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

Part II. An Integrated Qualitative and Quantitative HAZOP Framework

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 II. An Integrated Qualitative and Quantitative HAZOP Framework

February, 2017

DTU Electrical Engineering
Department of Electrical Engineering

Combining empirical knowledge and first principles qualitative and quantitative models in HAZOP, Part II. An Integrated Qualitative and Quantitative HAZOP Framework

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

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.

TABLE OF CONTENTS

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.

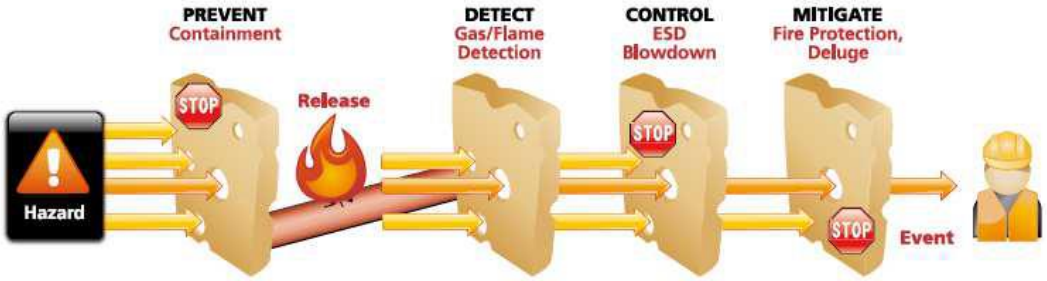


Figure 1. Application of the “Swiss cheese” model

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.

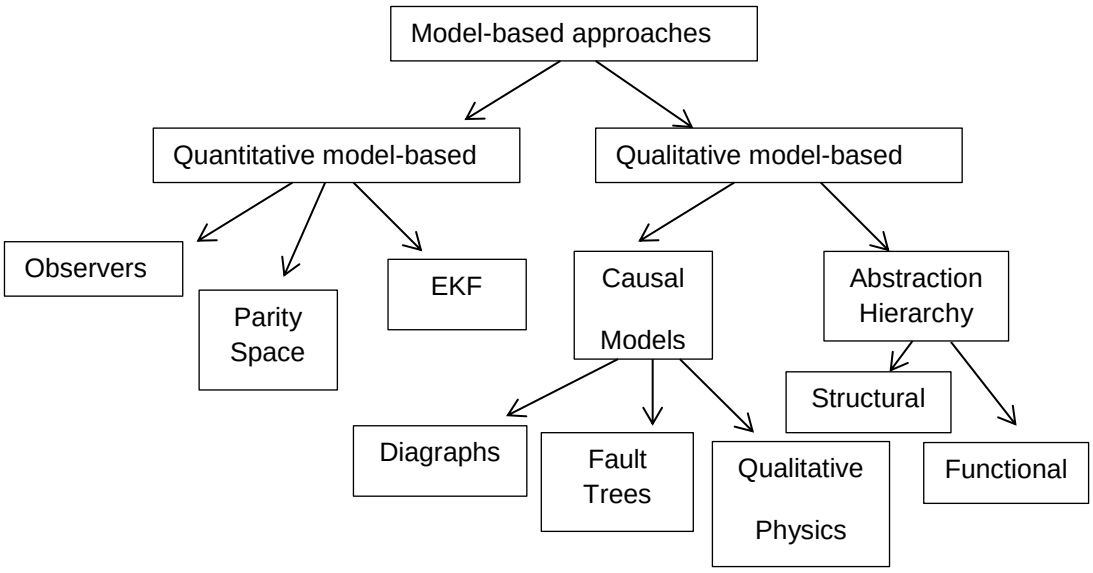


Figure 2. Classification of model-based approaches by Venkatasubramanian [11]

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.

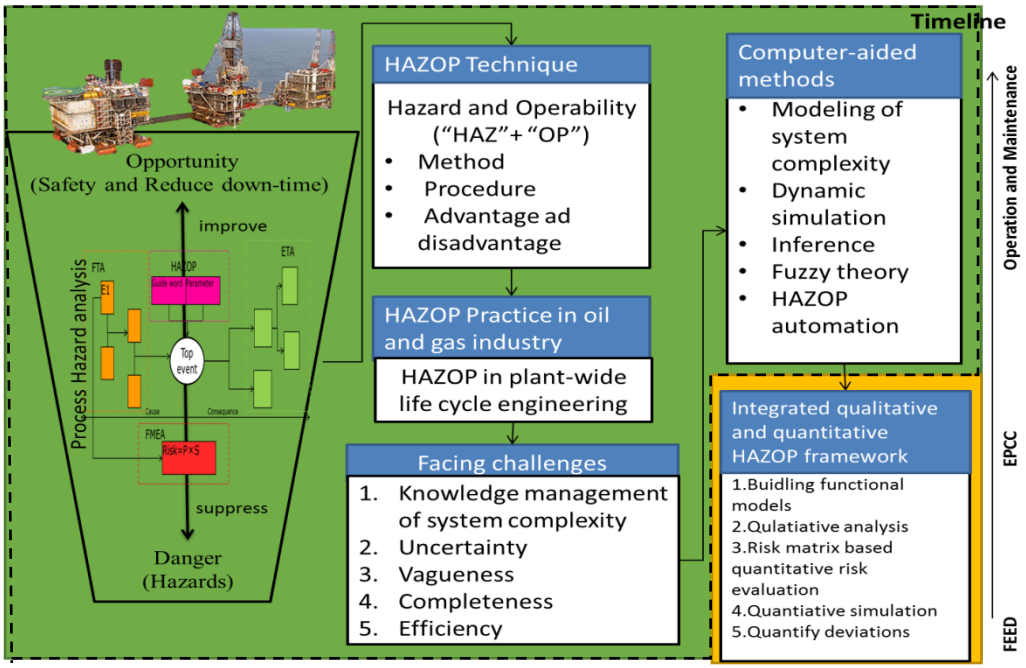


Figure 3. Report contents overview

2 MOTIVATIONS

The purpose of Part II is to demonstrate complementary strengths of the qualitative model-based and the quantitative model-based approaches explored in Part I by proposing an integrated qualitative and quantitative framework.

Hazard analysis using a qualitative model based approach is fast even for industrial scale processes. Also, the results produced by this approach are comprehensive. Hazard evaluation using the quantitative model-based approach can determine whether a given hazard is physically acceptable, given the dynamic model of the process and ranges on process inputs and disturbances. However, although the qualitative and quantitative methodologies for hazard analysis and risk assessment have been researched separately for years, the integration of the two aspects in a qualitative and quantitative modeling framework for cause and consequence analysis of hazards and operation problems has not been presented. Therefore, the initial idea for proposing an integrated qualitative and quantitative framework was to find out how the complementary strength will benefit HAZOP studies.

Specifically, the aim is to develop tools to assist with hazard identification in the proposed integrated qualitative and quantitative modeling framework, to develop the systematic qualitative and quantitative methods used and explore how the qualitative and quantitative methods may supplement each other. The purpose of the proposed framework is to support designers and system analyzers by representing the process from two perspectives: “goal-function-structure” and “phenomena-structure-behavior” and to identify hazards from the above two perspectives, and use the ALARP principle to rank and filter the hazards, which are output of the hazard analysis and at the basis for proposing possible countermeasures (including operator tasks and systems design changes). In summary, the proposed framework may be used to investigate process and/or control design modifications to mitigate the operational risk.

The proposed integrated qualitative and quantitative modeling framework is suggested to be used primarily during front-end engineering design (FEED) stage of a project as this is the stage where it makes the most sense to invest time and resources for a comprehensive hazard identification and risk analysis. However, as the tools and methods are generic, they can be applied during other stages of the project life cycle. The selected case study in this article focuses on the methodology development and validation of the framework, with in-depth discussions and result presentation. The extrapolation to an industrially relevant case study with more unit operations is straight forward, and therefore, kept outside this contribution. It can also be noted that in a typical topsides operation, one would have several unit operations in series. This does not present a challenge to the proposed framework. The following sections are the summary of the work.

3 AN INTEGRATED QUALITATIVE AND QUANTITATIVE FRAMEWORK

3.1 Methods and Tools

A Functional HAZOP assistant proposed by Rossing et al. [19] provided a very efficient paradigm for facilitating HAZOP studies and for enabling reasoning about potential hazards in safety critical operations. The functional HAZOP assistant uses multilevel flow modeling (MFM) representing functional knowledge of a process by mass flow, energy flow and control flow.

The MFM method is a process goal-based hierarchically structured methodology. By using the MFM modeling language expressed through a set of pre-defined formalized graphical symbols, the system goals, functions for the plant production process are represented. The MFM modeling languages provide formalized concepts for the description of the systems and as such serve as a modeling language. This qualitative modeling framework was proposed by Lind [20] in 1980s. Lind and his coworkers [21-2228] and the research groups in Japan [29-33], Sweden [34-36], Norway [37], Netherland [38], USA [39-40], Malaysia [41] and China [42-45] have been promoting and developing the method. In MFM modeling, means-end relations link the plant operating objectives and flow function structure. They can be seen either from the objective perspective, which describes how the objective is achieved by functions in the flow structure, or from the function flow structure perspective, to describe what objective is reached by its functions. MFM reasoning can propagate events in both directions depending on the nature of the reasoning (causes or consequences). Consequently the modeling of a process system can be done in either top-down manner or bottom-up manner or a combination thereof. For example, the top-down manner is suitable for the early phases of system design. The purpose of this top down procedure makes sure that the plant functions (flow functions and control functions shown in Figure 4) are defined in the context of the system objectives. It starts from the definition of objectives to end at the structure of the system. The concept of objective here represents a state which should be produced or maintained. Objectives are related to functional structures by means-end relations.

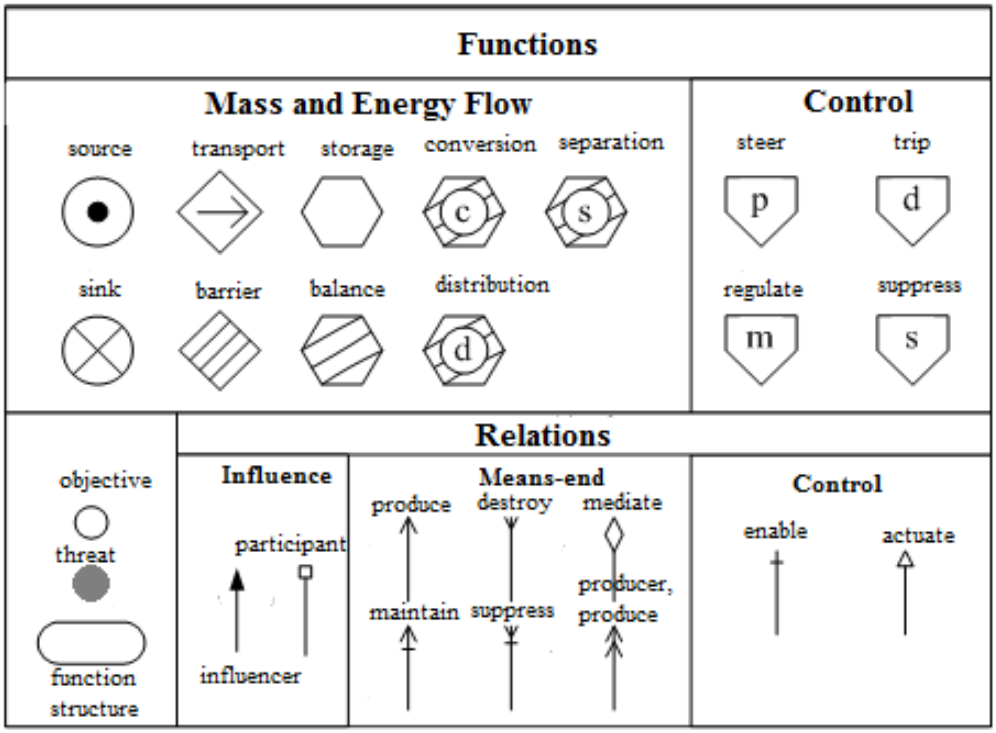


Figure 4. The basic MFM symbols

Reasoning with MFM models is based on cause effect relations associated with the function–function and function–objective relations, which comprise the elements of reasoning patterns, which are implemented in a rule-based reasoning system (called the MFM reasoning engine) developed at Technical University of Denmark (DTU). The reasoning system propagates state information of each function and can derive possible cause and consequence paths of a given deviation of a functional state.

The MFM method was originally dedicated to improve situation awareness for operators with automation and human machine interaction which has attractive features for modeling complex systems. The main features are 1) MFM represents systems and their interactions on several levels of abstraction, 2) MFM supports cause-effect reasoning, 3) MFM provides formalized representations of operational situations and 4) MFM concepts are coherent with human cognition. These four features indicate that it can deal with realistic engineering problems in different research domains, such as fault diagnosis, situation awareness, operational planning.

