transition. Such critical deviation should be paid more attention by considering quantitative information.

Li et al. [124] evaluated the consequences of hazard deviations and the efficiency of the proposed safety barriers in the context of HAZOP. The most efficient barrier to avoid producing an overheating of the reactor was found out by simulation. Isimite and Rubini [125] reported using a dynamic model of the sequence of events aiming at repeating the Texas City refinery explosion, however, an alternative pathway for the sequence of events leading to the accident was found.

3. Explore the effects of a counter action by introducing the information generated by a numerical simulation, which can facilitate to explain afterwards qualitatively.

Gofugu and Kondo [126] introduced the information generated by a numerical simulation to quantitatively explain the effects of a counter action. The applicability of the technique was examined by applying it to an oil refinery plant.

4. Find out time issues such as response time, safety reaction time, time of occurrence, and process safety time. Response time represents the time between detection of the event and response of the system. Safety reaction time stands for the time needed to detect a problem and initiate a safety shut down to the control element. Process safety time means the operating time before the detection of unsafe situations to avoid the development of these into a disaster. Some process behaviour is very critical, such as thermal runaway effect. It requires runaway effects investigation methods to detect such effect and avoid structural losses.

Several researchers are following this line. To avoid potential hazardous conditions during the transportation phase, Varga and Abonyi [127] used a dynamical analysis of an exothermic system allows determining possible necessary safety actions based on a method to design the process safety time. Svandova et al. [128] demonstrated that the dynamic simulation can provide an answer to the time response of a reactor to the generated deviations. What is more, it is possible to study also the influence of deviation duration on the reactor performance.

6.2.2.3. Bayesian Network

Bayesian Network proposes a systematic way of combining knowledge – prior information – and data in order to eliminate uncertainties from objective probability and update probabilities when new evidence, new data – prior data – or new information becomes available. Prior information is the

information that one can obtain from expert judgment, technical knowledge, producer information, and data from similar cases in the past. The probability of causes identified in HAZOP given by a process variable deviation can be calculated by Bayesian Network with consideration of observations. The BN technique for industrial processes - Gas, Oil and Chemicals assessing and avoiding Low-Probability, High-Consequence Events was reviewed [129]. More case studies can be found in research by Yao et al.,[130] Hu et al[131-132], Reitz et al[133], Unnikrishnan et al.[134], Wang et al.[135].

6.2.3 Computer aided methods for dealing with vagueness in HAZOP

Fuzzy set is a “zero to one” state set which has a variety of states. An element belongs to one state in the set with certain degree which is defined by a membership function. Comparing with a classical set, the fuzzy set eliminates the concept of “not belong to”, by contrast, it generates a possibility distribution curve for determining the degree of the element belongs to a state in the set, providing a status between in-set and not-in-set as the smooth transferring status. In another word, the “not belong to” is a special case that the element is with sharp zero degree. The fuzzy set in HAZOP can either be deviation cause, deviation consequence, and the risk of the failure scenario for a deviation. The states in these fuzzy sets are normally qualitatively described with different scales, e.g, low low, low, normal, high, high high. Recent research demonstrated fuzzy set theory [136] can handle the inherent vagueness of linguistic description for the HAZOP. This direction of HAZOP research is still rather rarely available in published papers.

Tao et al. [137] used fuzzy set theory to calculate the possibilities of deviation and consequence quantitatively, rather than to express the degree of the element features. Most recent research by Kuchta et al. [138] proposed fuzzy HAZOP method to look at the parameters features which is capable to identify all situations. Luis et al. [139] used fuzzy number and linguistic terms to evaluate risk. Also Ahn et al. demonstrated that the fuzzy set theory is more suitable for distinguishing the element located in the transitional ranges [140].Review of fuzzy set theory applications in safety assessment for marine and offshore industries can be found[141].

6.2.4 Computer aided methods for improving efficiency of HAZOP

It is widely accepted that HAZOP is time-consuming, laborious and costing. As summarized previously there are two questions: How long time to devote for a HAZOP study is the most beneficial and in which way the HAZOP study can be speeded up under the certain devoted time. The following section will be directed into two sub-sections to review possible answers to the two questions.

6.2.4.1 Time estimation for HAZOP study.

Chemical Industries Association in 1990 and Center for Chemical Process Safety (AIChE) in 1992 have proposed models for HAZOP study time estimation. Their models are based on the qualitative assessment of experts’ experience and the objective of study. The estimated time result comparing with real time consumed is 60-70% accurate. Obviously, there is a big gap to meet the demanded accuracy based on improved models.

In 1992, the first attempt to assess how long and how many hours a HAZOP study entails made by Freeman et al.[142] The equations used to represent the relations of factors contributing to operational

time are based on the number of major equipment items to be analyzed, the system's complexity and the skill level of the HAZOP team leader. The time to complete a first draft HAZOP report is comprised of 3 durations: preparation time, sessions' time and writing time. Each duration at first is counted by hours. The preparation time is defined in terms of number of P&ID, and P&ID complexity. Because a skilled leader will definitely reduce the needed time and enhance the effectiveness of the study, the sessions' time only consider the team leader experience as well as the number of P&IDs, and P&IDs complexity. The writing time is based on the preparation time. Finally, each duration is converted into weeks and then they are summed up to obtain the total time. Khan [143] claimed that there are some deficiencies in the model. First, the writing draft report duration is as 50% of the team's leader's preparation time. However, the activities of other team members should also count. Second, the model does not consider any cushion to cover uncertainty or delay, which will lead to underestimation of time. Third, the model converts each duration in weeks and then adds to get the total, which may deviate the final result to be lower than that of actual duration in weeks. Fourth, most of the equations adopted in the model are empirical (single variable) in nature. However, the accuracy of the HAZOP duration estimated by Freeman's model improved comparing with CIA and AIChE, with accuracy of 75%-85% for typical chemical industries.

In order to overcome the drawbacks of Freeman's model, Khan put forward a modified model. Besides the 3 durations, the delay time is added to compensate the time due to non-availability of member, documents or any other crucial items, and individuals responding time. The delay time is categorized into two groups: one is delay in schedule of preparation and discussion which is estimated as 15% of the preparation time and the other is delay in preparation of final report from rough draft which is predicted as 25% of the draft report writing time. The total estimated time firstly calculated in hours and then coverts it into number of weeks through analytical equation. Thus, the chance of uncertainty reduces. Additionally, the quantification of team leader's time in meeting is proportional to skill factor (Novice, moderately experienced, experienced, highly experienced) which is based on the different organization and references. Furthermore, the model takes into account team leader as well as team member preparation time. The model uses multivariable empirical equations instead of single variable equations. With different scales (simple, standard, complex) of case studies, all of estimated results produced by Khan's model is closer to real time than that of Freeman's model. What is more, interestingly to find the higher complexity of the studied system, the closer of the Khan's model to actual results than Freeman's. Therefore, it demonstrated that the additional features embedded in Khan's model gives ability to produce higher accuracy, around 85%-95%.

However, in Khan's model, there are still some uncertainties, such as indicators of complexity of system, subjective experiences. To better select criteria for those uncertainties, a new model based on Nodes Selection Methodology (NSM) and the Deviations Structural Hierarchy (DSH) is proposed by Dunjó et al. in continues chemical process[144] The composition of the total time required to conduct a HAZOP is the same as Freeman's. The number of pieces of major equipment present in the processes (ME), and the number of P&IDs required to define the process are used as two indicators to evaluate the complexity of the process. Based on 5 conducted HAZOP, the key parameters of each duration and the two indicators, least-square models are applied to establish an equation for preparation time. The writing time estimation again based the previous work of Freeman et al. and Khan et al., it is deemed that it is 40% of preparation time. For the important part of sessions' time, tentatively, based on the NSM, the sessions time is calculated by assuming that the deviation examination of nodes following DSH method which is more straightforward by following the procedure. Because HAZOP time-estimation model depends on how the sessions were brainstormed. As Dunjó argued that the

DSH method has two advantages. First, two sets of deviations (one for reviewing process nodes and the other for analyzing the global node) encourage team members to brainstorm for any specific departure from the design intent. Second, DSH establishes the order of application for deviations to avoid repetitive analysis, yet structure hazard identification without losing freedom for creative thinking. The estimation time obtained by the model is with a 95% level of confidence. However, it did not give comparison results with Freeman's and Khan's.

6.2.4.2 Tools of Assisting HAZOP

As indicated by the literature review presented by Dunjó et al. (2010), approximately 40 % of HAZOP-related research is focused on HAZOP automation. Some computer-aiding applied to HAZOP reviewed by Rushton [145] and a brief overview is made by Lees [146]. In principle, it is commonly agreed that it is impossible to completely eliminate the presence of a human expert team in the HAZOP execution process, but there are several attempts to create a robust support tool that is able to automate some of the procedures necessary to perform a HAZOP study. Zhao argued that the difficulties of fully automating HAZOP by computer lie in the fact that the highly flexible reasoning mechanism and knowledge structure of human experts cannot be effectively simulated by computer systems. In addition, it is problematic to assume we ever be possible to obtain complete knowledge.

Besides the available documentation tools which provided workflow support for HAZOP analysis, such as PHAWorks, and PHAPro, there are two basic approaches in HAZOP automation experts system with reasoning capabilities: shallow knowledge based and model based. Shallow knowledge-based approach uses large knowledge databases containing information about the failure mode, causes and consequences of various process units and/or pieces of equipment. Typical knowledge-based experts systems are e.g. projects of OptHAZOP[147], TOPHAZOP[148] and EXPERTOP[149] by Khan and Abbasi, ExpHAZOP+[150] by Rahman et al.. Typical model-based experts systems are e.g. HAZOPExpert[151], a HAZOP automation tool developed by Venkatasubramanian and Vaidhyanathan, PHAsuite[152-153] and PetroHAZOP[154] by Zhao et al., HAZID[155-159] by McCoy et al. These automation HAZOP tools are selected to review because they are representative with qualitative and quantitative features in the tool. And some of their application industries are more relevant with offshore oil and gas. More details of each representative tool are illustrated below. Finally, a new trend of computer aided HAZOP expert system integrated with smart plant P&ID was stressed, since it is also our intention to follow the lines.

6.2.4.2.1. Shallow Knowledge based experts system.

(1)OptHAZOP

Khan argued that the repetitive nature of steps in the procedure to perform a HAZOP study inevitably generates a feeling of drudgery and mental fatigue, even exhaustion. For improving effectiveness of HAZOP, they proposed named optHAZOP procedure in 1997 [160] shown in Figure 26 to produce reliability of results as well as save time. The procedure used an expert knowledge-base. The knowledge base is a large collection of facts, rules and information regarding various components of process plant. Along with the use of knowledge it also suggests a few recommendations to reduce the time with better solutions. The OptHAZOP saved more 45% total HAZOP study time and significantly reducing the requirement of HAZOP team members, which resulted in less costs as well as margins of error.