Rossing and co-authors made the first attempt to embrace the idea for using MFM for facilitating HAZOP studies through preparing a HAZOP assistant. The concept was further elaborated, extensively described in the proposed integrated qualitative and quantitative framework by Wu et al.. In the case study of this report, a graphical editor supporting MFM modeling (called the MFM Editor) developed is used[46]. This MFM Editor integrated with the MFM reasoning system developed by DTU can generate cause and consequence trees for a given deviation in a system function. Now the MFM Editor and reasoning system is integrated into a platform called MFMSuite still under development [47-48]. A quantitative simulator called K-Spcie® was used for doing dynamic simulation based on quantitative models.

The functional models are qualitative and display the relations between the means and the intention of the system in question. Thereby functional models capture much of the tacit knowledge, which normally is neither expressed nor communicated when quantitative models are developed and presented. Consequently, there is a direct connection from a qualitative model to a quantitative model of a given system with a specific purpose or design intention. Therefore, it is considered highly relevant to develop and investigate an integrated qualitative functional and quantitative framework.

3.2 The proposed integrated qualitative and quantitative framework

Generally speaking, integration of qualitative reasoning and quantitative process simulation for hazard analysis and risk management aims to complement each other by overcoming their respective gaps/shortcomings. In nature, the qualitative models formulate “goal-function” relations of systems in a logical way to represent how the system functions achieve system goals, where the system goals represent the combined technical and social (ethical) requirements[49] to the plant. In contrast, quantitative models deal with “goal-behavior” of system, which represent the plant behavior as perceived by the system developer. This understanding is unfortunately only seldom documented by the model developer, and therefore, in practice most often only tacit knowledge.

The proposed framework for integration of the qualitative and quantitative process simulation for HAZOP studies is shown in Figure 5. Based on the qualitative MFM model of the process system, qualitative simulations can be performed as follows: first, a deviation in one of the functions of the process is induced (one deviation at a time), and then the reasoning engine derives possible causes paths for the given deviation. The outcomes from this qualitative simulation are cause trees. Then selected potential root causes are evaluated by followed by a consequence analysis of root causes that leads to the deviation. In this way cause–consequence paths are derived. By performing risk assessment based on a qualitative risk matrix [50], the potential high risk causes are selected as input for the quantitative dynamic process simulator. From the quantitative dynamic simulator, on one hand, we can validate consequences, that is, results obtained from the qualitative consequence analysis derived from the MFM model. On the other hand, detail behavior of the system, such as quantified scenarios can be explored.

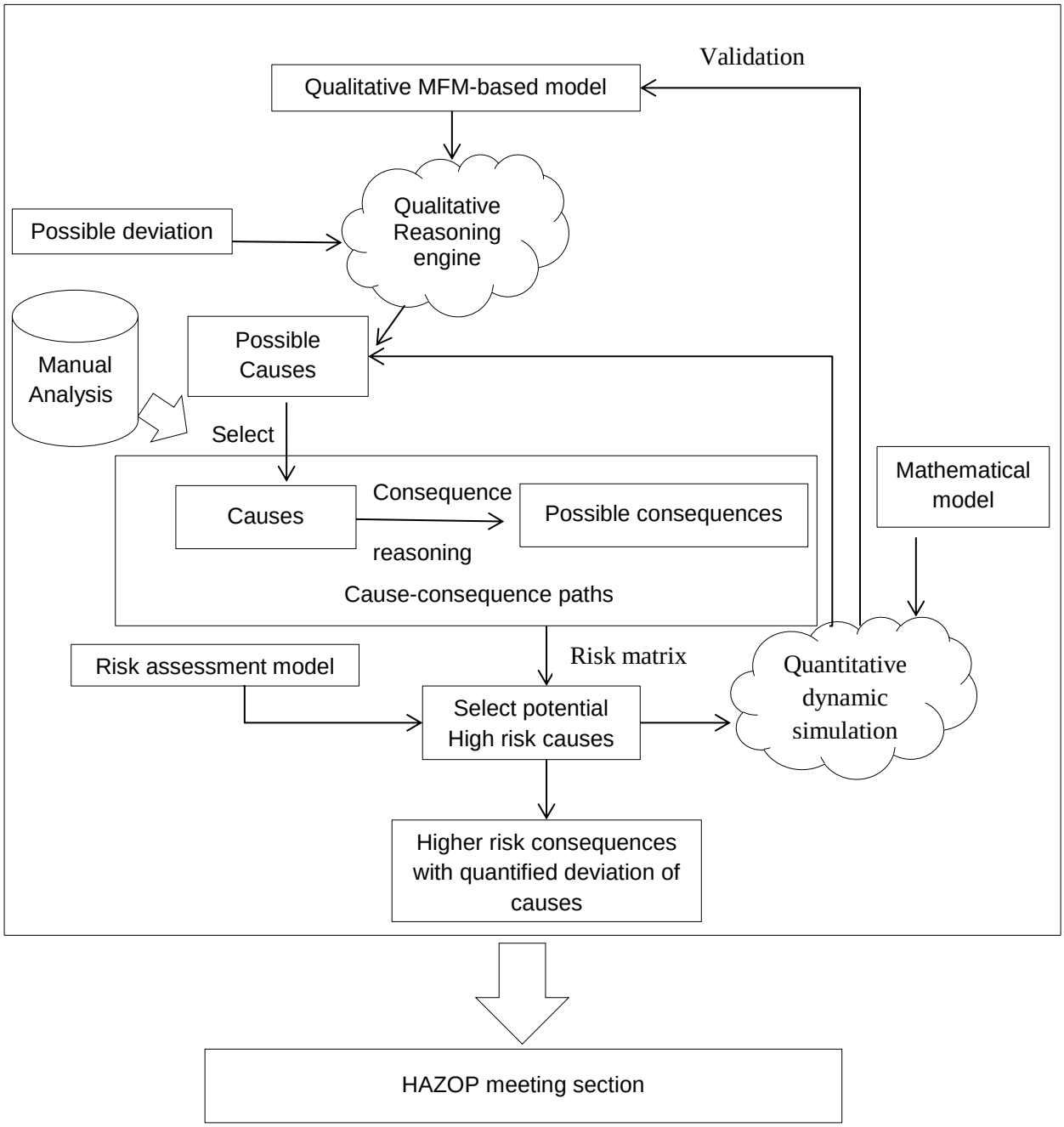


Figure 5. The proposed integration of qualitative and quantitative process simulation frameworks

3.3 A 5-steps integrated methodology in the proposed framework

A 5-steps integrated methodology for HAZOP was proposed in the framework.

- *1st Step: Buidling MFM models.* To build an MFM model following a formalized MFM modeling procedure: ①knowledge acquisition; ②system decomposition into subsystems; ③subsystem

decomposition into functional nodes; ④means-ends analysis in terms of components, functions, objectives; ⑤MFM modeling⑥Model verification and validations. The verification/validation of the model can be done in two ways: (1) The verification of the MFM model of the real system is handled by the built-in MFM syntax validation function of the MFM-editor. The software checks function connection patterns, causal relation links, and means-end relation links, and whether the model syntactically is properly connected. The MFM syntax is described in Zhang et al [51]; (2) To validate the MFM model, internal and external modeling purposes should be specified first. An internal modeling purpose is meant to inquire into whether the MFM model preserves the behaviors and characteristics of real system that modelers are interested in, while an external modeling purpose is meant to inquire into whether the applicable domain provides a sufficient representation for the intended system purpose. A validation procedure for an MFM model proposed in reference [52] is utilized for model verification and validation.

- *2nd Step: Qualitative HAZOP analysis.* To conduct qualitative HAZOP analysis for process based on the MFM model. In order to validate the results produced by the cause and consequence analysis for each deviation based on MFM reasoning, the qualitative manual HAZOP analysis is carried out as well.

- *3rd Step: Using the risk matrix for qualitative risk assessment.* To select potentially high risk hazard evaluated by the risk matrix.

- *4th Step: Validation of the qualitative analysis.* To validate the unacceptable failure scenarios identified by the qualitative analysis by using qualitative dynamic simulation. The failure of the control function of an anti-surge valve is demonstrated as an example.

- *5th Step: Real-time Simulation of Transient Behavior and Quantification of Deviation Scenarios.* To conduct detailed analysis for highly unacceptable consequences for further mitigation suggestions, i.e., quantification the deviation for identifying the process status at four levels (deviation, abnormal, critical, and catastrophic). It is demonstrated for the parameter of plugging fraction of the anti-surge valve.

4 CASE STUDY

The integrated qualitative and quantitative modeling framework is demonstrated on a three-phase separation process which is a commonly used unit operation on offshore platforms in the oil and gas industry [52]. The process schematic is shown in Figure 6. The feed to the process is a three-phase fluid flow consisting of gas, oil, and water, which is separated into a gas-rich, an oil-rich, and a water-rich stream. The two feed streams are mixed before entering the three-phase separator (23VA0001), which is designed to separate the gas, the oil, and water. A pressure safety valve (23PSV0001) provides protection against unwanted pressure buildup in the gas phase. The weir plate inside the separator separates the oil and water chamber and the level controller (LIC0001) maintains the water level. The oil is skimmed over the weir. The level of the oil downstream of the weir is controlled by a level controller (LIC0002) that operates the oil export valve (23LV0002). The gas flows out through the gas outlet pipe with the emergency safety valve (25ES0002). Then it passes to a centrifugal compressor (23KA0001) driven by a variable motor speed (23EM0002) which increases the pressure of the export gas. At the outlet side of the compressor, a heat exchanger (23HA0001) is connected with water as cooling medium (23COLD0001). The cooler is regulated by a temperature control loop (TIC0003). Also an anti-surge controller loop (23UV0001) is installed to protect the compressor from entering a surge condition. More details about the process can be found elsewhere [53].

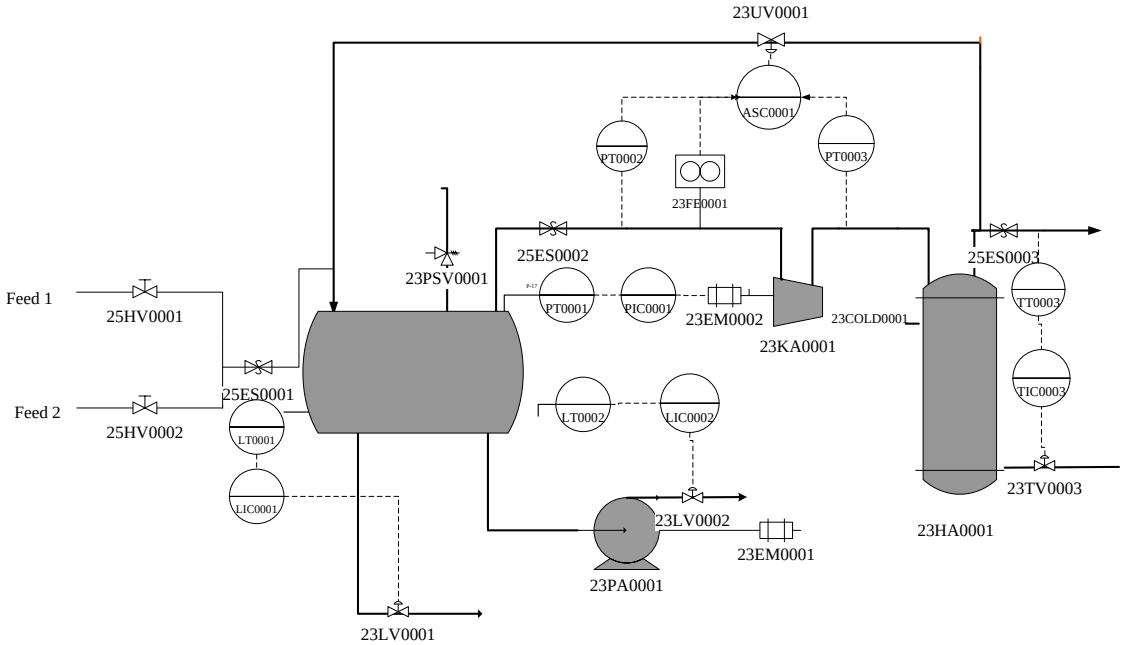


Figure 6. Simplified P&ID of three-phase separation process.

Based on the design intention and to facilitate to build MFM models of the system, the process is divided into two sections.

Section 1: three-phase separator section with the goal: Separate two fluid streams of mixture of gas, crude oil, and water into three streams, that is, gas, oil, and water.

Section 2: heat exchanger section with the goal: to recover as much heat as possible before shipping the gas through a pipeline.

4.1 Building MFM models (1st step)

Based on the formalized MFM modeling procedure, after system decomposition into function nodes, taking section 1 for example, shown in Table 1, using the MFM editor build MFM models of the process as shown in Figures 7 and 8. The explanations of the models and elements (flow structures, objectives, relations, and functions) in Figure 7 and Figure 8 are presented in Appendix A.