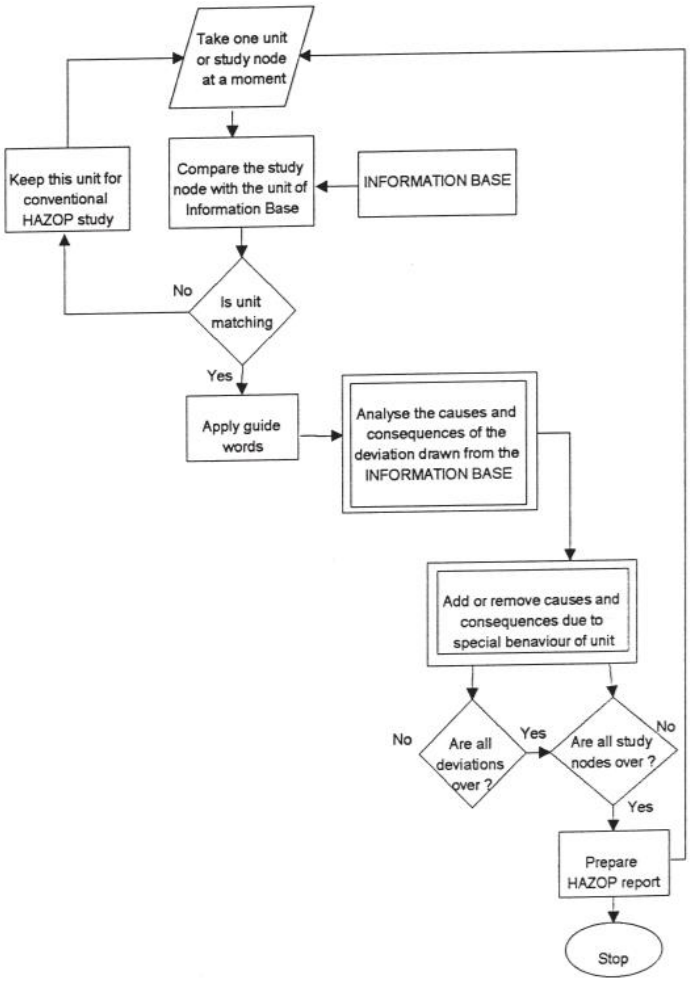


Figure 25. Algoithm for optHAZOP procedure [161]

In 2005, based on the OptHAZOP, Khan [162] proposed a knowledge-based HAZOP expert system for offshore process operation shown in Figure 27. It was unique in because the knowledge base includes the offshore process operation system and their failure scenarios and fault propagation. The knowledge base is object-oriented which include four main features: general process causes, general process consequences, process specific causes, and process specific consequences. The inference engine is rule network based. A case study of expert system application for HAZOP of a FPSO (Floating Production Storage and Offloading) process is illustrated in the paper. It concluded that the work was completed by 10 people in one week without any loss of accuracy or precision.

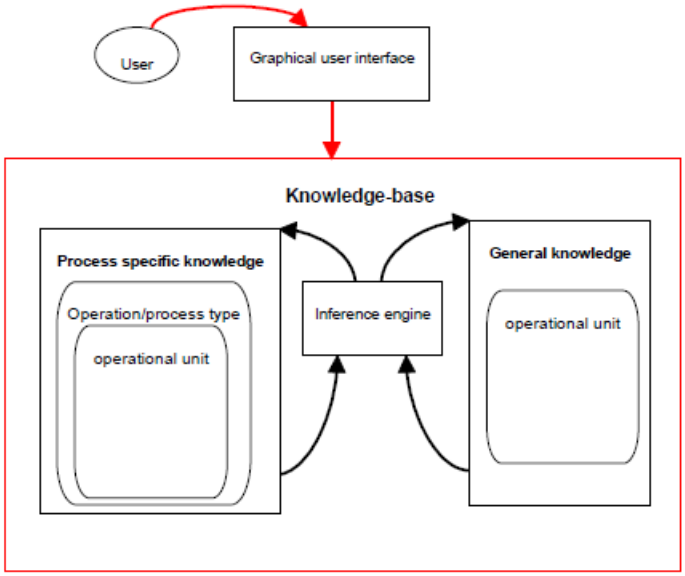


Figure 26. The architecture of the knowledge base expert system extracted from Khan [162]

(2)TOPHAZOP

In order to speed up the work of HAZOP team and reduce the requirement of manpower, in 1997, Khan developed TOPHAZOP (Tool for Optimizing HAZOP) to meet the objective. The knowledge base was implemented in terms of frame structure and rule networks. The knowledge base was classified into process specific knowledge and general knowledge. The process-specific knowledge has been classified in two main groups: objects (15 process units) and its attributes, causes and consequences. The objects are developed in framework structure with attributes while causes and consequences are developed in rule networks attached to the framework. The causes and consequences for a particular object are invoked by the forward chaining technique, while verification (justification) of results is done by backward chaining. The general knowledge was developed in the same way, except that there are no attributes attached to the objects. The working mechanism of inference engine is represented in Figure 28. The TOPHAZOP was applied to a LPG plant. The recorded time for performing HAZOP study with TOPHAZOP only took 3 hours include tasks of formulating problems as well as running TOPHAZOP, and another 1.5 hours to interpret the results. The results obtained can be comparable with manual conventional HAZOP; however, the comparison did not really show in the work.

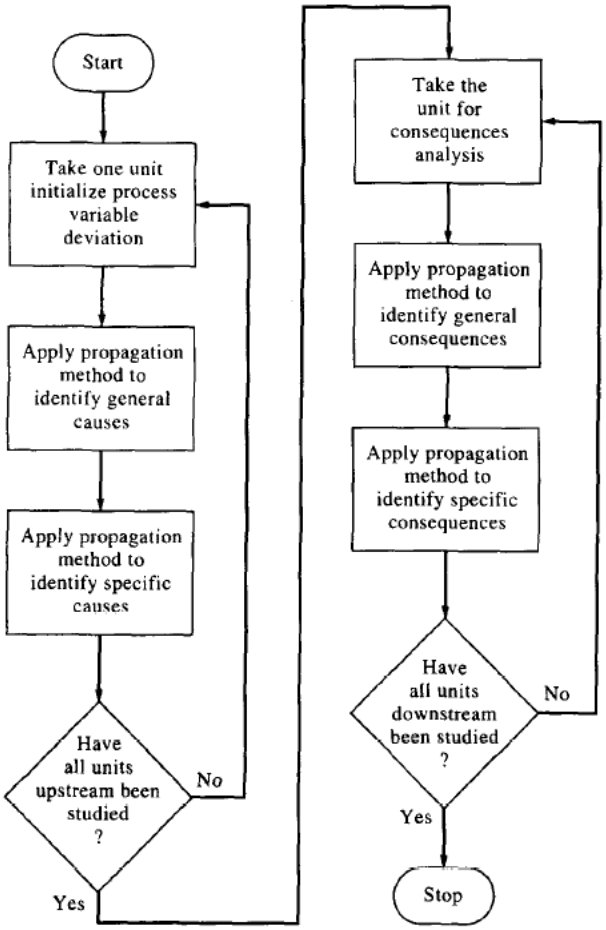


Figure 27. The TOPHAZOP inference engine

(3)EXPERTOP

In 2000, Khan and Abbasi, in order to explore advantage and utilize the good features of optHAZOP, EXPERTOP (EXPERT system for HAZOP study) was proposed. The main differences from TOPHAZOP were that the process units were expanded to 20 different types and for each deviation analysis, the remark was added to label the scenario hazardous scale. The Application of EXPERTOP was in completing a HAZOP study for a process of poly ethylene terephthalate manufacture. The whole study only took for two people in two days.

(4) ExpHAZOP+

ExpHAZOP+ embraced the core idea of optHAZOP developed by Rahman et al. in 2009, which is in tentative to apply in offshore oil and gas industries in terms of offshore HAZOP knowledge-base.

Its architecture consisted of a graphical user interface (GUI), a knowledge-base and an inference engine. The GUI is the platform where users can draw P&ID using existing defined equipment or add

new equipment by inputting the equipment graphically together with the process variables, deviations, their causes and consequences.

The knowledge-base includes information collected from previous practical industrial HAZOP studies of offshore oil and gas process systems, related to process operations, process equipment, operating problems, failure modes, failure frequencies as well as corrective actions. It is interesting to see that in the definition of consequence in knowledge-base which is considered a function of the process type, the process condition and the chemical in use with the observation that causes of an equipment failure does not vary much from different facilities. The knowledge-base has 19 different pieces of equipment as follows: absorber, air-cooled exchanger, blower, compact heat exchanger, centrifuge, compressor, cyclone, distillation column, dust collector, electrostatic precipitator, extractor, filter, heat exchanger, piping, pump, reactor, temperature sensor, temperature controller, and valve. The process-general knowledge and process specific knowledge is similar to TOPHAZOP.

The inference engine is more sophisticated compared to TOPHAZOP, with a fault propagation algorithm assumed that faults can propagate through pipelines that are connected to the pieces of equipment. The fault propagation algorithms allow to find the deviation for the identified fault to all downstream equipment by combining both forward and backward search techniques.

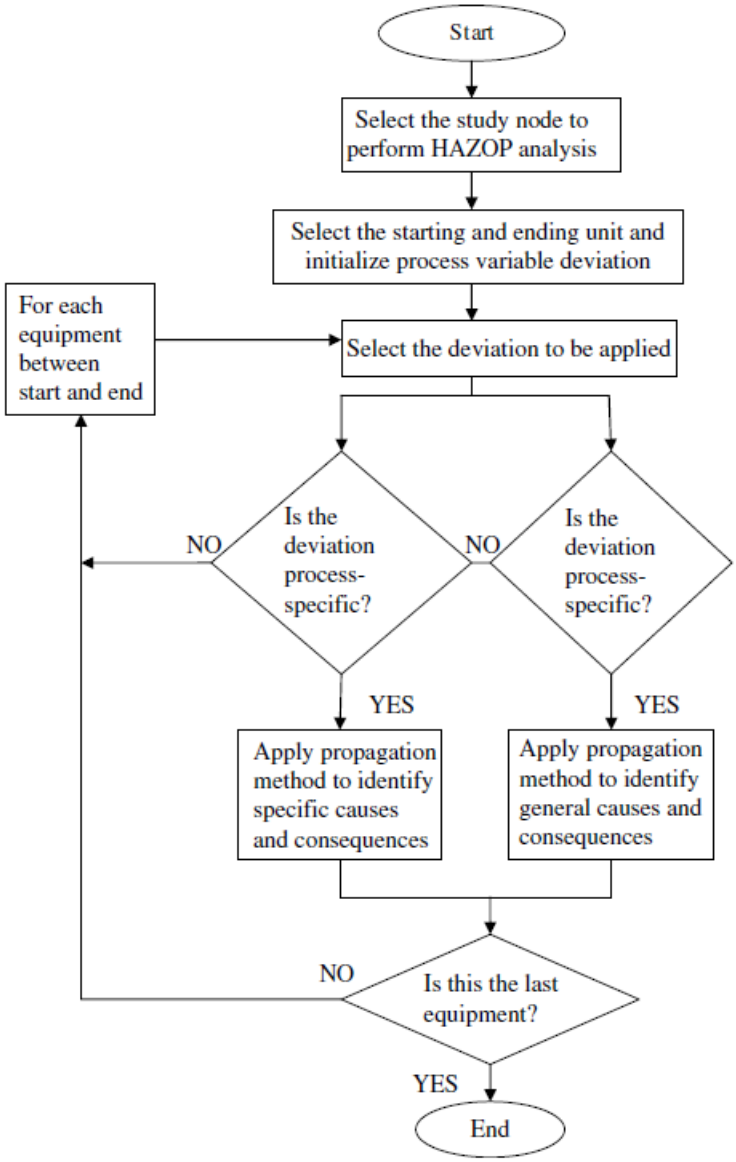


Figure 28. Fault propagation algorithm for ExpHAZOP+[150]

The results of causes of supplying hot nitric acid to the reactor in a nitric acid cooling facility were the same with comparison with analysis in Lapp and Powers[163] and Wang[164] used FTA for the same case, although it is qualitative assessment.