Table 1. Function nodes in section 1

Node number	Function	Structure
1	Fluid transport	Line from Feed1 to the three-phase separator (23VA0001)
2	Fluid transport	Line from Feed 2 to the three-phase separator(23VA0001)
3	separation	Three-phase separator, 23VA0001
4	Liquid transport	Line from the separator (23VA0001) to water outflow including water level control valve and other instrumentation
5	Liquid transport	Line from the separator (23VA0001)to oil outflow including a pump (23PA0001) and other instrumentation
6	Gas transport	Line from the separator (23VA0001) to compressor (23KA0001)
7	Gas transport	Compressor(23KA0001)
8	Gas transport	Line from the compressor (23KA0001) to heat exchanger (23HX0001)
9	Control function	Anti-surge control loop

It should be noted that the MFM model provides a hierarchical abstraction representation. The level of abstraction is defined by the level of operation by which a system is viewed, which is inversely proportional to the description level, the higher the level the less detail. A lower level could contain literarily hundreds or thousands of objects. So Figure 7 is a higher level abstraction of the three-phase separation process. Figure 8 is the lower level abstraction of separation function and reveals the equilibrium-surface phenomena of gas and liquid, which aids the reasoning of deviation in the separator.

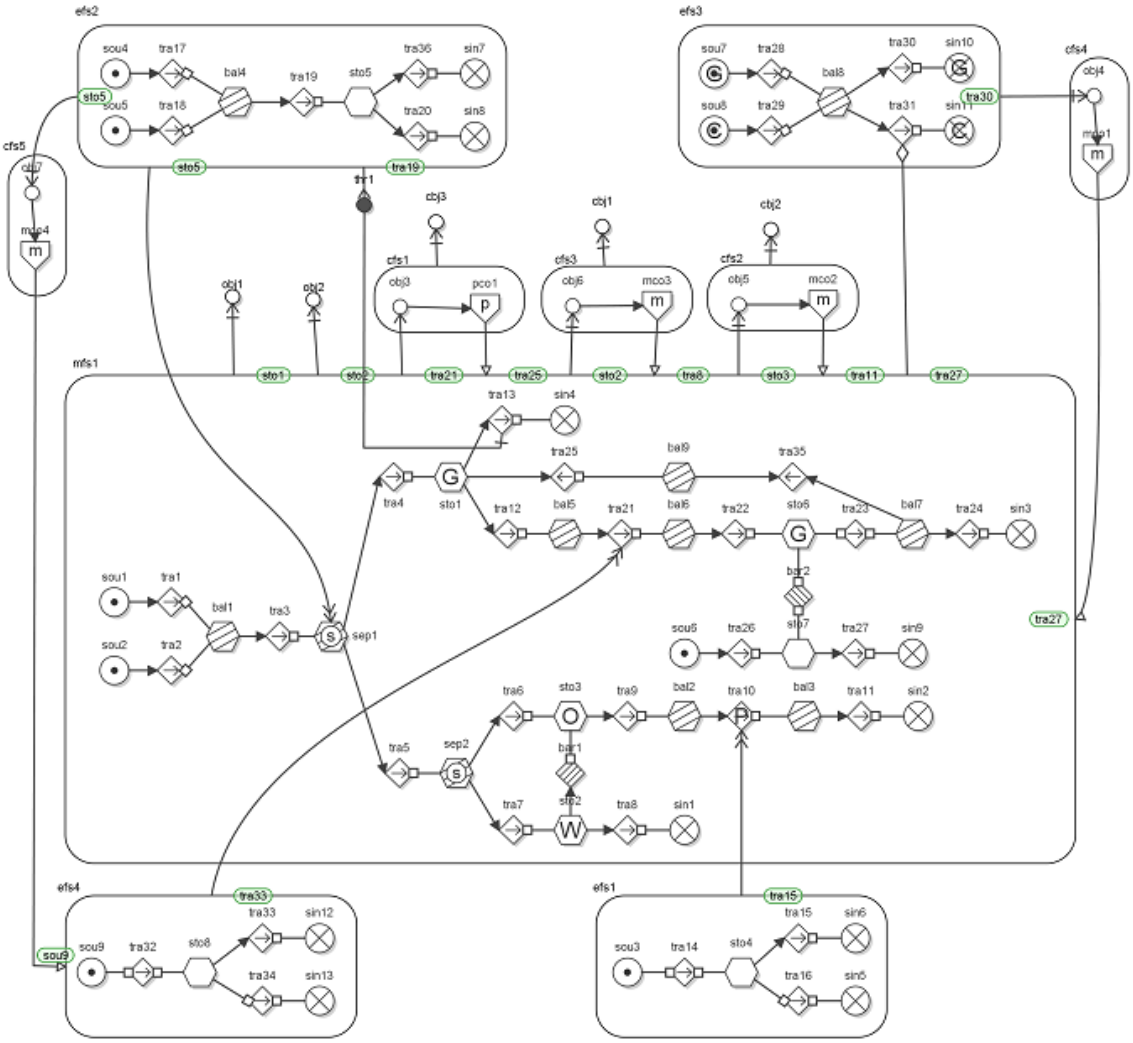


Figure 7. MFM model of three-phase separation process (higher level abstraction).

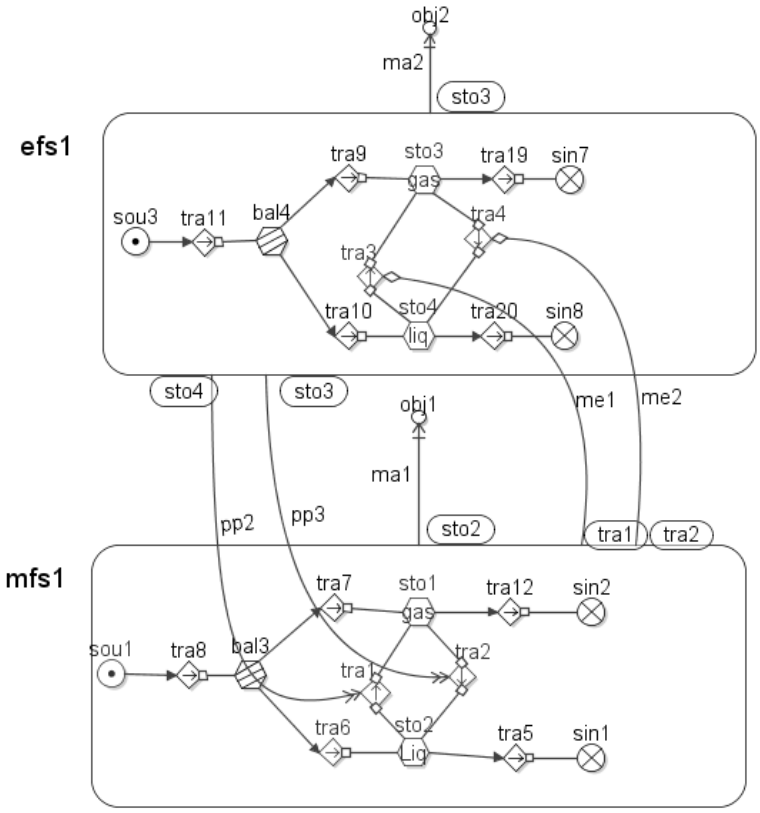


Figure 8. MFM model of three-phase separator section

(lower level abstraction of separation function).

4.2 Qualitative HAZOP analysis (2nd step)

To demonstrate the feasibility of the methodology for qualitative hazard analysis, we applied related deviations for the nodes of Section 1. We carried out a traditional HAZOP procedure to fill in the traditional HAZOP parts of the qualitative HAZOP worksheet. The result of traditional HAZOP and the results of functional HAZOP are compared. The qualitative HAZOP analysis result for node 3 “function of separator” is shown in Table 2. It should be noted that the consequences shown in Table 6 are in condition of the safety valve 23PSV0001 failure to open.

Table 2. The comparison result of modified HAZOP worksheet for higher pressure deviation in node 3"Function of Separator"

Process Parameters	GUIDE word	Deviation	Traditional HAZOP Causes	MFM-Based Causes	Traditional HAZOP Consequences	MFM-Based Consequences	Safeguards	Actions Required
Pressure	More	Higher pressure	Pipeline junction of heat exchanger is blocked	1	1. Pressure builds up on separator 23VA0001 2. Compressor possibly surge 3. Oil–water interface level , oil level and total level are lower due to higher pressure of separator preventing feed flow to enter in separator 4. A low oil level causes gas to exit via the oil output causing high pressure down-stream (pressure builds up on pump) 5. Less gas production	3,4,5,6,7	none	Monitoring the flow rate and consider maintenance pipeline
			Antisurge valve 23UV0001 stuck at more open position than normal gas output pipeline of the separator blocked or frozen	2	1. Pressure builds up on separator 23VA0001 2. Compressor could block due to too high inflow rate	7,8	none	Install a back up valve for antisurge recir-culation loop
				3	1. Pressure builds up on separator 23VA0001 2. Compressor can possibly surge 3. Oil-water interface level , oil level and total level are lower due to higher pressure of sep-arator preventing feed flow to enter in separator 4. A low oil level causes gas to exit via the oil output causing high pressure downstream (pressure builds up on pump)	3,4,5,7	PT0001 PIC0001 23PSV0001 Antisurge control loop of compressor (23UV0001 and 23ASC0001)	1. Add an alarm to indicate whether the isolation valve 25ES0002 is out of posi-tion, i.e. if the valve is requested to open and 23FE0001 shows no flow then alarm. This action applies to all valve position indicators 2. Add high pressure alarm 3. Install a manual bypass valve V-2 4. Line design pressure higher than pump deadhead pressure 5. Install kickback line to pump 6. Install relief valve 23PSV0002 for pump 7. Install stand-by pumping system
			Polytropic efficiency of compressor is degrading	4	1. Pressure builds up on separator 23VA0001 2. Compressor surge 3. A low oil level causes gas to exit via the oil output causing high pressure down-stream (pressure builds up on pump/pump damage)	3,4,5,6,7,9	none	Monitoring compressor working condition
			Pressure control system failure e.g. fail to increase compressor speed	5	1. Pressure builds up on separator 23VA0001 2. Compressor possibly surge 3. Oil-water interface level , oil level and total level are lower due to higher pressure of separator preventing feed flow to enter in separator 4. A low oil level causes gas to exit via the oil output causing high pressure down-stream (pressure builds up on pump)	1,2,3,4,5,6,7	none	1. Apply condition monitoring for motor 2. Ensure regular motor maintenance

In Table 2, the first two columns are selected process parameters and the guide words that can be selected from guide words list in traditional HAZOP. These two columns are combined to comprise the third column, that is, deviations. The fourth and sixth columns are filled in with results obtained from traditional HAZOP as causes and consequences for the deviation in third column, respectively.

The explanations of numbers in MFM-based causes and consequences refer to Tables 3 and 4. The gas out pipeline of the separator blocked as a cause for a deviation of higher pressure in Table 3 as an example illustrating the feasibility of the methodology for qualitative hazard analysis. The MFM-based consequences are the same as the results from a traditional HAZOP analysis. Increasing pressure in the separator will push the oil level lower, which in turn will press the water level lower inside the separator. If the safety valve failure to open on the separator, then this would eventually result in gas flowing toward the oil processing equipment through 23PA0001 and 23LV0002 and eventually toward the water processing equipment though 23LV0001. The remaining consequences from the MFM-based method and the traditional method for the same cause of a given deviation in Table 6 can also be compared in this way.

Table 3. Interpretation of each root cause

ID number	Root causes	Interpretations
1	Bal7fill	Pipeline joint is blocked
2	Bal9fill	Anti-surge valve stucks
3	Bal5fill	Low inlet gas flow to compressor due to plugging gas pipe
4	Sin12hivol	Polytropic efficiency of compressor is degrading
5	Sou9lovol	Motor failure

Table 4. Interpretation of all possible consequences for all root causes

ID number	Possible consequences	Interpretations
1	Sin13lovol	The compressor mechanical energy loss is reduced
2	Sin12lovol	The useful work of compressor is reduced
3	Sou2hivol	Inletflow of Feed2 is low leading to source of Feed2 flow, finally low level of oil and water, gas could exist via the oil output causing high pressure downstream
4	Sou1hivol	Inletflow of Feed1 is low leading to source of Feed1 flow accumulated, finally low level of oil and water, gas could exist via the oil output causing high pressure downstream
5	Obj3 false1	Compressor surges
6	Sin3lovol	Gas production is low
7	Sto1hivol	Gas mass in separator is high, which means separator pressure is high
8	Obj3 false 2	Compressor is blocked
9	Sou9hi	Electric energy for motor is accumulated

We filled in existing protection for each consequence and the required action. And the required actions in HAZOP worksheet are reflected in the P&ID diagram shown in Figure 9. From a means-end relation perspective, Figure 9 represents three strategies for process design to minimize hazards and perform the required safety function. The first strategy is the adequate level of redundancy in plant. This strategy displayed in Figure 9 is the redundant critical manual valves and stand-by pumping system. By redundancy, the end can be realized by the optional means with the same performance. The second strategy is improvement of system independence level. This strategy employed in Figure 9 is the indicators and alarm system. By installation of these devices, the spurious operation or failure of transmitter or controller could be displayed. The third strategy is the diversity. For example, during the start-up of the pump, the pump valve is hard to open, to allow proper starting and operation, the kick-back line is installed to pump as shown in Figure 9. Alternatively the gas or turbine driven pump could be provided in addition to the electric motor driven pump.