6.2.4.2.2. Model-based experts system.

(1)HAZOPExpert

HAZOPExpert divided the knowledge required to perform HAZOP analysis into process-specific and process general knowledge, and use generic HAZOP models of process units shown in Figure 23. The process-specific knowledge consists of information about the materials used in the process, their

properties and P&ID of the plant. The process general knowledge consists of the HAZOP-Digraph models (HDG)[165] which in nature is based on a modified Signed directed graph (SDG) of the process units by adding abnormal cause nodes and adverse consequence nodes which are qualitative causal models developed specifically for hazard identification. The models were produced based on the steady state material and energy balances and confluence equations [166]. The HAZOPExpert model library has the generic HDG models for 15 process units such as pump, tank, surge drum, heat exchanger, condenser, accumulator, reboiler, stripper, controller, valves, pipe, etc. One example is shown in Figure 30. The user can develop and add the HDG model of a new process unit to HAZOPExpert model library using the graphical HDG Model Builder facility in the system. Also, experience-based cause and consequence knowledge of the experts can be added to the existing HDG models. However, there are some deficiencies of HDG model because it is in nature based on a modified SDG. SDG represents causal interrelations of process variables. It may result in previously mentioned modeling uncertainty and is not able to be helpful for improving completeness of HAZOP.

It was claimed that HAZOPExpert found more number of causes and consequences than those recorded by the study team. This is partly due to the thorough nature of the analysis performed by the HAZOPExpert system. However the main reason for this is the strict qualitative reasoning approach for the analysis implemented in HAZOPExpert. Though HAZOP analysis is a qualitative approach, the experts in the study team filter their initial results using additional quantitative information in the form of the design specifications and normal operating conditions of the process units, and the quantitative properties of the process materials. Using this additional quantitative knowledge, the HAZOP team decides whether a process variable deviation will actually lead to the predicted hazardous consequences. Therefore, later on, a methodology was proposed for filtering the minor or unrealistic consequences found by the HAZOPExpert system using quantitative design and operating conditions specifications of the process units and the quantitative process material property values[167] . To realize it, the process specific knowledge in HAZOPExpert was modified to incorporate the additional knowledge and the inference engine was also augmented to allow using the quantitative knowledge to prune unrealistic consequences. Finally, the consequences were automatically ranked based on four severity levels of the hazards.

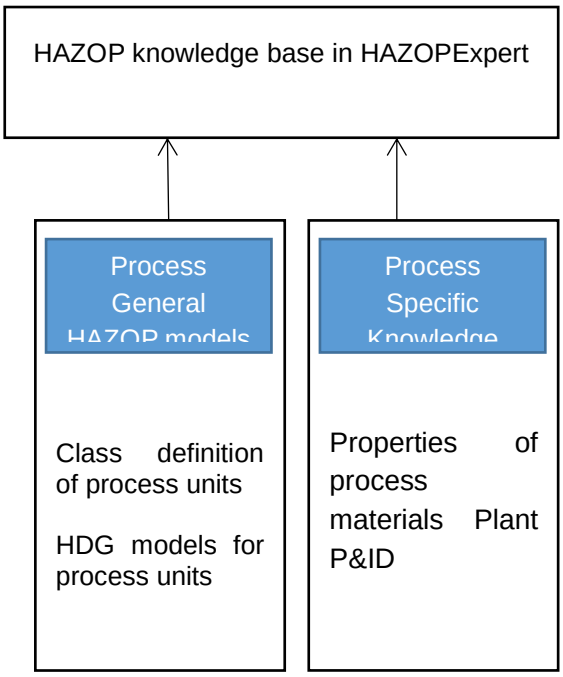


Figure 29. HAZOP knowledge base in HAZOPExpert[151]

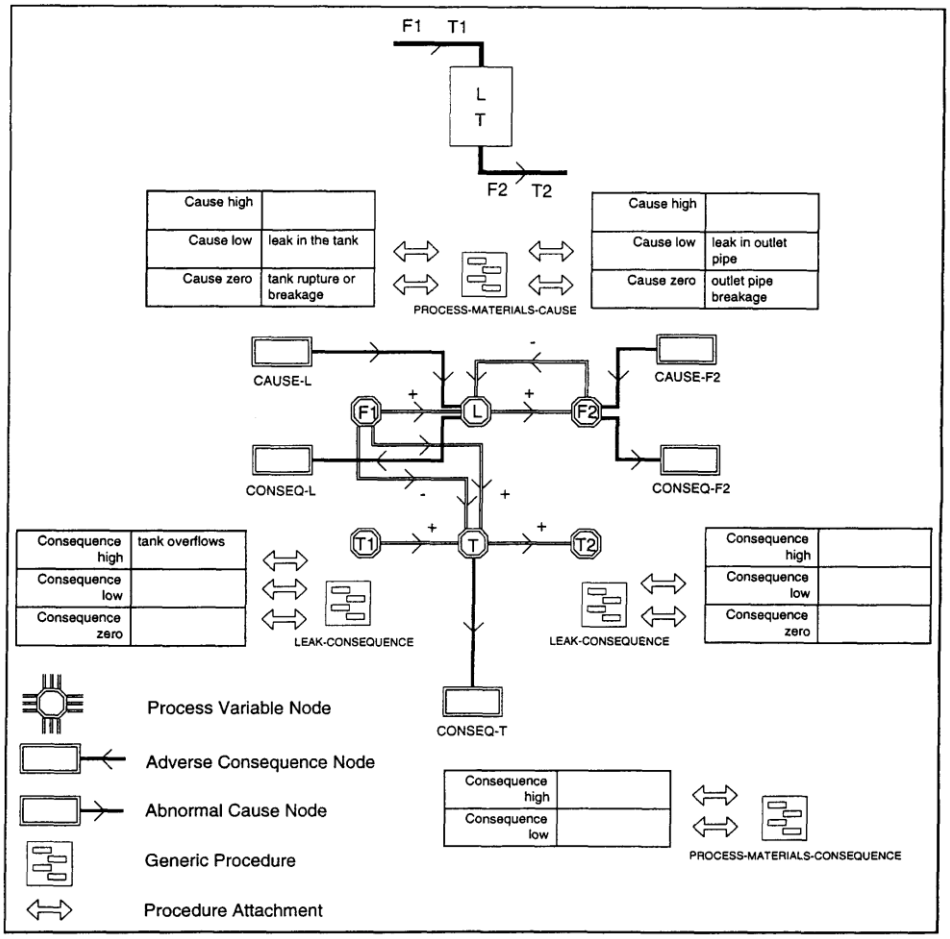


Figure 30. HDG model of a tank[151]

Later in 1997, Srinivasan et al.[168-169], integrated a dynamic model invented by Dimitriadis et al. [170]for representing a state-transition of the system to give a detailed analysis of some scenarios possible to lead to high adverse consequence into the integrated framework, after where the qualitative analysis is performed using HAZOPExpert. The purpose of such framework was to eliminate the ambiguity suffered by qualitative analysis, because quantitative analysis indicated if a hazard is realizable to be beyond the safety limit of the process parameter. Also, the quantitative approach takes into account all possible combinations of inputs which can lead the process to an unsafe state. Thus, multiple faults leading to hazards can be automatically detected, which compensated the disadvantage of a conventional HAZOP practically only considering one single fault scenario at a time.

(2) PHAsuite

PHAsutie was developed by Zhao et al. in 2005. The main features of the tool for automated HAZOP analysis are: 1. Based on ontologies, the information sharing scheme was developed to share process information and results with other systems. 2. Coloured Petri Nets was adopted for representing chemical processes knowledge and used for HAZOP analysis. 3. The operation level and equipment level abstraction of the process was bridged by functional representation. 4. The reasoning technique was used for knowledge management is Case-based reasoning.

PHASuite has been applied to a few industrial chemical processes for performing HAZOP analysis. It approved that the results coverage produced by PHASuite is 80% of that by manual HAZOP obtained by HAZOP team. However, with the help of PHASuite, about 50% time was saved.

(3) HAZID

HAZID initially was intended to screen plant designs prior to their submission to a conventional HAZOP study. The propagation of faults through the plant is described in terms of qualitative modeling called signed directed graph. HAZID uses each model of individual equipment to be connected together as a network of the whole plant to assist in search for possible causes and consequences by linking.

HAZID is comprised of 5 modules: AutoHAZID, Graphical Tool and the Graphical Configuration Tool, Application Programming Interface, the Unit Model Application Tool and the Physical Properties Link. AutoHAZID is the core module with functions of decomposition system, qualitative modeling of process units, generation of scenarios by an inference engine, using fluid model to differ feasible scenarios from infeasible ones, rules for detecting plant configuration problems, HAZOP worksheets output, defining new unit models. The Graphical Tool and the Graphical Configuration Tool allows users to use or create/modify visual icons to draw simplified engineering line diagrams as plant descriptions. The plant descriptions are saved in Application Programming Interface for retrieving later by AutoHAZID. The Unit Model Application Tool is for creating and saving qualitative SDG models of equipment items. The Physical Properties Link allows various calculations of physical properties to be carried out in external software package.

The searching mechanism for causes and consequences for a deviation implemented in HAZID only allows for local consequence but both for local and distant causes, which is a big deficiency for satisfying completeness of HAZOP. And the selection right for showing the analysis was given to user. Zhao pointed out the percentage of scenarios identified by conventional HAZOP also identified by HAZID ranged from 33% to 60%, and the percentage of scenarios identified by HAZID which were judged to be corrected ranged from 33% to 83%. Moreover, the percentage of scenarios identified by HAZID which were judged to be correct and of interest was much lower, ranging from 9.5% to 29%.