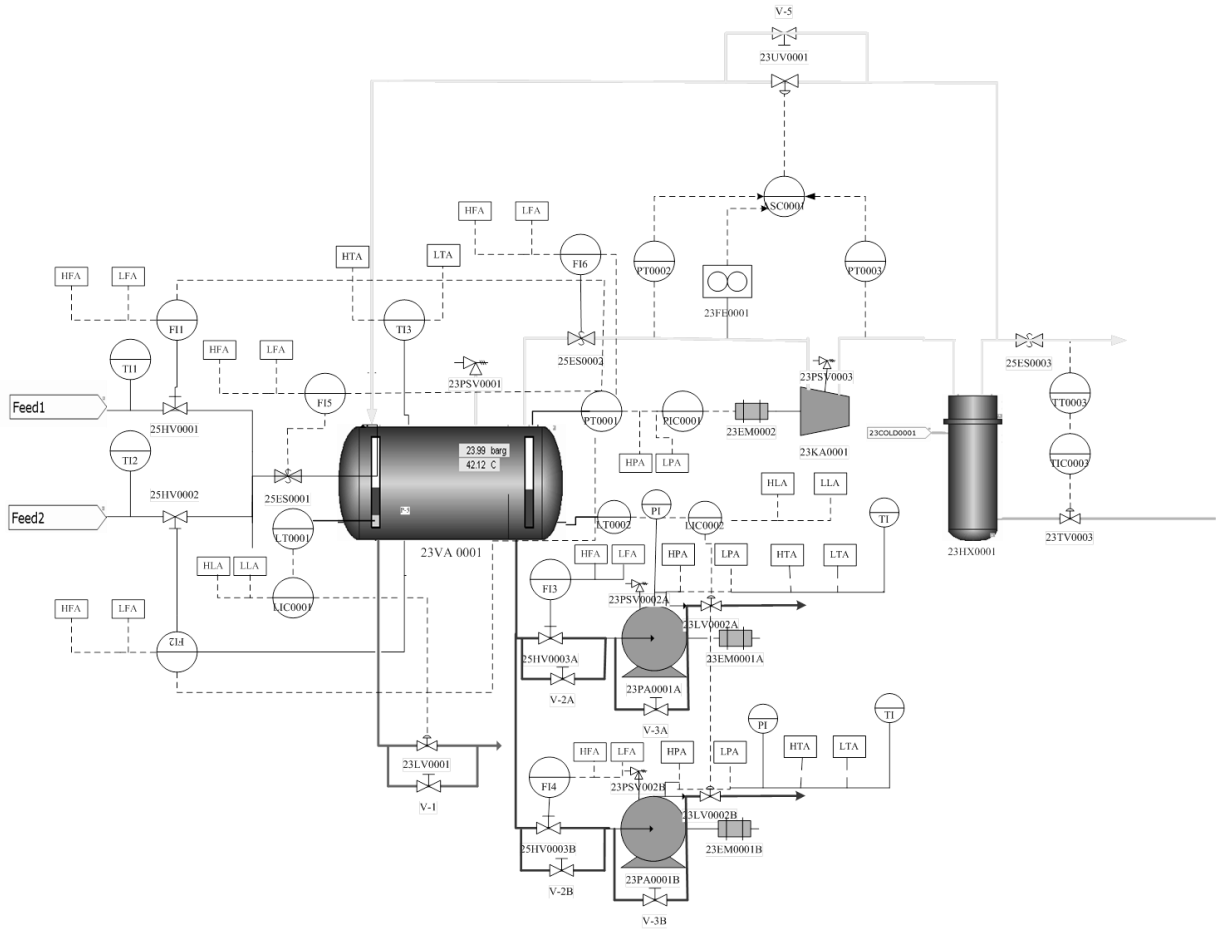


Figure 9. Modified P&ID diagram for section 1

4.3 Using the Risk Matrix for Qualitative Risk Assessment (3rd step)

Following step 3 of the methodology, the likelihood and severity of each cause-consequence path is evaluated by using the risk matrix as shown in Figure 10. The pairwise numbers indicate a cause and consequence path. The numbers in the figure represent the scenarios (possible cause-consequence paths for higher pressure of separator) analyzed in Qualitative HAZOP analysis section above. And high potential risk hazards are marked by dark grey color. The total number of high potential risk paths is 20. Among them, the consequences of higher pressure in separator, compressor working condition towards surging or block, oil escaping via oil output line leading to high downstream high pressure, low water level and low oil level are of considerable interest because the consequences have several causes. These are the causes that can lead to high risk consequences. An evaluation of the severity of these consequences will require detailed quantitative dynamic simulation to be examined in the following step.

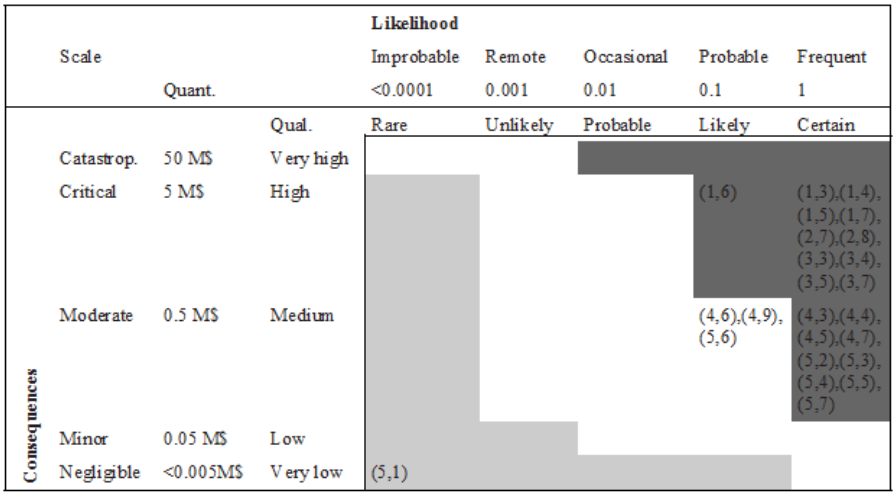


Figure 10. Risk matrix for higher pressure deviation of separator

4.4 Validation of The Qualitative Analysis (4th step)

Step 4 of the integrated methodology is applied in this section, to demonstrate the validation methodology for the qualitative analysis. Configuration of the quantitative dynamic simulation by software K-spice®, measured variables and normal operation conditions are omitted here. The linking of the qualitative analysis outputs as input for quantitative dynamic simulation is shown in Table 5, where each root cause is represented by a corresponding failure scenario. The detailed quantitative analysis is represented in Table 5 for one of the failure scenarios in Table 6, namely the failure of the control function of the anti-surge valve (UV0001). The consequences of the other root causes are summarized in Appendix B. The normal valve fractional position in the anti-surge pipeline is 0.5. In this failure mode, the valve position was assumed to be stuck at 0.9 fractional position. This means that the normal anti-surge loop mass flow (pf_25ES0006) is 1.94 kg/s, while when the anti-surge valve get stuck at 0.9 fractional position the mass flow increases to 47.22 kg/s

Table 5. Generation of failure scenarios from qualitative analysis to quantitative dynamic simulation as input to K-Spice®

Root cause ID number	Qualitative function name	Function states	Equipment	Failure mode	Process input variable
1	Balance 7	fill	Heat exchanger 23HX0001_tube	plugging	Plugging fraction 0.8
2	Balance 9	fill	Anti-surge valve (UV0001)	stuck	Stuck position 0.9 fraction
3	Balance 5	fill	Outlet gas pipeline from the separator	plugging	Plugging fraction is 0.8
4	Sink 12	high	Compressor	Polytropic efficiency deterioration	Deterioration fraction 0.8
5	Source 9	low	Motor (23EM0002)	Mechanical failure	The machine failure is true

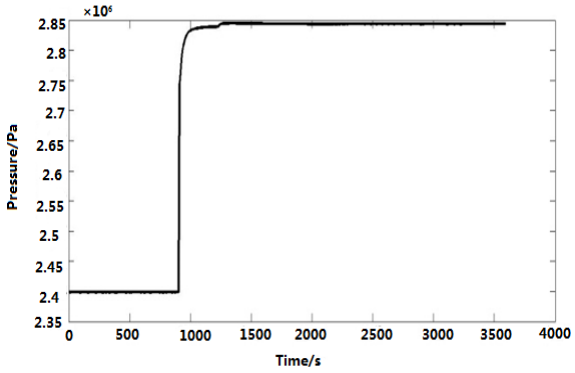
Table 6. Consequences of anti-surge valve stuck at 0.9 fractional position failure scenario

Cause ID number	Failure scenario			Equipment	Process parameters						Consequences
	Failure mode	Parameter value			T[K]	Lw [m]	Lo [m]	Lt [m]	P[10^6Pa]	F[kg/s]	
					Failure value						
2	Anti-surge valve stuck at 0.9 fractional position	0	0.9	Pf_25HV0001 Pf_25HV0002 Separator Heat exchanger tube Export oil Export gas Export water Pump Compressor Anti-surge loop	318.15 317.55 317.25 318.15 315.35 313.95 316.15 317.15 369.25 308.85	0.05	0.15	0.156	2.98 2.98 2.84 5.00 2.85 2.84 2.85 5.73 5.04 2.85	61.11 53.33 114.72 84.17 73.89 84.44 73.89 73.89 84.44 47.77	The pressure of the separator rises up from 2.4×10^6Pa to 2.84×10^6Pa within 180s. The separator shifts from original steady state to another new steady state. To control the growth of separator pressure, the outlet gas flow rate from the separator increases. The working condition of the compressor is approaching a blocking state

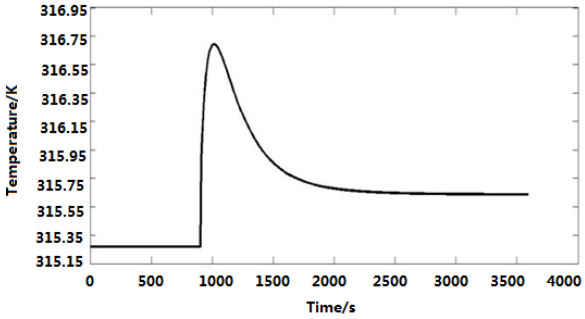
The failure scenario of 0.9 fraction leakage of the anti-surge valve (cause 2) is introduced after the simulator has been running in normal state runs for 900s. The failure scenario trend time is 2700s and the simulation results are recorded for every 8s. The simulation results are shown in Figure 11- 13. The pressure of three phase separator rises from 2.4MPa to 2.84MPa within 3 minutes. The growth of pressure is in accordance with the evaluated risk by the qualitative risk matrix of the cause-consequence path (2, 7) identified by the functional model. The temperature of three phase separator climbs to a peak at 316.65K and comes down to another stable state at approximately 315.55K, which has little impact on the separator (See Figure 11). Whereas the water-oil interface level and oil level in the separator are only decreased a little in a very short period then moves back to the normal state. We can see the separator shifts from the original steady state to a new steady state. The control loop for the separator pressure plays an important role in controlling pressure increases. Due to the loop, the outlet gas flow rate from the separator increases from 40.55kg/s to

84.44kg/s. (See Figure 12) Accordingly, the inlet volume flow rate for the compressor increases from 1.98m^3/s to 3.6m^3/s, and the head-flowrate performance curve of the compressor in Figure 13 shows that the working condition of the compressor is approaching a blocking state. So this behavior is regarded as highly unacceptable, which is in accordance with the cause-consequence path (2, 8) identified by the functional model.

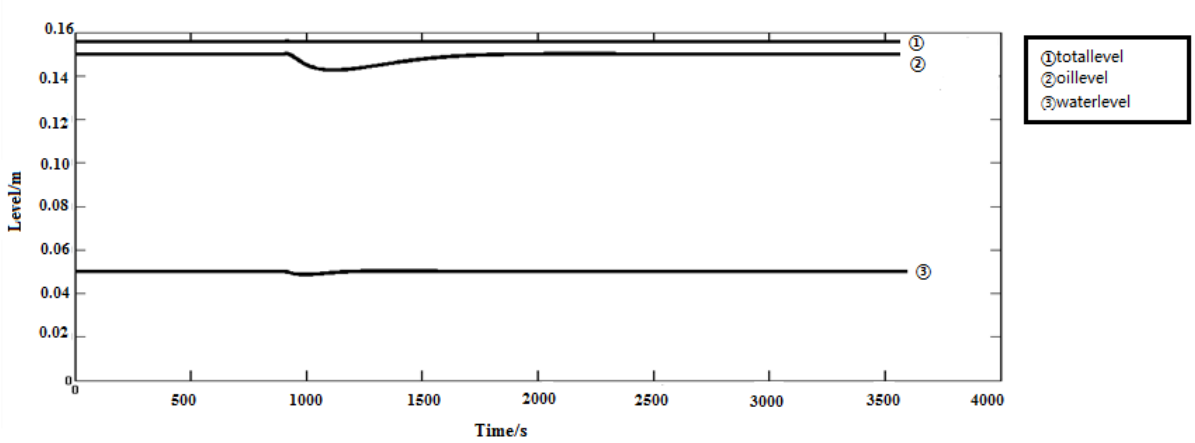
The consequence analysis of the other failure scenarios in Table 5 summarized in Appendix B, validate the cause-consequence paths in highly risk area in the risk matrix. What is more, the quantitative dynamic simulation allows the HAZOP meeting to give priority to high risk scenarios. For example, in the five failure scenarios, mechanic failure of the motor for the compressor is the most dangerous situation because the operators cannot be expected to be able to cope with the motor failure within a short time period. Thus if the emergency trend has been observed, the proper action is to shut down the process following the shut-down procedure in the operation manual. It suggests that condition monitoring of the motor indeed should be applied as is normally done using an alarm system for the motor.