(4) PetroHAZOP

In 2009, to overcome low completeness and correctness problem of results produced by HAZID, Zhao et al., developed a new learning HAZOP expert system called PetroHAZOP based on the integration of case-based reasoning (CBR) and ontology that help automate “routine” as well as “ non-routine” HAZOP analysis. Because it argued that the capability of knowledge representation by the existing unit models in HAZID was not able to include the knowledge for doing “ non-routine” HAZOP analysis, whose aiming at analyzing deviations generated by guidewords “other than”, “as well as” and “part of”.

To improve the ability of machine learning, six ontologies: process ontology, process unit ontology, unit operation ontology, equipment ontology, material ontology and HAZOP ontology were integrated with CBR for reasoning. The workflow of PetroHAZOP is shown in Figure 32.

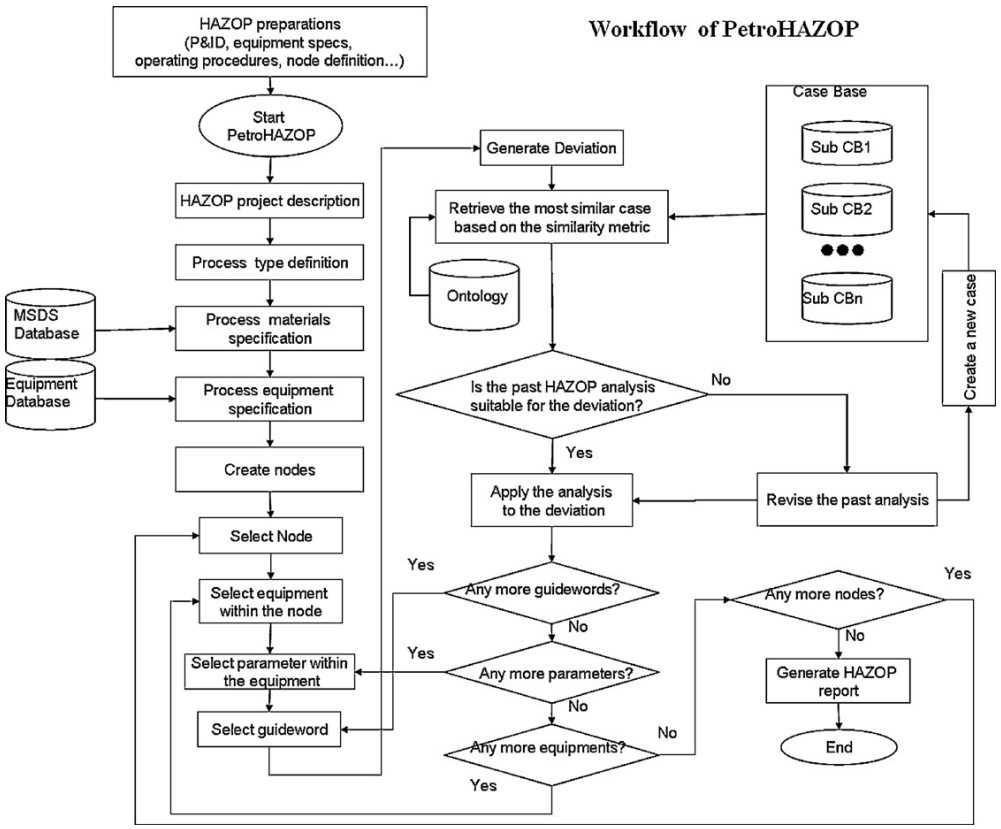


Figure 31. Workflow of PetroHAZOP [154]

6.2.4.2.3 New development.

HAZOP studies is a part of safety review analysis in process design stage. As pointed out earlier, the study should take place as soon as the PFD and the P&ID are ready but also before the detailed design starts. To facilitate this analysis the integration of the system performing the HAZOP and the tool used to implement the P&ID would be advantageous. It would save time and will always use the most recent and updated diagrams. Cui et al. (2010) showed the integration between the commercial process design package Smart Plant P&ID (SPPID) with their expert system named LDGHAZOP, which uses a layered digraph model of the process. It improved the efficiency for LDG model building.

Rodriguez et al. also worked on the integration of the D-higraph HAZOP assistant with the simulation environment Aspen Plus. The available P&I representation of the process is translated to an Aspen Plus model. Then, this steady state model is converted to a dynamic model (Aspen Dynamics or Aspen Custom Modeler) which is the structural representation of the process. Such integration improved the efficiency for generation of quantitative simulation models for HAZOP analysis.

As a part of HAZID system, a tool invented by Loughborough University [171] related to maintenance work can realize two functions for safe isolation: calculate the boundary for maintenance by searching in P&ID to identify the boundary for given specific equipment to be maintained needs to be closed off, and HAZOP study related to the associated isolation tasks. It helped with the efficiency for HAZOP analysis from the maintenance safety point of view.

Therefore, the integration with other tools to facilitate capturing knowledge of process structure or

converted into models in quantitative simulation environment is a new trend of computer-aided methods for improving efficiency of HAZOP.

6.2.5 Computer aided methods for improving completeness of HAZOP

Completeness is a function of the quality of features. As discussed in completeness challenge of HAZOP section, the incompleteness resources may come from an inherent method limitation, not in scope of work, not enough time or budget, limited expertise or industry state of knowledge, inappropriate PHA method, outdated or inaccurate P&ID, ignored incident history-plant, company or industry, non-independent safeguard , not maintained safeguard, analysis mistake, incorrect safe operating limits, neglected human factors , external factors like fire or earthquake, not have process safety information or mechanical integrity(MI)data, non-routine operating modes such as startup and shutdown, valid guide word, not consider key process variable. Therefore all the methods to reduce the effect of above resources can contribute to improve completeness of HAZOP. Those methods already discussed in tackling with other challenges in HAZOP.

7 DISCUSSION AND PERSPECTIVES

Part I of the report has introduced HAZOP techniques and their practice in oil and gas industry. To find out the benefit of qualitative and quantitative models to improve HAZOP, the challenges of HAZOP and computer-aided methods to overcome the challenges are reviewed. This section is to again emphasize on several viewpoints.

7.1 Discussion and perspectives of HAZOP Technique

1. **Bridge the gap between designers and operators.** HAZOP provides an opportunity for designers, operators, managers to sit together and discuss potential hazards and operability problems of the target system. It is a safety analysis tool [172] to bridge the gap of understanding the process system among them. Therefore, the brainstorming meeting carried out by the HAZOP team should not be replaced, although qualitative and quantitative models, dynamic simulations can reduce the subjectivity aspects of HAZOP analysis.

2. **Integration with other PHA methods.** To make full use of limited resources, HAZOP can be improved and executed at the same time with other PHA techniques, especially with Layers of Protection Analysis (LOPA). Time and cost can be saved by combination of HAZOP team and LOPA team efforts from different perspectives, the LOPA can be helpful to find out the barrier layers concerning safety to lower the risk to acceptable levels and to fill in the safeguard column in a HAZOP worksheet. Some research already starts to look into how HAZOP and LOPA can be combined efficiently for an offshore platform [173].

7.2 Discussion and perspectives of HAZOP Practice in Oil and Gas Industry

1. **Safety life cycle of a plant should be properly re-defined and be in place.** Typical safety life cycle (SLC) generally refers as a concept for optimizing the design of a safety instrumented system (SIS). The safety life cycle concept should be broader than the typical concept in terms of time scale and systems covered in a plant. The time scale means the duration of data collected for hazards analysis in different phases of a plant development varies, and the hazards analysis activities is supposed not only cover the first PHA of a plant but also the later production process after changes in technological process, equipment, safety requirements, operating procedures, personnel, organization structures. The systems should not only include the SIS, but also extend to the engineered safety systems. Management of adverse situations in a system consists essentially in ensuring a limited number of safety functions (example: maintaining the sub-criticality, etc.) which are the final ends of the plant management, by making use of some engineered safety systems, which are the means dedicated to these objectives. Therefore, Extended SLC (E-SLC) needs to be proposed to distinguish

the traditional SLC. The E-SLC is the series of phases for system safety process (SSP) in a safety-critical system (SCS) from initiation and specifications of safety requirements, covering design and development of safety features, and ending in decommissioning of that system. Safety-critical systems [174] are those systems whose failure could result in loss of life, significant property damage, or damage to the environment, which can be a process system. To better frame the SSP in the context of E-SLC of a process system, the suggested procedure of SSP is proposed. Process hazard analysis should be carried out in different stages of E-SLC.

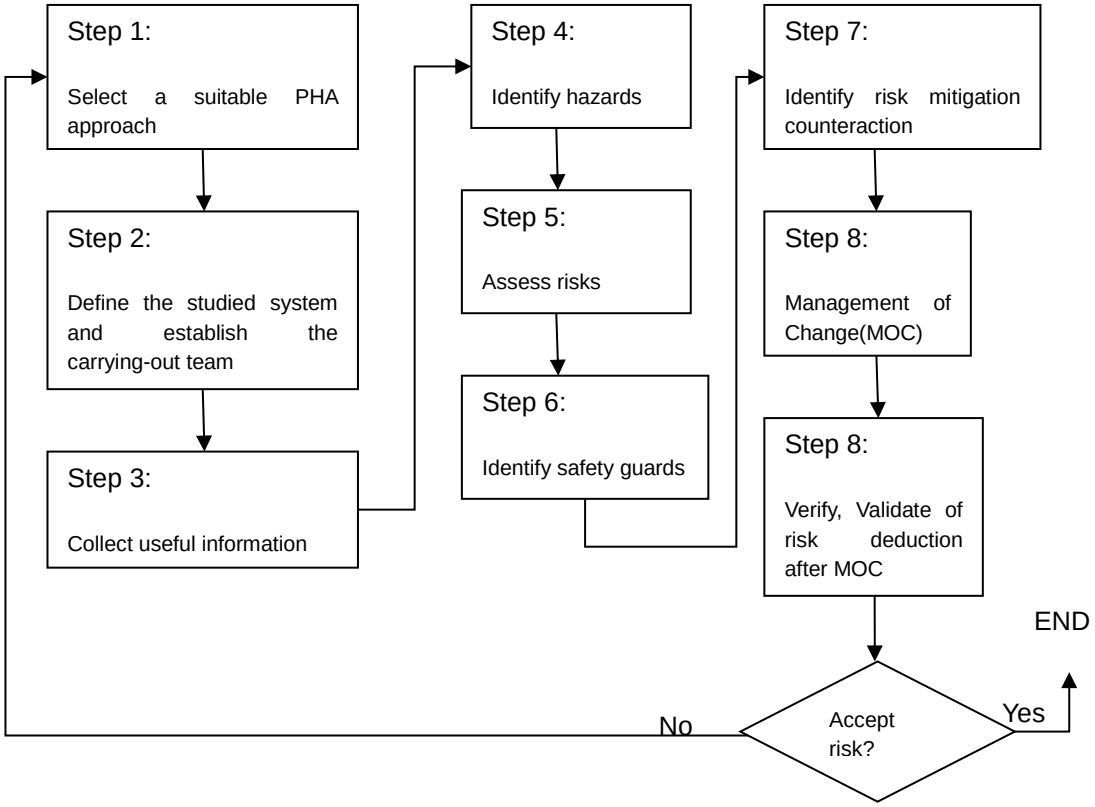


Figure 32. The procedure of SSP in the context of E-SLC of a process system

2. Update HAZOPs when process knowledge changes in a plant-wide life cycle. A HAZOP worksheet is a living document. Ideally, it reflects management's current knowledge of the process hazards, the consequences of those hazards and the controls necessary to reduce the process risk to a tolerable level. HAZOPs lose their effectiveness over time when they are not updated regularly. The Occupational Safety & Health Administration in 1992 claimed revalidation of PHA should be done at least every five years to ensure consistency of PHA and the current process[175]. Center for Chemical Process Safety (CCPS) defined that the revalidation process attempts to protect this investments by identifying and building upon the still pertinent portions of the prior PHA. The procedures of revalidation of PHA may be different from the prior PHA in old system. This depends on the company safety culture as well as the efficiency and cost of revalidation. However, the SSP mentioned above should cover the revalidation parts for improving understanding of risk and ultimately ensuring the safety level of the system, although big challenges may be imposed on it. Some researchers have done some work to

find out new ways to perform the revalidation activity [176-179]. Therefore, the HAZOP reports also have their own life cycle in order to meet with the requirements of identifying all possible failure scenarios and bringing the risks under control before and after changes as shown in Figure 34. In addition, recent accidents or near misses on a site process, or a similar process elsewhere, should trigger a HAZOP review to ensure that the same or similar scenario has already been considered and documented during the most recent HAZOP and that effective controls are in place to prevent a similar incident from occurring in the future.

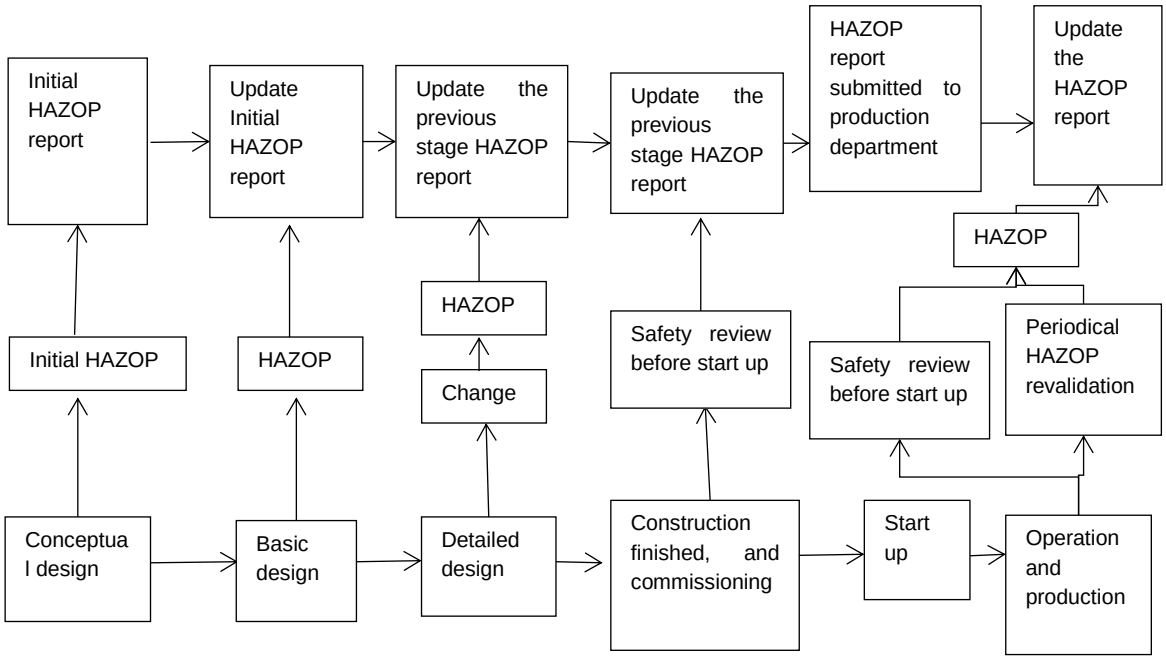


Figure 33. HAZOP reports life cycle.

3. Pay more attention on HAZOP analysis for unsteady operation. For some unsteady operation or so called non-routine modes of operation, e.g. start-up, shutdown, online maintenance, HAZOP analysis needs to be paid more attention. The accident profile[180] stated that about 70% of major accidents occur during unsteady operation, Because the system state changes dynamically with sequence operations and the potential adverse effect of one wrong operation may have domino effect in following operations during unsteady operation [181]. At the same time, operators normally are not well trained or less experience in such situations, totally relying on decision making of the operator. In contrast, 60%-80% of the accident scenarios are missed by PHA, partly reason is less devoting time for evaluating the risks of non-routine modes of operation.

7.3 Discussion and Perspectives of Challenges of HAZOP and computer-aided methods

1. Functional modelling may reduce the modelling complexity and thereby reduces the complexity of HAZOP studies. Modeling of a plant from functional perspectives may be abstract; however, it is coherent with the functional requirement of process system design. The functional requirements for a process system are less than the possible physical objects combinations such as plant structure model of ISO 15926. In this way, the modeling complexity decreases. Multilevel Flow Modeling is a best suitable technique for functional modeling. Traditionally, HAZOP only considers one node at a time, and the node boundary selected maybe based on the structural decomposition, which could result in poor boundary selection. The different isolated nodes may contribute to the same function requirements. By contrast, if the process is modelled by functional stream, the isolated nodes can be aggregated into one node await for the following HAZOP analysis since the functional nodes decomposition attempt to capture the functional requirements. Consequently, it reduces the complexity of HAZOP studies.

2. Qualitative functional models facilitate better understanding the process system in a high level abstraction and require capability of representing knowledge associated with non-routine HAZOPs to improve completeness. Functional models represent safety functions together with plant process functions. Control function in models can represent mode shift by additional studies on means-ends decomposition of the control system so that it can assist in HAZOPs for non-routine modes of operation, namely, non-routine HAZOPs.

3. Ontology in modeling library for HAZOP studies needs to be well-defined. Conceptual modeling layer are crucial to any attempt to support modeling building and even more to automate it. The interconnected components or interacting processes studied in HAZOP demands ontologies models to represent them and afterwards based on qualitative reasoning, the scenarios are visualized in qualitative models[182-183].

4. Quantitative HAZOP complements the traditional HAZOP procedure, but it does not replace qualitative models. There are still many processes that cannot be modeled for the lack of enough quantitative information, particularly in emergency situations. Thus, the quantitative version needs to be taught and used with the standard HAZOP procedure.

5. **Casual reasoning in computer-aided HAZOP is based on tacit knowledge.** The communication among HAZOP team members is based on the sharing prototypical definitions of physical objects because they have similar experience, so called tacit knowledge[184]. The causal reasoning is an analog formalizing process. The qualitative casual reasoning is useful to guide reasoning during design tailored to a specific domain. On the other hand, the quantitative reasoning related to formal analysis of relations between variables is useful for finding its limits [185]. The complementary feature is similar to the Hadamard's[186] finding between the use of intuitive judgement and formal proof by mathematicians.

8 CONCLUSIONS

The report introduced the overall problem to address and the research methodology, HAZOP. The three problems are: what is risk management in oil and gas industry, what are empirical knowledge and first principle qualitative and quantitative models, why and how the qualitative and quantitative models are combined. To answer the three questions, firstly, it provided a scientific review of the current PHA techniques in oil and gas industry. Then, generally it gave a HAZOP technique introduction and introduced the concept of plant-wide life cycle engineering and HAZOP implementation in different stages in industrial practice. Finally, it pointed out the HAZOP challenges and the computer aided methods for HAZOP involve with application of different qualitative and quantitative knowledge and models to deal with those challenges in aspects of knowledge management of system complexity, uncertainty, vagueness, completeness and efficiency, respectively..

It concludes that HAZOP technique is a key in Process Safety Review methodology for risk management. The benefits of first principles qualitative and quantitative models and empirical knowledge support to tackle with challenges of HAZOP are worthy to devote efforts and funds for research even companies to explore. To pursue such benefits, an integrated qualitative and quantitative HAZOP framework is required to develop for all stages of a plant-wide life cycle. Based on the review of different techniques in computer-aided methods and by comparing different qualitative models and reasoning, the use of qualitative hazard analysis based on functional modelling, Multilevel Flow modeling (MFM) should be selected to do modelling of process systems and reasoning to generate hazard scenarios afterwards, risk matrix should be used for screening high risk consequences scenarios and finally with dynamic simulation, the uncertainty and vagueness of HAZOP results should be studied. The completeness of such HAZOP results can be verified by industrial HAZOP studies. Although best HAZOP practice is always the target to achieve in oil and gas industry, the performance satisfactory varies from companies. Therefore, companies should be encouraged to have an open mind to embrace such advanced safety technologies by all means.

REFERENCES

[1] QIAN X. (1981). System science, thinking science and human science. Chinese Journal of Nature, 1(3): 3-9.

[2] Popovici, V. (2012). EU develops regulatory response to Macondo oil spill. Offshore.

[3] Arora S., Barak B. (2009). Computational Complexity: A Modern Approach. Cambridge University Press, 1 edition.

[4] Redmill, F. (2010). ALARP Explored.

[5] Chajai, H., & Smith, C. (2014). Defining and improving process safety for drilling and well services operations. Spe/Iadc Drilling Conference, Proceedings, 1, 290–303.

[6] Sukrajaya, I. M., & Thaliharjanti, M. (2014). Process safety walkthrough reviews. 10th Process Plant Safety Symposium, Topical Conference at the 2008 Aiche Spring National Meeting, 278–286.

[7] Guidelines for Consequence Analysis of Chemical Releases (2010). By Center for Chemical Process Safety of the American Institute of Chemical Engineers.

[8] Vinnem, J. E. (2010). Offshore Risk Assessment: Principles, Modelling and Applications of QRA Studies. Springer Publishing Company, Incorporated.

[9] Guidelines for Initiating Events and Independent Protection Layers in Layer of Protection Analysis. (2015). Wiley.

[10] Venkatasubramanian, V. (2011). Systemic Failures: Challenges and Opportunities in Risk Management in Complex Systems. Aiche Journal, 57(1), 2–9.

[11] Venkatsubramanian, V., Rengaswamy, R., Yin, K., & Kavuri, S. N. (2003). A review of process fault detection and diagnosis Part I: Quantitative model-based methods. Computers and Chemical Engineering, 27(3), 293–311.

[12] Stevens, S. S. (1946). On the Theory of Scales of Measurement. Science, 103(2684), 677–680.

[13] Ljung, L. (2014). System identification. Introduction to Mathematical Systems Theory, 15(4), 221-246.