(a)Pressure of the separator



(b) Temperature of the separator



(c) Level of the separator

Figure 11. Changes in operating condition of the three phase separator when anti-surge valves stuck

(a)Pressure changes (b) Temperature changes (c) Level changes

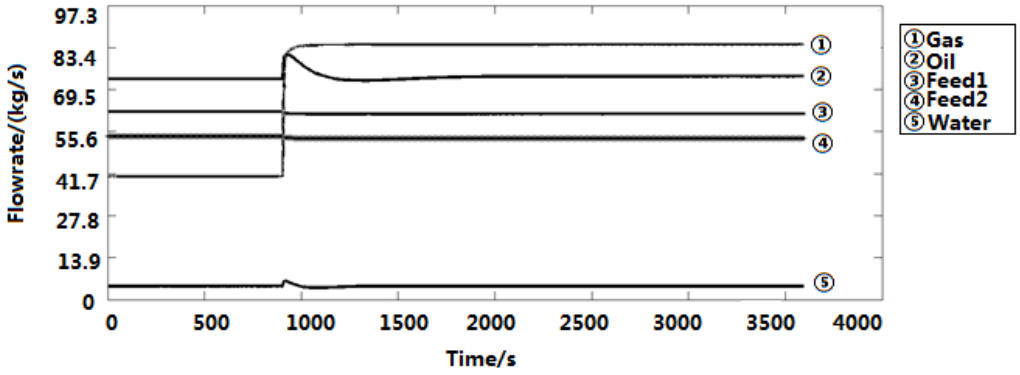


Figure 12. Mass flow rate changes of feed flows, separated oil, water and gas flow when anti-surge valves is stuck

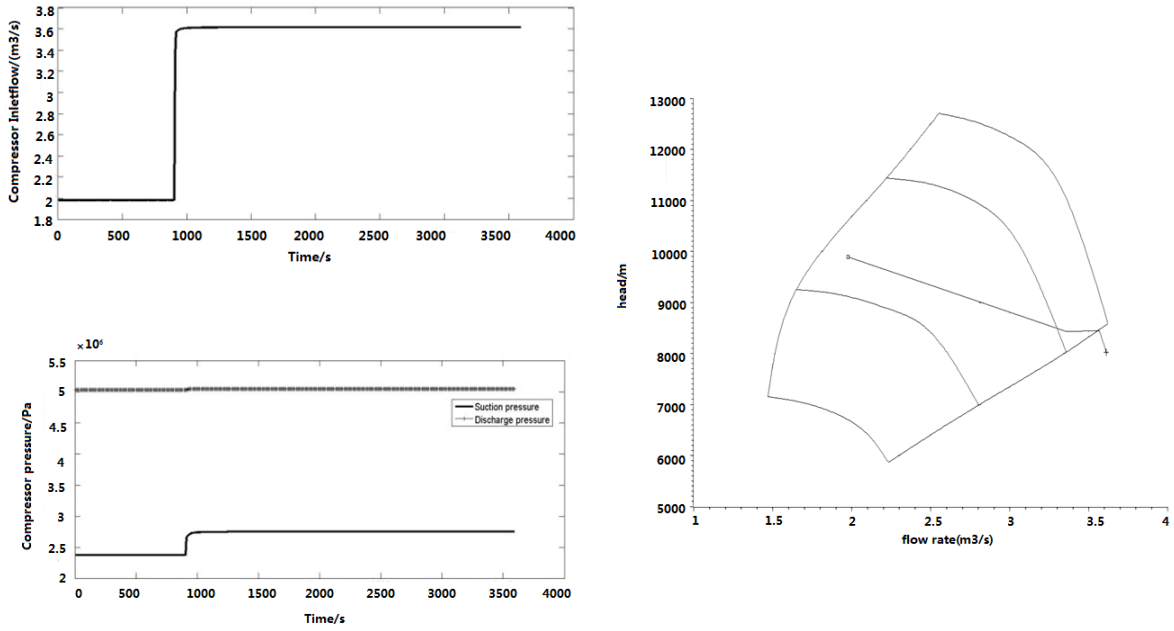


Figure 13. Changes in operating condition of the centrifugal compressor when the anti-surge valves is stuck

4.5 Real-time Simulation of Transient Behavior and Quantification of Deviation Scenarios(5th step)

The purpose of the quantitative analysis for serious failure scenarios is to make a detailed investigation of the transition of the process state from deviation via abnormal and critical to catastrophic. The failure scenario with plugging of the separator outlet gas pipeline (root cause 4) is selected as an example. This failure could happen due to hydrate formation. At normal condition, the mass flow rate is 40.55 kg/s at a plugging fraction at 0. In the K-Spice® dynamic model, the plugging fraction is set to simulate a failure

scenario. The plugging fraction is increased successively from 0.1, 0.2 ….to 0.9, and to simulate an extreme abnormal situation, 0.95 fraction and 0.98 fraction we also introduced. The results are sampled every 48s. It is assumed that the other equipment state is normal at the beginning of the simulation.

We monitored the variables and determine whether the changes can satisfy the safety demands. The plugging fraction deviation will be quantified. The influences of the plugging fraction upon other parameters changes are shown in Figure 14-17. Along with the successive changes of separator outlet gas pipeline plugging fraction with time in Figure 14, the pressure of the separator starts to increase after the plugging fraction increases to 0.7. And the temperature of the separator goes through a similar trend as shown in Figure 40. At a pipeline plugging fraction of 0.9, the separator pressure dramatically rises to 4.8MPa. The transients of oil level and water level inside the separator during the time period where the plugging fraction changes from 0.7 to 0.9 can be observed in Figure 15. After the plugging fraction increases to 0.9 the centrifugal compressor surges, as can been seen from the performance curve of centrifugal compressor in Figure 17. By investigating the other parameters, it can be seen in Figure 16, that the water level is almost 0. In other words, since the pressure rises above the safety relief pressure limit, the three-phase separation process is at a *catastrophic* state. (Referring to Table 7) All the quantitative results validate the unacceptable high risks resulting from the cause-consequence paths derived from the qualitative functional modeling. Furthermore, the deviation of the plugging fraction can be quantified as shown in Table 7. From the 0-0.6 plugging fraction, the process state is deviating. If the plugging fraction increases further to be in the range between 0.6 and 0.8, the process state change from the deviation to abnormal. More seriously, if there is no counter measures taken to control the deteriorating trend, the process state turns into the critical situation when the plugging fraction is in the range 0.8-0.9. Beyond the plugging fraction 0.9, the process state can be *catastrophic*.

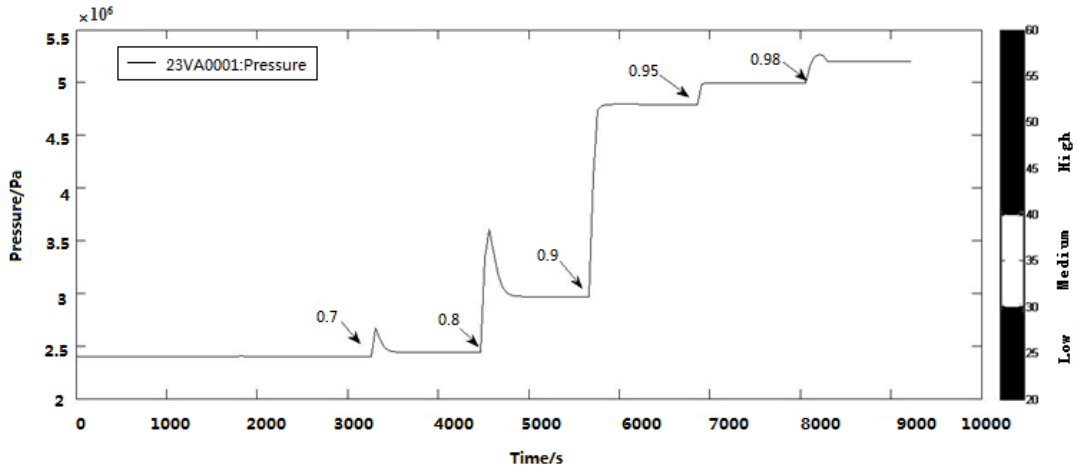


Figure 14. Pressure changes of the separator along with the changes of separator outlet gas pipeline plugging fraction

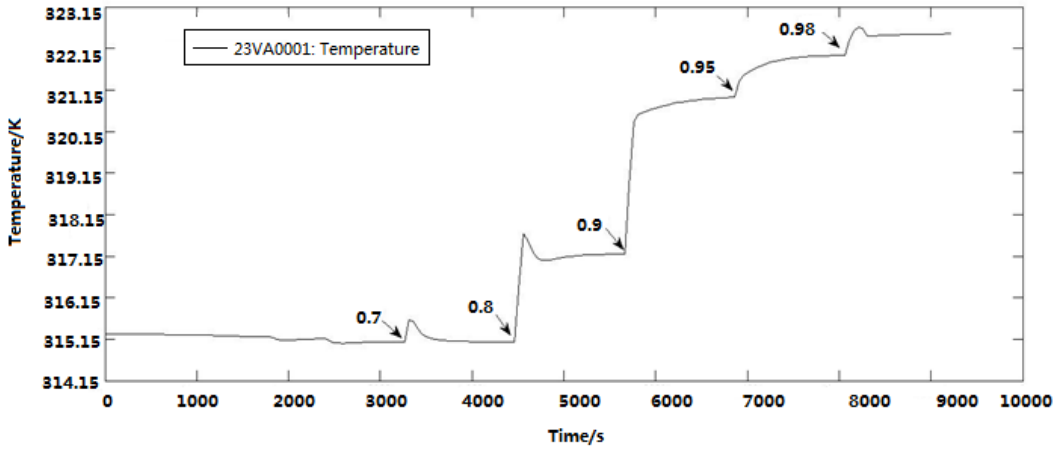


Figure 15. Temperature changes of the separator along with the changes of separator outlet gas pipeline plugging fraction

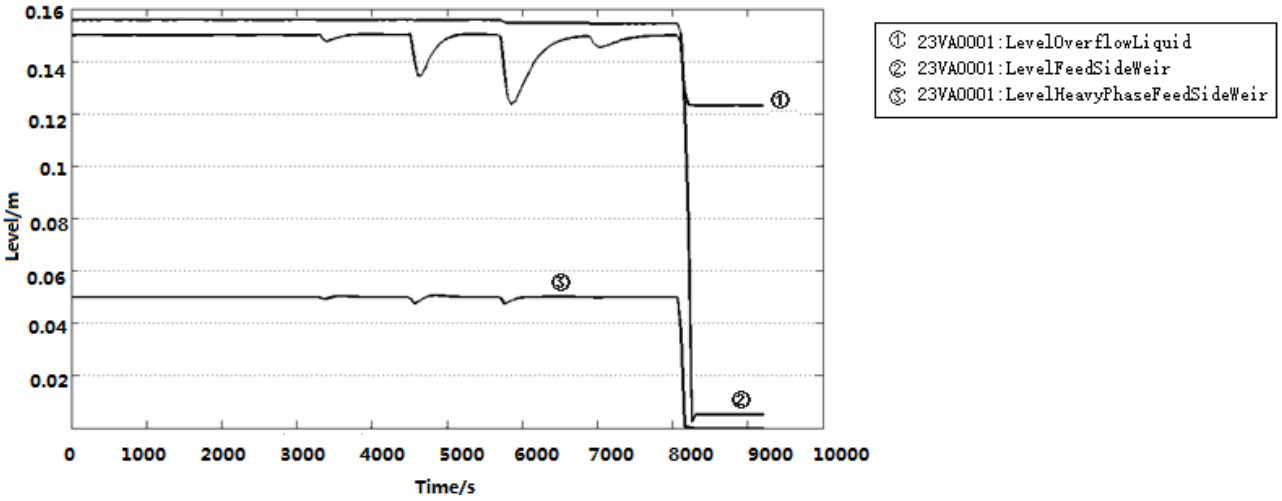
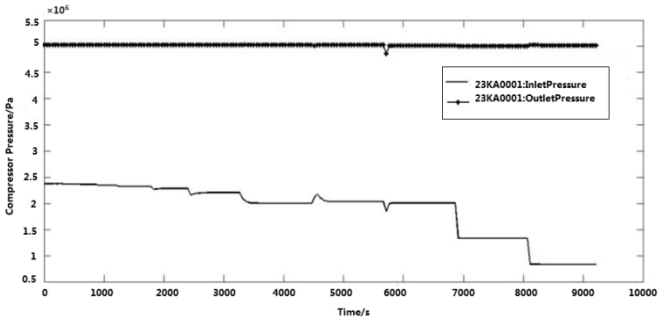


Figure 16. Level changes of the separator along with the changes of separator outlet gas pipeline plugging fraction



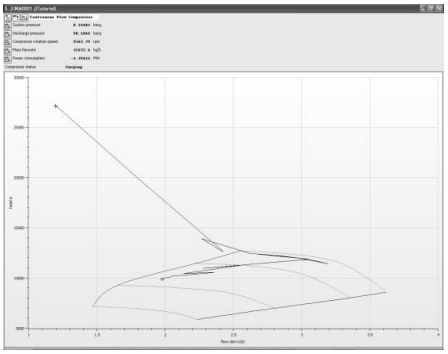


Figure 17. Changes in operating condition of centrifugal compressor along with the changes of separator outlet gas pipeline plugging fraction

Table 7. Quantification of the plugging fraction deviation

Process state	Deviation	Abnormal	Critical	Catastrophic
Plugging fraction	0-0.6	0.6-0.8	0.8-0.9	0.9-1

5 CONCLUSIONS AND COMMENTS FOR THE INTEGRATED FRAMEWORK

5.1 Conclusions

To systematically identify cause and evaluate the potential effect of a failure, an integrated system safety analysis and risk assessment method was innovatively proposed. And the functional knowledge-based tool for computer-aided HAZOP study was implemented. Firstly, cause-consequence reasoning of identified different failure scenarios based on MFM model was performed. Secondly, qualitative risk assessment matrix was used for screening the unacceptable failure scenarios with high risk. These high risk failure scenarios were simulated in quantitative simulator. On one hand, it validated results of the qualitative risk assessment. On the other hand, it quantified the process deviations. Finally, the safety precautions were put forward. The integrated method was successfully applied to the three-phase separation process system. The application provided a good test for the integrated methodology and the computer-aided tool, MFM editor and cause-consequence reasoning capability of the MFM reasoning engine. The methodology generated a HAZOP worksheet which resembled quite closely that obtained from a traditional HAZOP.

The research revealed feasibility and a promising potential of the integrated knowledge-based tool to assist both the more trivial tasks involved in a HAZOP and in particular also some of the more complicated analyses of high risk hazards. Consequently it potentially contributed to better use of resources and time for a HAZOP team. The integrated methodology could be suitable already at the FEED (Front End Engineering Design) stage of process development as well as other stages of the plant life cycle.

5.2 Comments

The work has been cited by books [54] and journal papers [55]. The comments of the reviewers and citations are: “The method developed has a good potential to improve the Hazop process and will on the longer term contribute to increasing efficiency.”, “The method shows equipment objectives and functions, and it describes e.g., dynamic simulation in combination with interactions of mass, energy and information flows, combined to flow structures, it increases HAZOP efficiency also for reliability.” The approach has been caught attention and was cited in the following Table 8.

Table 8. Various, relatively recent approaches to support and to(semi-) automate HAZOP from Table 7.5 in Book of Risk Analysis and Control for Industrial Processes - Gas, Oil and Chemicals: a System Perspective for Assessing and Avoiding Low-probability, High-consequence Events.

Year	Authors	Approach
1995	Vaidhyanathan and Venkatasubramanian[14]	*Digraph*-based HAZOP. Digraph is explained in Chapter 8, Section 8.3.2. Basically it is modeling material and information flows initiating or undergoing changes.
1996	Vaidhyanathan and Venkatasubramanian[15,16]	HAZOPExpert is a *DiGraph* (HDG) model-based, object-oriented, intelligent system for automating HAZOP. The *expert system* is provided with semiquantitative reasoning that is checking whether, in case of loss of containment, conditions surpass the autoignition threshold and whether a spill presents a toxicity risk. It further checks the adequacy of protective devices and ranks consequences.
1998	Srinivasan and Venkatasubramanian[17]	HAZOP applied to batch processes (with additional challenges compared to continuous process of operator procedures and actions, and discrete process steps). This is realized by *Timed Petri Net* (see Section 7.8) representation of the batch process and DiGraph to represent causal relations between process variables in sub-tasks. In combination with the earlier *expert system* work it constituted the batch HAZOPExpert.
1999–2000	McCoy et al.[11,18]	Software system HAZID consisting of several modules: AutoHAZID is the heart of the system. The description is quite detailed. It has at the start a configuration checker after the program read in the plant description and built a Signed DiGraph (SDG) of the process units. It further has a qualitative effects module. The HAZOP emulation module was developed in the earlier STOPHAZ project. It is *a rule-based inference engine* generating scenarios. VTT (Finland) contributed with a fluid library and fluid rules distinguishing feasible from infeasible scenarios. Fault propagation was modeled by means of SDG. The output is filtered to remove redundant information.
1997–2000	Khan and Abbasi[19,20]	Development of a procedure to speed up "HAZOP-ing": optHAZOP, followed by development of a *knowledge-based inference engine* software tool enabling automation. The tool consists of a general and a process specific part. It generates deviations and contains rule-based trees linking process specific attributes, via process parameters, and deviations to causes and consequences. Renamed from TOPHAZOP to EXPERTOP.
2005	Zhao et al.[21]	Software system PHASuite: Instead of DiGraph the process is now represented by *colored Petri net* (see Section 7.8), but the Petri net also represents the methodology to perform the HAZOP. The process is abstracted to two levels: operation and equipment, which have been functionally linked. Knowledge is externally stored in layered operation and equipment models in a structured database that can be approached by a user via knowledge builder. A *case-based reasoning engine* (CBR, stories containing knowledge/experience from experts) operating on two levels and two layers performs the automated HAZOP. Application is again to pharmaceutical batch processes, more difficult to HAZOP than continuous ones. Gain in time spent is about 50%.
2008–2009	Cui et al.[22]; Zhao et al.[23]	As an extension of the digraph method of Vaidhyanathan and Venkatasubramanian,[15,16] a *Layered DiGraph* (LDG) expert system was proposed. The digraph is now three-dimensional, which enlarged the flexibility and knowledge storage capability. Each layer or workspace is associated with a guideword. The workspaces contain nodes representing variables interconnected by (unsigned directed) arcs, implying that the deviation in the "parent" node determines the direction of deviation in the "child." Linked nodes can also be in different workspaces. The authors claim that a higher degree of completeness of HAZOP scenarios is achieved. Later the same group developed *PetroHAZOP*, an expert system but this time it is learning by *case-based reasoning* (see PHASuite above) making use of CAPE ontology (explicit specification of conceptualization) for process systems. A case consists of problem/situation, solution, and outcome description. A new problem is judged on similarity by an algorithm based on predefined indexes. It is thus highly domain dependent. It functions in the Chinese petrochemical industry with 900+ cases. A future effort was announced to combine the two approaches.
2009	Rahman et al.[24]	Further development of Khan and Abbasi's EXPERTOP to ExpHAZOP+ with some added features as an enhanced graphical user interface (GUI) and a selection method for an equipment node. It also added an update possibility of the knowledge base and introduced a unique *fault propagation algorithm*, identifying downstream causes and consequences from an identified upstream event.
2010 2014	Rossing et al.[25] Wu et al.[26]	*Multilevel flow modeling* (MFM), developed by coauthor Lind in the early 1990s, is applied to describe the plant goal-function structure. MFM can be used at various abstraction levels, applies symbols (of which a few resemble Petri net ones) for objectives (source, transport, storage) and functions (sink, barrier, balance), and it describes the interactions of mass, energy, and information flows, combined to flow structures. Also, symbols are available for functions as management, decision, and actor action. Further, a set of means-to-ends relations (with symbols for produce, producer product, maintain, and mediate) and causal roles (with condition, agent, participant symbols) describe dependencies between functions. The interconnected flow structures to achieve a goal are represented graphically. Combined with a rule-based causal reasoning engine, and quantitative dynamic simulation (with e.g., HYSYS), MFM can generate fault/cause and consequence trees/paths for a given deviation in a system function, and with a goal reasoning engine goal trees. The different trees can be used in reasoning to develop counteraction plans. The whole is called MFM workbench. After process variable deviations have been specified, the workbench facilitates HAZOP as a functional assistant by diagnosing the causes of abnormal situations. It does not have the aim of automating HAZOP. The concept is further elaborated, extensively described, and demonstrated on an offshore three-phase separator case by Wu et al.[26]

Continued

Table 7.5 Various, Relatively Recent Approaches to Support and to (Semi-)automate HAZOP *Continued*

Year	Authors	Approach
2012	Rodriguez and De la Mata[27]	*D-higraphs* are another way of modeling a process including controls. Developed in the late 1980s, D-higraphs represent in yet another way states (blobs, being a function effected by an actor—a machine—with an optional condition as a Boolean variable) and transitions (edges). Hence, D-higraphs combine in their representation function and equipment/structure, so there is more direct correlation with the real installation than with MFM. Distinction is made between mass, energy, and information edges. There are process (green), control (orange), and mixed (blue) blobs. The edges can be triggered or fired resulting in state changes. A blob can contain other (sub-) blobs and can also be partitioned to represent an OR-statement. Causal rules have been established. The system description is in three layers: structural, behavioral, and functional. Deviations are coded and the reasoning engine is constructing cause and consequence trees. For comparison the same distillation unit was "HAZOP-ed" as Rossing et al. did. The D-higraph HAZOP assistant results were not different.
2012	Hu et al.[28] Hu et al.[29]	Having in mind prognosis for enabling predictive maintenance to prevent process upset a HAZOP method was developed assisted by a *dynamic Bayesian network* (DBN), see Section 7.5. Application was for a gas turbine plant where wear, fouling, and corrosion lead to faults. A DBN was chosen because process faults often have multiple propagation paths to different effects, some of which propagate to adjacent parts. This may lead to fault coupling and disaster. A DBN can represent these interactions in space and time by conditional probabilities. Variables are represented by nodes and the causal structure between variables by edges (arcs). Degradation of components is modeled by a distribution, for example, Weibull. Observable variable values can be obtained from the supervisory control and data acquisition (SCADA) system. Then, DBN-HAZOP can predict failure before it occurs.

However, the maturity of the proposed qualitative and quantitative framework to automate each complicated task of HAZOP for industrial scale process is still insufficient. We can call the tool as MFM-HAZOP. If a HAZOP team carries out a study using the tool, more efforts to define the study scope, divide nodes are embedded and shifted to modeling work in the framework. This requires a fundamental procedural change for implementing HAZOP. Future work listed in the next section is to improve the quality of the HAZOP study aided by the tool in terms of efficiency, consistency, coverage, credibility, and so forth. On the other hand, the future study lines also consolidate the MFM method theory foundation and modeling itself for better feasibility.

6 ON-GOING AND FUTURE RESEARCH

6.1 Knowledge acquisition toolbox

Normally, it takes long time to carry out hazard identification because searching of proper information in the relevant documents tends to be time-consuming. In order to satisfy industrial needs of efficiency and low risk, it is necessary to develop methods and tools for computer assisted importing from existing plant documents such as P&IDs, design specification data, process chemistry, and design information on currently installed/considered protection layers and subsequent mapping of the information into MFM models. It is the first step of automated generation of MFM models from plant documents.

In order to facilitate automatically generated MFM models, a knowledge acquisition tool of process systems should be integrated with modeling methods and tools such as piping and instrumentation diagrams and a computer aided design package. Because such diagrams explicit annotations about material and energy flows and their paths and explicit descriptions of the functions of plant components and subsystems defining their functions by transformations and interaction of the energy and material flows. In the tool, rules should be developed to map this information into diagrammatic form representing relations between flows and components/subsystems. These diagrams can be seen as a kind of an abstracted MFM model.

6.2 Knowledge representation toolbox

Current model building is supported by graphical editors and reasoning systems which are used to capture and validate model information. But constructing the model is essentially a manual process which requires knowledge of MFM concepts and theory and experience in model building. This approach to model building has been adequate for research purposes, but from industrial perspective it is both ineffective and risky. However, the possibility and degree of full automated generating MFM models which can be obtained is presently unknown and should be helped and evaluated with a MFM modeling libraries. Building of the library can be based on a systematic ontology-template based MFM modeling methodology. Each template for a function is represented by MFM modeling patterns. The knowledge representation toolbox should realize modeling templates library of MFM models, model storage, re-use and update, aggregation of each template of MFM patterns into a comprehensive plant model, model verification/validation.