[14] Kuipers, B. (1995). Qualitative reasoning: modeling and simulation with incomplete knowledge. Automatica, 25(4), 571-585.

[15] Lind, M. (2007). The what, why and how of functional modeling. Proceedings of International Symposium on Symbiotic Nuclear Power Systems for the 21'St Century, 174–179.

[16] Lind, M., & Zhang, X. (2014). Functional modelling for fault diagnosis and its application for npp. Nuclear Engineering & Technology, 46(6), 753-772.

[17] Komulainen, T. M., Enemark-rasmussen, R., Sin, G., Fletcher, J. P., & Cameron, D. (2012). Experiences on dynamic simulation software in chemical engineering education. Education for Chemical Engineers, 7(4), 153–162.

[18] Cameron, D., Clausen, C., & Morton, W. (2002). Chapter 5.3: Dynamic simulators for operator training. Computer Aided Chemical Engineering, 11(C), 393–431.

[19] Michalis Christou and Myrto Konstantinidou. (2012). Safety of offshore oil and gas operations: Lessons from past accident analysis-Ensuring EU hydrocarbon supply through better control of major hazards. EUR-Scientific and Technical Research series.

[20] OGP Safety Performance Indicators –2015 data

[21] GL Noble Denton Report - Review and Comparison of Petroleum Safety Regulatory Regimes CER11015.pdf

[22]“Out of Control - why control systems go wrong and how to prevent failure” (2nd Edition), UK Health and Safety Executive - Ref HSG238, ISBN 0-7176-2192-8, 2004

[23] Khan, F. I., & Abbasi, S. A. (1997). OptHAZOP—an effective and optimum approach for HAZOP study. Journal of loss prevention in the process industries, 10(3), 191-204.

[24] Haddon, W. (1973). Energy damage and the 10 countermeasure strategies. 1973. Human Factors the Journal of the Human Factors & Ergonomics Society, 15(4), 355-66.

[25] Rasmussen, J., & Svedung, I. (2000). Proactive risk management in a dynamic society. Karlstad: Swedish Rescue Services Agency,

[26] Wells, G., of Chemical Engineers, I., & IChemE. (1997). Hazard identification and risk assessment (pp. 302 s.).

[27]Nigel Hyatt, (2003).Guidelines for Process Hazards Analysis (PHA, HAZOP), Hazards Identification, and Risk Analysis, CRC Press

[28] Hazard Analysis Techniques for System Safety. (2005). Hazard Analysis Techniques for System Safety. Chapter 15 Functional Hazard Analysis. John Wiley & Sons

[29]Felix Redmill, Morris Chudleigh and James Catmur.(l999). System safety: HAZOP and software HAZOP. John Wiley & Sons Ltd., 248pp.

[30] Catmur, James, M. Chudleigh, and F. Redmill. Use of Hazard Analysis Techniques During the Product Life Cycle: HAZOP and FMEA Compared. Safety and Reliability of Software Based Systems. 1997:368-377.

[31] Schlechter, W. P. G. (1996). Facility risk review as a means to addressing existing risks during the life cycle of a process unit, operation or facility. International Journal of Pressure Vessels and Piping, 66(1-3), 387–402.

[32] Potts, H. W. W., Anderson, J. E., Colligan, L., Leach, P., Davis, S., & Berman, J. (2014). Assessing the validity of prospective hazard analysis methods: a comparison of two techniques. Bmc Health Services Research, 14(1), 41.

[33] Kletz, T. (1998). Origins of Hazop. Chemical Engineer-London, (671), 25–25.

[34] Schurman, D. L., Blackman, H., & Fleger, A. . Human factors in hazops: guide words and parameters. Professional Safety, 25(2), 145-159.

[35] Aspinall, P. (2006). Hazops and human factors. Institution of Chemical Engineers Symposium Series, (151), 820–829.

[36] Ellis, G. R., & Holt, A. (2009). A PRACTICAL APPLICATION OF 'HUMAN-HAZOP' FOR CRITICAL PROCEDURES. Inst Chem E, (155), 434–439.

[37] Avila, S. F., Pessoa, F. L. P., & Andrade, J. C. S. (2013). Social HAZOP at an Oil Refinery. Process Safety Progress, 32(1), 17–21.

[38] Ebrahim, F.& Luna-Mejias, G. (2013). Performing a HAZOP on start-up/shutdown procedures. Aiche Annual Meeting, Conference Proceedings.

[39] guidelines, procedures and templates that are necessary to perform this HAZOP

[40] Fenelon, P., Dd, Y., & Hebbron, B. (2009). Applying HAZOP to Software Engineering Models.

[41] A. Mcdermid, J., & J. Pumfrey, D. (2009). A Development of Hazard Analysis to Aid Software Design.

[42] Whitty, S. & Foord, T. (2009). Is HAZOP worth all the effort it takes? Inst Chem E, (155), 143-148.

[43] Kletz TA. (2001).Hazop and Hazan: identifying and assessing process industry hazards. Institution of Chemical Engineers.

[44] Tyler, B. J. (2012). HAZOP study training from the 1970s to today. Process Safety and Environmental Protection, 90(5), 419–423.

[45] Duhon, H.,J.,& Suton.I. (2010). Why we don’t learn what w eshould from HAZOPs. Spe Projects, Facilities and Construction, 5(2), 104-109.

[46] Nolan, D. P. (2014). Safety and security review for the process industries: Application of HAZOP, PHA, what-IF and SVA reviews. (4th Edition). Elsevier Science.

[47] HAZOP: Guide to best practice: guidelines to best practice for the process and chemical industries.

[48] Guidelines for Hazard Evaluation Procedures, Third Edition. (2010). John Wiley & Sons, Inc.

[49] IEC61882:2016 Hazard and operability studies (HAZOP studies)- Application Guide

[50] ISO. (2000). ISO 17776.Guidelines on tools and techniques for hazard identification and risk assessment. Geneva: International Organization for Standardization.

[51] Crawley.,F.K. (1995). Do hazard and operability studies have their limitations? Loss Prevention Bulletin, 121, 3-5.

[52] Tyler, B. and Simmons, B. (1995) Hazop studies: knowing their limitations. Loss Prevention Bulletin, 121, 6-8.

[53] Baybutt, P. (2015). A critique of the Hazard and Operability (HAZOP) study. Journal of Loss Prevention in the Process Industries, 33, 52–58.

[54]Janošovský J., Labovský J., Jelemensky L., 2016, Automated model-based hazop study in process hazard analysis,Chemical Engineering Transactions, 48, 505-510

[55] Jeswiet, J. (2013). Life Cycle Engineering. Springer Berlin Heidelberg.

[56] Occupational Safety and Health Administration (OSHA). 1992. 29 C.F.R. 1910.119, Process Safety Management of Highly Hazardous Chemicals.

[57] Donnelly, R. E. (2004). An overview of osha's process safety management standard (u.s.a.). Process Safety Progress, 13(2), 53-58.

[58] Shimada, Y., Kitajima, T., & Takeda, K. (2009). Practical framework for process safety management based on plant life cycle engineering. 20-24.

[59] Naka, Y., Seki, H., Hoshino, S., & Kawamura, K. (2007, June). Information Model And Technological Information-Infrastructure For Plant Life Cycle Engineering. In ICheaP-8 The eight International Conference on Chemical & Process Engineering.

[60] Papen, V.,Harvey, R. Qaasim, H.,Spielholz, P. (2011).Implementing Hazard & Operability (HAZOP) Studies Throughout the Project Life Cycle. APTA Rail Conference 2011 Proceedings.

[61] Smith, D. J. (1993). Reliability, maintainability and risk: practical methods for engineers. , 11(5), 234–245.

[62] Khan, F. I., & Amyotte, P. R. (2002). Inherent safety in offshore oil and gas activities: a review of the present status and future directions. Journal of Loss Prevention in the Process Industries, 15(4), 279–289.

[63] Kyriakdis,I.,(2003): HAZOP—Comprehensive guide to HAZOP in CSIRO, CSIRO Minerals, National Safety Council of Australia

[64] BOUCHE, D. (1992). WHEN TO HAZOP. Chemical Engineering, 99(9), 9–9.

[65]Wozniak, S. M., & Wiede, B. (2015). Combining traditional UOP HAZOP analysis with dynamic simulation a new process safety / risk assessment tool. 4th Process Safety Management Mentoring (psm2) Forum 2015 - Topical Conference at the 2015 Aiche Spring Meeting and 11th Global Congress on Process Safety, 155–175.

[66] Cui, L., Zhao, J., & Zhang, R. (2010). The integration of HAZOP expert system and piping and instrumentation diagrams. Process Safety and Environmental Protection, 88(5), 327–334.

[67] Mody, D., & Strong, D. S. (2011). An overview of chemical process design engineering. Proceedings of the Canadian Engineering Education Association, 325-331.

[68] Swann, C. D., & Preston, M. L. (1995). Twenty-five years of hazops. Journal of Loss Prevention in the Process Industries, 8(6), 349-353.

[69] McBride, M., Marsh, C., Herbert, I., & Robinson, C. (2009). Retrospective hazard identification and assessment of ageing plant. Inst Chem E, (155), 468–476.

[70] Lind, M. (2014). Functional Modeling of Complex Systems. Risk Management in Life Critical Systems, 95–114.

[71] Ottino, J. M. (2004). Engineering complex systems. Nature, 427(6973), 399–399.

[72]Kreimeyer, M., & Lindemann, U. (2011). Complexity Metrics in Engineering Design. Springer Berlin Heidelberg.

[73] Vilela-Mendes, R., & Garrido, M. S. (1992). Complexity in physics and technology.

[74] Langton, C. G. (1987). Computational complexity . Mathematical Biosciences, 85(85), 105–107.

[75] Elmaraghy, W., Elmaraghy, H., Tomiyama, T., & Monostori, L. (2012). Complexity in engineering design and manufacturing. CIRP Annals - Manufacturing Technology, 61(2), 793-814.

[76] Colwell, B. (2005). Complexity in design. Computer, 38(10), 10–12.

[77] Nordvik, J. P., Mitchison, N., & Wilikens, M. (1994). The role of the goal tree—success tree model in the real-time supervision of hazardous plants. Reliability Engineering & System Safety, 44(3), 345-360.

[78] Dunjo, J., Fthenakis, V. M., Darbra, R. M., Vilchez, J. A., & Arnaldos, J. (2011). Conducting HAZOPs in continuous chemical processes: Part I. Criteria, tools and guidelines for selecting nodes. Process Safety and Environmental Protection, 89(4), 214–223.

[79] Khazaei, B. (1993). CASE∗ method: Function and process modelling. Information and Software Technology, 35(35), 703.

[80] Searle, J. R. (1995). The construction of social reality. Simon and Schuster.

[81] Wu, J., Zhang, L., Jørgensen, S. B., Jensen, N., Lind, M., & Zhang, X. (2014). Procedure for validation of a functional model of a central heating system. The 5 th World Conference of Safety of Oil and Gas Industry, 228-232.