However, to build such knowledge representation toolbox by MFM modeling method faces some challenges associated with the fundamental modeling theory in MFM. As follows, each challenge is clarified and summarized.

1. Formalized and systematic semantics of functions and means-ends relations. Basic semantics of function primitives and means-ends relations in MFM models are formulated and clarified well. However, the semantics of some functions especially such as energy conversions context is not explored much. The differences between producer-product and mediate means-end relations are not formulated well yet. Therefore, extending or clarifying semantics is required to better explicitly and accurately represent

knowledge of the system.

2. Consistent roles ontologies. Roles can be seen as binary relations between an action (function, e.g., transport) and the concrete structural entities serving the roles, that is, the pump and the water. They can also be seen as representing structural entities of the plant in the context of plant goals and functions and are, therefore, conveying information about purposes of these elements. The roles can improve the model expressivity. It requires establishing consistent role ontologies to represent their functionality.

3. Represent control on several levels of means-end abstraction. To help with identification of operability problem, critical task is to incorporate the control information process into the model. The control flow structure is intended to represent the process of observing, assessment, plan and execute to the flow function. However, the semiotic aspects of control are not explicitly modeled in the control flow structure. The states of different types of functions can be indicated by what process parameters are not defined. Also the means used to achieve the control objective is presently not represented. This lack of information in model prevents the model ability to cope with control problems.

4. Aggregation of MFM patterns. The MFM patterns template for an equipment item needs a formalized procedure and method to be combined with other MFM patterns templates for other equipment so that it can be aggregated into a complete plant model. The model aggregation may be realized by a procedure based on the connection between means-ends relation and connecting functions representing interaction between equipment. It requires research efforts.

5. Methods for model verification/validation. To produce reliable results based on MFM models, it is necessary to perform model verification/validation. Validation of each template may be based on a general hypothetical-deductive-test procedure. MFM model patterns of each template and aggregation of templates into a comprehensive plant model based on the proposed general validation method can be validated through interviews, operational procedures, FMEA analysis, HAZOP analysis and quantitative simulator.

6.3 Hybrid qualitative and quantitative reasoning system tool

It is necessary to rank the consequences and to remove the less significant, and less-likely. Even if a consequence is retained as significant, there can still be a problem with an excessive number of causes, most of which are unimportant. This requires specific treatment. A hybrid qualitative and quantitative reasoning system may accomplish the task. The following sections pointed out the improvement space for current MFM reasoning system and how a quantitative reasoning system can be facilitated for pruning reasoning cause-consequence paths, which signifies that a hybrid qualitative and quantitative reasoning system tool is needed.

6.3.1 Rule-based MFM reasoning system

The reasoning of an MFM model is based on cause-effect relations. These casual relations are generalized, i.e. independent from the modeling object. Limited to MFM language syntax rules, MFM model reasoning library is comprised of a fixed pattern of inference rules. However, there are several aspects to improve in the reasoning system and these features are required to be developed.

1. Dynamic reasoning. Although the reasoning system used for HAZOP does not require dynamic reasoning, it is essential for real time alarm system for finding plausible root cause. The states of functions need to be updated along time, based on the updated states to dynamically trigger fault and consequently

using dynamic reasoning; the identification process of faults detention and diagnosis becomes dynamic. It is critical for tackling tasks of fault diagnosis or alarm tracking based on real time online-data in industry.

2. Reasoning about control. In a HAZOP study, a type of causes for a deviation may fail due to the transmitter or the control system out of function. Some accidents report also point out such causes leading to a disaster to happen. However, currently the reasoning about control is missing. Therefore, such malfunction of control system causes identified is purely manual process.

3. Reasoning about objectives/goals. Current objectives/goals in MFM models are assigned two states: true and false. If the state of associated function to realize the objectives/goals is not normal, then the state of objective/goal is false. This lacks of reasoning about the task fulfillment satisfaction degree or quality. If a modified reasoning about objectives/goals, it may decrease the ambiguity of HAZOP results.

4. Reasoning about function and structure relation. Because the generic formalized representation of relation between MFM patterns and a structure is missing, the reasoning of such relation is not in place as well. However, the drawback leads to difficulty in interpreting reasoning results for HAZOP in structural level and let alone completeness.

6.3.2 Quantitative reasoning

The reasoning methods presently used for MFM for cause and consequence analysis generate failure paths without taking into account the probability of each cause-consequence path. With the support of roles ontology linking function and structure, the description of the components failures and reliability may be made at the level of structure, quantitative reasoning system such as Bayesian inference system may be able to be adopted for pruning less likely causes in identified cause paths for scenarios. It takes advantage of Bayes theorem to update the probability of events given new observations, called evidence, to yield the posterior probability.

Although, it is intuitive to see the possible connection between qualitative and quantitative reasoning system, it demands exploration for how to integrate the two reasoning method.

*6.*4 *Integrating qualitative knowledge and quantitative knowledge for process safety verification*

As demonstrated with the offshore three phase separation process, when the quantitative knowledge for the process is available, it can be used to prune redundant paths in the cause or consequence trees obtained from the qualitative analysis. This means that only the validated paths are kept. Such advantage could be helpful for ensuring more consistent results from qualitative analysis. As regards pruning and validation, the feedback from quantitative to qualitative modeling has been demonstrated on selected specific cases in the present study using process insights and expert judgment. Conversely, the development of a more general and systematic methodology for pruning is needed and expected to be straight forward, since pruning is related to reduce the space of possible consequences from a qualitative reasoning engine using the information obtained from quantitative simulation. Therefore this remains as an interesting and challenging opportunity.

6.5 Explanation and Communication toolbox

As can be seen in the MFM-based HAZOP results, the results are represented obscurely without linguistic description. It requires a natural language explanation tool to explicitly explain the represented scenarios which easily can be understood by designer or operator. Accordingly, improved user interface for MFMSuite is necessary as well. Such explanation and communication toolbox will also be beneficial for validation of MFM models by comparing results and behavior of the system efficiently. Such toolbox should be computer-aided for better implementation.

6.6 Auxiliary toolkit

Auxiliary toolkit is intended to facilitate additional information storage for helping with HAZOP analysis. Inside the toolkit, the FMEA analysis of equipment item should be found in order to validate each template of MFM patterns of equipment, which can really represent failure scenarios. It also gives the implication of each template modeling details.

7 DISCUSSION AND PERSPECTIVES

From the case study results, some significant features of qualitative models, risk matrix, quantitative models in the framework for computer-assisted HAZOP studies are discussed below:

First, MFM models capture deep knowledge of systems e.g. objectives and functions of systems to represent designed system working mechanisms. It also provides faster reasoning of deviation from intentions. This enables better solutions than Shallow knowledge-based methods. Because shallow knowledge base collect all pertinent HAZOP or known rational variables, so it does not identify unknown or unexplored hazard scenarios.

Second, reasoning capability based on rules in MFM enables HAZOP team to examine the cause/effect of deviation upstream and downstream. This overcomes the limitation of HAZOP restricted into one node study at a time.

Third, the potential hazard scenarios are ranked by risk matrix based on likelihood and severity. Judgment about likelihood, severity and the tolerability of the resulting risk is made on a subjective basis using the empirical knowledge of the HAZOP team members. If more applicable to industry in line with safety culture of companies, the risk matrix can be replaced. e.g. by Maersk Prioritisation Matrix (MPM) tool to be the better fit into safety management in Maersk Oil.

Fourth, within the integrated qualitative and quantitative modeling framework for HAZOP studies, the quantitative analysis using dynamic simulation verify and validate the unacceptable risks identified and evaluated by the qualitative analysis. Moreover, in the case of clearly unacceptable high risk scenarios, the simulation workload for HAZOP deviations can be effectively reduced using the results of the qualitative analysis as the starting point for quantitative simulation.

Fifth, when the quantitative knowledge for the process is available, it can be used to prune redundant paths in the cause or consequence trees obtained from the qualitative analysis. This means that only the validated paths are kept. Such advantage could be helpful for ensuring more consistent results from qualitative analysis.

Sixth, the integrated framework can be used in various stages during the plant life cycle. In the early stage, functional modeling is suitable for qualitative process modeling. For the dynamic modeling, in the later stage has already an appropriate dynamic model. Hence our methodology can be combined to already existing models. Describing the systems qualitatively and quantitatively will take time and efforts such that this step needs to be only performed once. MFM modeling patterns for generic features of basic processes and units need to be developed such that later they can be easily maintained, expanded, and updated. However, as our tools and methods are generic they are ideally suited for reusage of the MFM models at different levels of abstraction. Thereby the generic modeling tools can be directly be applied during other stages of plant development as well as later during the plant life cycle.

Last but not least, it is noted that the aim of qualitative reasoning-based technology for HAZOP studies is not to replace the industry standard HAZOP technique with the HAZOP teams' experiences and insights. Rather it is meant to bring fundamental improvements and support to the HAZOP procedure.

8 CONCLUSIONS

An integrated qualitative and quantitative HAZOP framework for exploring how qualitative models, quantitative models and empirical knowledge contribute to HAZOP studies is proposed. With the case study of an offshore three-phase separation production process, it approves the framework applicability and feasibility. The challenges of improved quality of HAZOP facilitated by such tool named MFMSuite HAZOP are pointed out. Most potential improvement space is the semantic expression of MFM models and reasoning about the control systems. Quantitative reasoning combine with qualitative models and qualitative reasoning may advance accuracy of HAZOP results. More case studies of offshore oil and gas process systems modeled by MFM are needed to enrich the modeling experience for developing MFM model library. The framework can be extended with the available data stream in system life cycle consistent with the core idea of integrated qualitative and quantitative models and reasoning.

In addition, current MFM model building is supported by graphical editors and reasoning systems which are used to capture and validate model information. But constructing the model is essentially a manual process. A framework for automating generation of MFM models is required to make a significant progress towards to the industrialization of MFM methods and is accordingly of importance based on the models automatically generated by the framework for conducting HAZOP studies.

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] Rossing, N. L., Lind, M., Jensen, N., & Jørgensen, S. B. (2010). A functional hazop methodology. Computers & Chemical Engineering, 34(2), 244-253.

[20] Lind, M. (1982). The use of flow models for design of plant operating procedures (Vol. 2341, pp. 23 s.).

[21] Norby Larsen, M., & of Denmark, T. U. (1993). Deriving action sequences for start-up using multilevel flow models (pp. 229 s.).

[22] Rossing N.L. (2006). Method Development for systematic Risk Assessment. Master Thesis. Technical University of Denmark, CAPEC, Department of Chemical Engineering.

[23] Gernaey, K. V. B., Lind, M., & Jørgensen, S. B. (2005). Modelling for control: Understanding role and function of regulatory networks in microorganisms. 16th Ifac World Congress, 16, 13–18.
[24] Us, T., Jensen, N., Lind, M., & Jørgensen, S. B. (2011). Fundamental Principles of Alarm Design. International Journal of Nuclear Safety and Simulation, 2(1), 44–51.
[25] Petersen, C. R., & Lind, M. (1999). A Systematic Approach to Design of Process Displays.
[26] Petersen, J., & Lind, M. (2000). Knowledge Based Support for Situation Assessment in Human Supervisory Control. PhD Thesis. Lyngby, Denmark: Technical University of Denmark: Ørsted-DTU, Automation.
[27] Heussen, K., Lind, M., & Niemann, H. H. (2011). Control Architecture Modeling for Future Power Systems. PhD Thesis. Technical University of Denmark, Department of Electrical Engineering.
[28] Zhang, X., Ravn, O., & Lind, M. (2015). Assessing Operational Situations. PhD Thesis. Technical University of Denmark, Department of Electrical Engineering.
[29] Gofuku, A. (1996). Deriving behaviour of an engineering system from a functional model. Journal of Japanese Society for Artificial Intelligence, 11(1), 112–20, 112–120.
[30] Gofuku, A., Seki, Y., & Tanaka, Y. (1999). Support of conceptual design of engineering systems applying functional modeling. 2nd report, support technique of component assignment to functions by effectively using past cases. Transactions of the Japan Society of Mechanical Engineers, 65(632), 1544-1549.
[31] Gofuku, A., & Lind, M. (1994). Knowledge-based support for efficient design of engineering systems. International Conference on Intelligent Systems Engineering (pp.89-94). IEEE Xplore.
[32] Zhang Q., Yoshikawa H., Ishii H., Shimoda H. (2010). Integrated and visual performance evaluation model for thermal systems and its application to an HTGR cogeneration system. Nuclear Safety and Simulation, 1(3):258-265.
[33] Yoshikawa, H., Yang, M., Hashim, M., Lind, M., & Zhang, Z. (2014). Design of risk monitor for nuclear reactor plants. Progress of Nuclear Safety for Symbiosis and Sustainability: Advanced Digital Instrumentation, Control and Information Systems for Nuclear Power Plants, 125–135.
[34] Dahlstrand F. (2000). Methods for alarm reduction with multilevel flow models of industrial processes. Licentiate Thesis, Department of Information Technology, Lund Institute of Technology, Lund, Sweden.
[35] Dahlstrand, F. (1999). Alarm Analysis with Fuzzy Logic and Multilevel Flow Models. Research and Development in Expert Systems XV. Springer London.
[36] Ohman, B. (2001). Alarm analysis on large systems using multilevel flow models. Ifac Symposia Series, 95–100.
[37] Thunem, H. P. J., Thunem, A. P. J., & Lind, M. (2012). Using an agent-oriented framework for supervision, diagnosis and prognosis applications in advanced automation environments. Advances in Safety, Reliability and Risk Management - Proceedings of the European Safety and Reliability Conference, Esrel 2011, 2368–2375.
[38] Paassen, M. M. V., & Wieringa, P. A. (1999). Reasoning with multilevel flow models. Reliability Engineering & System Safety, 64(2), 151-165.
[39] Souza, L. E. D., & Veloso, M. M. (1996). Flexible planning knowledge acquisition for industrial processes.
[40] Veloso, M. M. . Acquisition of flexible planning knowledge from means-ends models for industrial processes.
[41] Khalil, M. A. R., Ahmad, A., Abdullah, T. A. T., Al-Shatri, A., & Al-Shanini, A. (2016). Multi-state analysis of process status using multilevel flow modelling and bayesian network. , 78(8), 33-41.
[42] Wu, J., Zhang, L., Liang, W., & Hu, J. (2013). A novel failure mode analysis model for gathering system based on multilevel flow modeling and hazop. Process Safety & Environmental Protection, 91(s 1–2), 54–60.