[82] N. P. Suh. (2012). Complexity: theory and applications, Oxford University Press, New York

[83] Suh, N. P. (2004). On functional periodicity as the basis for long-term stability of engineered and natural systems and its relationship to physical laws. Research in Engineering Design, 15(1), 72–75.

[84] Suh, N. P. (1999). A theory of complexity, periodicity and the design axioms. Research in Engineering Design, 11(2), 116-132.

[85] Maurer, M. (2007). Structural Awareness in Complex Product Design.

[86] Hendershot, D. C., Post, R. L., Valerio, P. F., Vinson, J. W., & Lorenzo, D. K. (1998). Let's put the "OP" back in "HAZOP". International Conference and Workshop on Reliability and Risk Management, 153–167.

[87] Kirchhübel, D. (2016). Operational modes in Multilevel-Flow-Modeling.

[88] Polanyi, M. (1964). Personal knowledge : Towards a Post-Critical Philosophy(pp. 428 s.). Harper & Row.

[89] Lind, M. (2014). Functional Modeling of Complex Systems. Risk Management in Life Critical Systems, 95–114.

[90] Markowski, A. S., Mannan, M. S., Kotynia, A., & Siuta, D. (2010). Uncertainty aspects in process safety analysis. Journal of Loss Prevention in the Process Industries, 23(3), 446–454.

[91] Qadir, R. M. (2014). Increase hazard discovery and minimize errors in your Process Hazard Analyses: A graph theoretical approach. Process Safety Spotlights 2014 - Topical Conference at the 2014 Aiche Spring Meeting and 10th Global Congress on Process Safety, 203–220.

[92] CSB. (2009). T2 Labs, Inc., Runaway Reaction, Jacksonville, Florida, December 19, 2007, Investigation Report No.2008-3-I-FL, U.S. Chemical Safety and Hazard Investigation Board, Washington DC.

[93] CSB. (2002). Thermal Decomposition Incident, (5 Killed), BP Amoco Polymers, Inc., Augusta, Georgia, March 13, 2001, Investigation Report No.2001-03-I-GA, U.S. Chemical Safety and Hazard Investigation Board, Washington DC.

[94] CSB. (2009). Uncontrolled Oleum Release, Petrolia, Pennsylvania, (Three towns evacuated), Case Study No.2009-01-I-PA, U.S. Chemical Safety and Hazard Investigation Board, Washington DC.

[95] CSB. (2007). Refinery Explosion and Fire, (15 killed, 180 Injured), BP Texas City, Texas, March 23, 2005, Investigation Report No. 2005-04-I-TX, U.S. Chemical Safety and Hazard Investigation Board, Washington DC.

[96] CSB. (2007). Vinyl Chloride Monomer Explosion, (5 Dead, 3 Injured, and Commuity Evacuated), Formosa Plastics Corporation, Illiopolis, Illinois, April 23, 2004, Investigation Report No. 2004-10-I-IL, U.S. Chemical Safety and Hazard Investigation Board, Washington DC.

[97] CSB. (2013). Chevron Richmond Refinery Fire, Chevron Richmond Refinery, Richmond, California, August 6, 2012, Interim Investigation Report, U.S. Chemical Safety and Hazard Investigation Board, Washington DC.

[98] OSHA. Citation and Notification of Penalty-Formosa Plastics Corporation, 19800 Old Route-36, Illiopolis, IL 62539, U.S. Occupational Safety and Health Administration, Inspection No. 305893679, Issuance Date 10/22/2004.

[99] CSB. Sterigenics,(4 employees hurt), Sterigenics, Ontario, California, August 19, 2004, Investigation Report No., 2004-11-I-CA, U.S. Chemical Safety and Hazard Investigation Board, Washington DC.

[100] Mckelvey, T. C. (1988). How to improve the effectiveness of hazard and operability analysis. IEEE Transactions on Reliability, 37(2), 167-170.

[101] Mulvihill, R. J. (1988). Design-safety enhancement through the use of hazard and risk analysis. IEEE Transactions on Reliability, 37(2), 149-158.

[102] Leveson, N. G. (2002). System safety engineering: back to the future. Aeronautics and Astronautics Department, Massachusetts Institute of Technology.

[103] Luis de la Mata, J., & Rodriguez, M. (2012). HAZOP studies using a functional modeling framework. Computer-Aided Chemical Engineering, 30, 1038–1042.

[104] Rodriguez, M., & Luis de la Mata, J. (2012). Automating HAZOP studies using D-higraphs. Computers and Chemical Engineering, 45, 102–113.

[105] Rossing, N. L., Lind, M., Jensen, N., & Jørgensen, S. B. (2010). A Goal based methodology for HAZOP analysis. International Journal of Nuclear Safety and Simulation, 1(2), 134–142.

[106] Schlechter, W. P. G. (1996). Facility risk review as a means to addressing existing risks during the life cycle of a process unit, operation or facility. International Journal of Pressure Vessels and Piping,

66(1-3), 387–402.

[107] Burgazzi, L. (2004). Evaluation of uncertainties related to passive systems performance. Nuclear Engineering and Design, 230(1-3), 93–106.

[108] CCPS (Center for Chemical Process Safety). (2009). Guidelines for Developing Quantitative Safety Risk Criteria, Appendix B. Survey of worldwide risk criteria applications. New York, USA: AIChE.

[109] Saaty T.The Analytic Hierarchy Process [M].McGraw-Hill Inc，NewYork，1980

[110] Saaty T.L. Decision making with the analytical hierarchy process.Int J Serv Sci 2008;1:83-98

[111] Pillay, A., & Wang, J. (2003). Modified failure mode and effects analysis using approximate reasoning. Reliability Engineering and System Safety, 79(1), 69–85.

[112] Gilardi, C., & Gotti, M. (2013). Semi-quantitative HAZOP methodology applied to upstream oil and gas activities. Chemical Engineering Transactions, 31, 229–234.

[113]Perez-Marin, M. f, & Rodriguez-Toral, M. A. (2013). HAZOP - Local approach in the Mexican oil & gas industry. Journal of Loss Prevention in the Process Industries, 26(5), 936–940.

[114] Othman, M. R., Idris, R., Hassim, M. H., & Ibrahim, W. H. W. (2016). Prioritizing HAZOP analysis using analytic hierarchy process (AHP). Clean Technologies and Environmental Policy, 18(5), 1345–1360.

[115] Kotek, L., & Tabas, M. (2012). HAZOP study with qualitative risk analysis for prioritization of corrective and preventive actions. Procedia Engineering, 42, 808–815.

[116] Guimaraes, A. C. F., & Lapa, C. M. F. (2006). Hazard and operability study using approximate reasoning in light-water reactors passive systems. Nuclear Engineering and Design, 236(12), 1256–1263.

[117] Ilangkumaran, M., & Thamizhselvan, P. (2010). Integrated hazard and operability study using fuzzy linguistics approach in petrochemical industry. International Journal of Quality and Reliability Management, 27(5), 541–557.

[118] Komulainen, T. M., Enemark-rasmussen, R., Sin, G., Fletcher, J. P., & Cameron, D. (2012). Experiences on dynamic simulation software in chemical engineering education. Education for Chemical Engineers, 7(4), e153–e162, e153–e162.

[119] Pugi, L., Conti, R., Rindi, A., & Rossin, S. (2014). A thermo-hydraulic tool for automatic virtual hazop evaluation. *Metrology & Measurement Systems, 21*(4), 631-648.

[120] Kirchsteiger, C. (1999). On the use of probabilistic and deterministic methods in risk analysis. Journal of Loss Prevention in the Process Industries, 12(5), 399–419.

[121] Kang, J., & Guo, L. (2016). Hazop analysis based on sensitivity evaluation. Safety Science, 88, 26-32.

[122] Enemark-Rasmussen, R., Cameron, D., Angelo, P. B., & Sin, G. (2012). A simulation based engineering method to support HAZOP studies. Computer-Aided Chemical Engineering, 31, 1271–1275.

[123] Sin, G., Gernaey, K., & Eliasson Lantz, A. (2009). Good Modeling Practice for PAT Applications: Propagation of Input Uncertainty and Sensitivity Analysis. Biotechnology Progress, 25(4), 1043–1053.

[124] Li, S., Bahroun, S., Valentin, C., Jallut, C., & De Panthou, F. (2010). Dynamic model based safety analysis of a three-phase catalytic slurry intensified continuous reactor. Journal of Loss Prevention in the Process Industries, 23(3), 437–445.

[125] Isimite, J., & Rubini, P. (2016). A dynamic HAZOP case study using the Texas City refinery explosion. Journal of Loss Prevention in the Process Industries, 40, 496–501.

[126] Gofugu A., and Kondo Y. (2011). Quantitative effect indication of a counter action in an abnormal plant situation. Nuclear Safety and Simulation, 2(3), 255-264.

[127] Varga, T., & Abonyi, J. (2010). Novel Method for the Determination of Process Safety Time. Chemical and Biochemical Engineering Quarterly, 24(3), 283–293.

[128] Svandova, Z., Markos, J., & Jelemensky, L. (2005). HAZOP analysis of CSTR with the use of mathematical modelling. Chemical Papers, 59(6B), 464–468.

[129] Pasman, H. (2015). Risk Analysis and Control for Industrial Processes - Gas, Oil and Chemicals: A System Perspective for Assessing and Avoiding Low-Probability, High-Consequence Events. Risk Analysis and Control for Industrial Processes - Gas, Oil and Chemicals: a System Perspective for Assessing and Avoiding Low-Probability, High-Consequence Events, 1–474.

[130] Yao, X. W., Xu, K. L., Tang, G. C., & Wang, W. J. (2014). Integrative risk analysis and application of HAZOP-LOPA based on bayesian networks inference. Dongbei Daxue Xuebao/Journal of Northeastern University, 35(9), 1356–1359.

[131] Hu, J., Zhang, L., Cai, Z., & Wang, Y. (2015). An intelligent fault diagnosis system for process plant using a functional HAZOP and DBN integrated methodology. Engineering Applications of Artificial Intelligence, 45, 119–135.

[132] Hu, J., Zhang, L., Cai, Z., Wang, Y., & Wang, A. (2015). Fault propagation behavior study and root cause reasoning with dynamic Bayesian network based framework. Process Safety and Environmental Protection, 97, 25–36.

[133] Reitz, A., Levrat, E., & Pétin, J. F. (2014). Quantitative risk analysis in radiotherapy using Bayesian networks. Safety, Reliability and Risk Analysis: Beyond the Horizon - Proceedings of the European Safety and Reliability Conference, Esrel 2013, 2471–2478.

[134] Unnikrishnan, G., Al-Zalzalah, F., Shrihari, & Siddiqui, N. (2014). Risk management in the process industry-new directions with Bayesian approach. Society of Petroleum Engineers - Spe International Conference on Health, Safety and Environment 2014: the Journey Continues, 2, 964–983.

[135] Wang, H., Khan, F., & Ahmed, S. (2015). Design of Scenario-Based Early Warning System for Process Operations. Industrial and Engineering Chemistry Research, 54(33), 8255–8265.

[136] Zadeh, L. A. (1983). A computational approach to fuzzy quantifiers in natural languages.Computers & Mathematics with Applications, 9(1), 149–184.

[137] Tao, C., Huabing, Z., Honglong, Z., Yufeng, Y., & Xin, W. (2012). Quantitative hazop risk analysis for oil tanks using the fuzzy set theory. Proceedings of the Biennial International Pipeline Conference, Ipc, 1, 379–385.

[138] Kuchta, D., Stanek, S., Drosio, S., & Gładysz, B. (2017). Application of fuzzy rules to the decision process in crisis management: The case of the silesian district in poland. Intelligent Systems Reference Library, 113, 119–133.

[139] Luis Fuentes-Bargues, J., Gonzalez-Gaya, C., Carmen Gonzalez-Cruz, M., & Cabrelles-Ramirez, V. (2016). Risk assessment of a compound feed process based on HAZOP analysis and linguistic terms. Journal of Loss Prevention in the Process Industries, 44, 44–52.

[140] Ahn, J., & Chang, D. (2016). Fuzzy-based HAZOP study for process industry. Journal of Hazardous Materials, 317, 303–311.

[141] Mentes, A., & Helvacioglu, I. H. (2011). Review of fuzzy set theory applications in safety assessment for marine and offshore industries. Lecture Notes in Computer Science, 2, 875–884.

[142] FREEMAN, R. A., LEE, R., & MCNAMARA, T. P. (1992). PLAN HAZOP STUDIES WITH AN EXPERT SYSTEM. Chemical Engineering Progress, 88(8), 28–32.

[143] Khan, F. I., & Abbasi, S. A. (1997). Mathematical model for HAZOP study time estimation. Journal of Loss Prevention in the Process Industries, 10(4), 249–257.

[144] Dunjo, J., Fthenakis, V. M., Darbra, R. M., Vilchez, J. A., & Arnaldos, J. (2011). Conducting HAZOPs in continuous chemical processes: Part I. Criteria, tools and guidelines for selecting nodes. Process Safety and Environmental Protection, 89(4), 214–223.

[145] Rushton, A. G., 1997, Knowledge-Based HAZOPs, Pts 1 and 2 (European Process Safety Centre reports)

[146] Lees, F. P. (1996). Loss prevention in the process industries: hazard identification, assessment and control. Loss prevention in the process industries : hazard identification, assessment and control. Butterworths.

[147] Khan, F. I., & Abbasi, S. A. (1997). Opthazop—an effective and optimum approach for hazop study.

Journal of Loss Prevention in the Process Industries, 10(3), 191-204.

[148] Khan, F. I., & Abbasi, S. A. (1997). Tophazop: a knowledge-based software tool for conducting hazop in a rapid, efficient yet inexpensive manner. Journal of Loss Prevention in the Process Industries, 10(5), 333-343.

[149] Khan, F. I., & Abbasi, S. A. (2000). Towards automation of hazop with a new tool expertop. Environmental Modelling & Software, 15(1), 67-77.

[150] Rahman, S., Khan, F., Veitch, B., & Amyotte, P. (2009). ExpHAZOP(+): Knowledge-based expert system to conduct automated HAZOP. Journal of Loss Prevention in the Process Industries, 22(4), 373–380.

[151] Vaidhyanathan, R., Venkatasubramanian, V., & Dyke, F. T. (1996). Hazopexpert : an expert system for automating hazop analysis. Process Safety Progress, 15(2), 80-88.

[152] Zhao, C., Bhushan, M., & Venkatasubramanian, V. (2005). Phasuite: an automated hazop analysis tool for chemical processes : part ii: implementation and case study. Process Safety & Environmental Protection, 83(6), 533-548.

[153] Zhao, C., Bhushan, M., & Venkatasubramanian, V. (2005). Phasuite: An automated hazop analysis tool for chemical processes Part II: Implementation and case study. Process Safety and Environmental Protection, 83(B6), 533–548.

[154] Zhao, J., Cui, L., Zhao, L., Qiu, T., & Chen, B. (2009). Learning HAZOP expert system by case-based reasoning and ontology. Computers and Chemical Engineering, 33(1), 371–378.

[155] Mccoy, S. A., Associate, Wakeman, S. J., Larkin, F. D., Associate, & Jefferson, M. L., et al. (1999). Hazid, a computer aid for hazard identification: 1. the stophaz package and the hazid code: an overview, the issues and the structure. Process Safety & Environmental Protection, 77(B6), 317–327.

[156] Mccoy, S. A., Wakeman, S. J., Larkin, F. D., Chung, P. W. H., Rushton, A. G., & Lees, F. P. (1999). Hazid, a computer aid for hazard identification : 2. unit model system. Process Safety & Environmental Protection, 77(6), 328-334.

[157] Mccoy, S. A., Wakeman, S. J., Larkin, F. D., Chung, P. W. H., Rushton, A. G., & Lees, F. P., et al. (1999). Hazid, a computer aid for hazard identification : 3. the fluid model and consequence evaluation systems. Process Safety & Environmental Protection, 77(6), 335-353.

[158] Mccoy, S. A., Wakeman, S. J., Larkin, F. D., Chung, P. W. H., Rushton, A. G., & Lees, F. P. (2000). Hazid, a computer aid for hazard identification : 4. learning set, main study system, output quality and validation trials. Process Safety & Environmental Protection, 78(2), 91-119.

[159] Mccoy, S. A., Wakeman, S. J., Larkin, F. D., Chung, P. W. H., Rushton, A. G., & Lees, F. P. (2000). Hazid, a computer aid for hazard identification: 5. future development topics and conclusions. Process Safety & Environmental Protection, 78(2), 120-142.

[160] Khan, F. I., & Abbasi, S. A. (1997). TOPHAZOP: A knowledge-based software tool for conducting HAZOP in a rapid, efficient yet inexpensive manner. Journal of Loss Prevention in the Process Industries, 10(5-6), 333–343.

[161] Khan, F. I., & Abbasi, S. A. (2001). Risk analysis of a typical chemical industry using ORA procedure. Journal of Loss Prevention in the Process Industries, 14(1), 43–59.

[162] Khan, F. I. (2005). Knowledge-based expert system framework to conduct offshore process HAZOP study. 2005 Ieee International Conference on Systems, Man and Cybernetics, 3, 2274,2275,2276,2277,2278,2279,2280, 2274–2280 Vol. 3.

[163] Lapp, S. A., & Powers, G. J. (1977). Computer-aided synthesis of fault-trees. Ieee Transactions on Reliability, R-26(1), 2–13, 2–13.

[164] Wang, Y. (2004). Development of a computer-aided fault tree synthesis methodology for quantitative risk analysis in the chemical process industry. Texas A & M University.

[165] Vaidhyanathan, R., & Venkatasubramanian, V. (1995). Digraph-based models for automated hazop analysis. Reliability Engineering &System Safety, 50(1), 33-49.

[166] De Kleer, J., & Seely Brown, J. (1984). A qualitative physics based on confluences. Artificial Intelligence, 24(1), 7-83.

[167] Vaidhyanathan, R., & Venkatasubramanian, V. (1996). A semi-quantitative reasoning methodology for filtering and ranking HAZOP results in HAZOPExpert. Reliability Engineering and System Safety, 53(2), 185–203.

[168] Srinivasan, R., Dimitriadis, V. D., Shah, N., & Venkatasubramanian, V. (1997). Integrating knowledge-based and mathematical programming approaches for process safety verification. Computers and Chemical Engineering, 21(1), S905–S910.

[169] Srinivasan, R., Dimitriadis, V. D., Shah, N., & Venkatasubramanian, V. (1998). Safety verification using a hybrid knowledge-based mathematical programming framework. Aiche Journal, 44(2), 361–371.

[170] Dimitriadis, V. D., Shah, N., & Pantelides, C. C. (1997). Modeling and safety verification of discrete/continuous processing systems. Aiche Journal, 43(4), 1041–1059.

[171] An, H., Chung, P. W. H., Mcdonald, J., & Madden, J. (2008). A computer tool to support safe isolation for maintenance. 2nd World Conference on Safety of Oil and Gas Industry, Mary Kay O'Connor Process Safety Center, College Station, Texas, 406-415.

[172] Skelton, B. (2002). HAZOP as a safety analysis tool. Nuclear Engineer, 43(2), 35-39.

[173] Ellis, G. (2016). Practical experience of retrospective HAZOP and LOPA studies for an offshore platform. Instituion of Chemical Engineers Symposium Series, 2016-(161):517-524.

[174] Knight, J. C. (2002). Safety critical systems: challenges and directions. International Conference on Software Engineering (pp.547-550). ACM.

[175]Xu, J., Ge, C., & Zhang, Y. (2016). The study of HAZOP revalidation approach. 5th Process Safety Management Mentoring Forum 2016, Psm2 2016 - Topical Conference at the 2016 Aiche Spring Meeting and 12th Global Congress on Process Safety, 219–228.

[176] Crumpler, D. K., & Whittle, D. K. (1996). How to effectively revalidate PHAs. Hydrocarbon Processing, 75(10), 55–60.

[177] Wagner, T., & Champion, J. (2012). A Work Process for Revalidating LOPAs and Other Risk Analyses. Process Safety Progress, 31(2), 122–129.

[178] Abhulimen, K. (2001). Update and revalidate PHAs. Chemical Engineering Progress, 97(7), 8.

[179] Smith, K. E., & Whittle, D. K. (2001). Six steps to effectively update and revalidate PHAs. Chemical Engineering Progress, 97(1), 70–77.

[180] Brideges, W.& Clark, T. (2011). How to effeicently perform the hazard evaluation (PHA) required for non-rountine modes of operation (startup, shutdown, online maintenance). Aiche Annual Meeting. Conference Proceedings.

[181] Zhang, Y., Zhang, W., & Zhang, B. (2015). Automatic HAZOP analysis method for unsteady operation in chemical based on qualitative simulation and inference. Chinese Journal of Chemical Engineering, 23(12), 2065–2074.

[182] Batres, R., Shimada, Y.,& Fuchino, T. (2008). A graphical approach for representing hazard scenarios. Aiche Annual Meeting, Conference Proceedings.

[183] Kwamura, K., Naka, Y., Fuchino, T., Aoyama, A., & Takagi, N. (2008). HAZOP Support system and its use for operation. Computer-Aided Chemical Engineering, 25, 1003–1008.

[184] Polanyi, M. (1967). The tacit dimension. New York: Doubleday& Co.

[185] Pedersen, S.A.,& Rasmussen, J. (1991). Causal and diagnostic reasoning in medicine and engineering. Cognitive Processes and Resources. Proceedings. Vol. 3, 51-81.

[186] Hadamard, J.L. (1945). The psychology of invention in the mathematical field. Princeton: Princeton University Press.