[43] Ming, Y., Li, J., Peng, M., Yan, S., & Zhang, Z. (2006). A Hybrid Approach for Fault Diagnosis based on Multilevel Flow Models and Artificial Neural Network. IEEE.
[44] Wu, J., Zhang, L., Lind, M., Liang, W., Hu, J., Jørgensen, S. B., … Khokhar, Z. U. (2013). Hazard identification of the offshore three-phase separation process based on multilevel flow modeling and HAZOP. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 7906, 421–430.
[45] 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.
[46] Thunem, H. P. J. (2014). The development of the MFM Editor and its applicability for supervision, diagnosis and prognosis. Safety, Reliability and Risk Analysis: Beyond the Horizon - Proceedings of the European Safety and Reliability Conference, Esrel 2013, 1807–1814.
[47] Thunem, H. P. J., & Zhang, X. (2015). The continued development of the MFM suite and its practical application on a PWR system. Safety and Reliability of Complex Engineered Systems - Proceedings of the 25th European Safety and Reliability Conference, Esrel 2015, 2463–2471.
[48] Zhang, X., Thunem, H. P.- J., Lind, M., Jørgensen, S. B., & Jensen, N. (2014). Practical Application of the MFM Suite on a PWR System: Modelling and Reasoning on Causes and Consequences of Process Anomalies.
[49] Searle, J. R. (1995). The Construction of Social Reality. The construction of social reality /. Free Press.
[50] International Standards Organization, Space Systems Risk Management, ISO 17666.
[51] Zhang, X., Lind, M., & Ravn, O. (2013). Consequence Reasoning in Multilevel Flow Modelling. Proceedings of the 12th Ifac/Ifip/Ifors/Iea Symposium on Analysis, Design, and Evaluation of Human - Machine Systems, 12(1), 187–194.
[52] Wu, J., Lind, M., Zhang, X., Jørgensen, S. B., & Sin, G. (2015). Validation of a functional model for integration of safety into process system design. Computer-Aided Chemical Engineering, 37, 293–298.
[53] KONGSBERG K-Spice® Tutorial, Training Manual, May 2012 © Kongsberg Oil & Gas Technologies AS.
[54] Pasman, H. (2015). Chapter 7 – new and improved process and plant risk and resilience analysis tools. Risk Analysis and Control for Industrial Processes - Gas, Oil and Chemicals, 285-354.
[55] Pasman H. ,Rogers W. (2016).How can we improve HAZOP, Our old work horse, and Do more with Its Results? An Overview of Recent Developments. Chemical Engineering Transactions. 48,829-834.

APPENDIX A

The explanations of elements in (flow structures, objectives, relations, functions) in Figure 7 and Figure8 are presented in detail as below.

Elements explanation in MFM model in Figure 7				
Flow structure	**Objective**	**Function name**	**Function**	**Structure**
mfs1:The Feed flow is separated into crude oil, water and gas stream	obj1:Separate gas stream and liquid stream	sou1	Provide feed flow 1	Upstream flow
	obj2:Separate crude oil and water	sou2	Provide feed flow 2	Upstream flow
	obj5: Maintain the oil level in oil chamber	sou6	Provide cold water	Cold water
	obj6:Maintain the water level in water chamber	tra1	Transport feed flow 1	Pipeline
		tra2	Transport feed flow 2	Pipeline
		tra3	Transport gathered feed flow	Pipeline
		tra4	Transport the separated gas	Gas density is lower than the liquid density
		tra5	Transport the separated liquid	Liquid density is higher than the gas density
		tra6	Transport the separated crude oil	Crude oil density is lower than water density
		tra7	Transport the separated water	Water density is higher than crude oil
		tra8	Transport the outflow of the separated water	Pipeline
		tra9	Transport the outflow of the separated oil	Pipeline
		tra10	Transport the separated crude oil	Pump
		tra11	Transport the outflow of the separated crude oil	Pipeline
		tra12	Transport the separated gas	Gas outlet of separator
		tra13	Transport the over-pressurized gas into environment	Relief valve
		tra21	Transport the compressed gas	Compressor
		tra22	Transport the compressed gas into heat exchanger tube	Tube-side fluid in
		tra23	Transport the exothermic gas	Tube-side fluid out

		tra24	Transport the exothermic gas to downstream	Pipeline
		tra25	Transport bypass gas backflow after bypass valve	Pipeline
		tra26	Transport cold water	Shell-side fluid in
		tra27	Transport the endothermic water	Shell-side fluid out
		tra35	Transport bypass gas backflow before bypass valve	Pipeline
		bal1	Balance the feed flow 1 and feed flow 2 with gathered feed flow	Valve group
		bal2	Balance the outflow of the separated crude oil with the inflow of the crude oil in pump	Valve
		bal3	Balance the outflow of the crude oil in pump with the inflow of the crude oil in pipeline	Valve
		bal5	Balance the outflow of the separated gas with the inflow of the compressed gas in compressor	Pipeline
		bal6	Balance the outlet gas flow from compressor with the inlet gas flow to heat exchanger	Pipeline
		bal7	Balance the exothermic gas flow with bypassing reflux gas stream and outlet compressed gas downstream	Pipeline
		bal9	Balance the	Anti-surge Valve
		sep1	Separate the gas and liquid	Separator
		sep2	Separate the crude oil and water	Separator
		sto1	store the separated gas	Gas chamber
		sto2	Store the separated water	Water chamber
		sto3	Store the separated crude oil	Oil chamber
		sto6	Store the exothermic gas	Heat exchanger tube
		sto7	Store the endothermic water	Heat exchanger shell
		bar1	Block the water flowing into crude oil	Weir plate
		bar2	Block the mixture of exothermic gas with endothermic water	Tube bundle with straight tubes
		sin1	Collect the outflow of the separated oil	Downstream

		sin2	Collect the outflow of the separated water	Downstream
		sin3	Receive the exothermic gas	Downstream
		sin4	Receive the released over-pressurized gas	Environment
		sin9	Collect the endothermic water	Downstream
ef1:the energy conversion of the pump	Producer-produce (pp1)the function of transport of the crude oil in pump	sou3	Electrical energy supply for the pump	Electrical source
		tra14	Transport the electrical energy	Electrical wire
		tra15	Transport the kinetic energy	Water power
		tra16	Transport the friction loss	Pump friction loss and leakage power
		sto4	Store the electrical energy	Pump
		sin5	Receive the kinetic energy	Pump shaft
		sin6	Receive the friction loss	Pump shaft friction
efs2:Energy flow structure of separator	obj7:maintain the motor rotation speed	sou4	Feed flow 1 energy	Feed flow 1
	thr1:threaten the set pressure of the relief valve	sou5	Feed flow 2 energy	Feed flow 2
		tra17	Transport the feed flow 1 energy	Feed flow1 and pipeline
		tra18	Transport the feed flow 2 energy	Feed flow 2 and pipeline
		tra19	Transport the gathering energy flow	Pipeline
		tra20	Transport the liquid energy flow	gas phase
		tra36	Transport the gas energy flow	Liquid phase
		bal4	Balance the feed flow 1 and 2 energy flow with gathering energy flow	Gathering valve group
		sto5	Store energy in the separator	Separator
		sin7	Keep the gas phase energy	Gas
		sin8	Keep the liquid phase energy	Liquid
efs3:heat exchange between water and compressed gas	obj4:maintain the temperature of the compressed gas	sou7	Energy of the cold water	Cold water
		sou8	Energy of the compressed gas	Compressed gas
		tra28	Transport the energy of cold water	Shell and cold water
		tra29	Transport the energy of the compressed gas	Tube and compressed gas
		tra30	Transport the exothermal gas energy	exothermal gas and heat transfer tube
		tra31	Transport the endothermic water	endothermic water

		bal8	Balance the heat exchange between water and compressed gas	heat exchanger
		sin10	Keep the exothermal energy	exothermal gas
		sin11	Keep the endothermic energy	endothermic water
efs4:the energy conversion of the compressor	Producer-produce (pp3)the function of compressed gas transport	sou9	Electrical energy supply for the compressor	Electrical motor
		tra32	Transport the shaft power	Motor shaft
		tra33	Transport the kinetic energy	impeller
		tra34	Transport the energy loss	leakage, impeller resistance, flow loss
		sto8	Store the electrical energy	Compressor
		sin12	Receive the kinetic energy	Compressed gas
		sin13	Receive the energy loss	Impeller

Elements explanation in MFM model in Figure 8				
Flow structure	**Objective**	**Function name**	**Function**	**Structure**
mfs1: representing gas-liquid equilibrium from mass flow perspective	obj1: maintain the right liquid level, i.e. the right amount of mass in storage Liq (sto2).	sou1	Gathered feed flow source	Gathered feed flow
		tra1	Transform the liquid phase into gas phase	Liquid and gas interface
		tra2	Transform the gas phase into liquid phase	Liquid and gas interface
		tra5	Transport the separated liquid	Liquid density is higher than the gas density
		tra6	Transport the liquid	Liquid density is higher than the gas density
		tra7	Transport the gas	Gas density is lower than the liquid density
		tra8	Transport the gathered feed flow	inlet pipe of separator
		tra12	Transport the separated gas	Gas density is lower than the liquid density
		bal3	Balance the gathered inflow with liquid phase flow and gas phase flow	Mass balance
		sto1	Store the gas phase	Gas phase
		sto2	Store the liquid phase	Liquid phase
		sin1	Collect the separated liquid	Oil and water chamber
		sin2	Collect the separated gas	Gas chamber
\ef1: representing gas-liquid equilibrium	obj2: maintain the right pressure (obj2), i.e. the right	sou3	Gathered feed flow energy source	Gathered feed flow
		tra9	Transport the energy of gas	Temperature and pressure of the gas

from energy flow perspective	amount of energy in storage (sto3)	tra10	Transport the energy of liquid	Temperature and pressure of the liquid
		tra11	Transport the gathered feed energy	inlet pipe of separator
		tra19	Transport the separated gas energy	Gas density is lower than the liquid density
		tra20	Transport the separated liquid energy	Liquid density is higher than the gas density
		bal4	Balance the gathered inflow energy with liquid phase energy and gas phase energy	Energy balance
		sto3	Store the gas phase energy	gas phase
		sto4	Store the liquid phase energy	liquid phase
		sin7	Collect the separated gas energy	Gas chamber
		sin8	Collect the separated liquid energy	water and oil chamber

Appendix B

The consequences analysis of the other failure scenarios in Table 5 (except failure scenario 2) is summarized below.

Failure Scenario					Process Parameters						
					T (K)	Lw [m]	Lo [m]	Lt [m]	P [MPa]	F [kg/s]	
Cause ID Number	Failure Mode	Parameter Value		Equipment	Failure value						Consequences
1	Heat exchanger 23HX0001_tube plugging	0	0.8	Pf_25HV0001	316.55				2.56	62.2	Heat exchanger tube outlet stream temperature increases
				Pf_25HV0002	315.95				2.56	54.2	
				Separator	315.15	0.05	0.15	0.156	2.4	116.4	
				Heat exchanger tube	323.15				5.02	42.8	
				Export oil	315.15				2.4	73.1	
				Export gas	314.85				2.4	42.8	
				Export water	315.15				2.4	4.4	
				Pump	316.75				5.32	73.1	
				Compressor	381.15				5.14	42.8	Antisurge valve open at 0.0558965
				Antisurge loop	305.95				2.41	3.9	
3	Outlet gas pipeline from the separator plugging fraction is 0.8	0	0.8	Pf_HV0001	316.55				2.56	61.1	
				Pf_HV0002	315.95				2.56	53.1	The pressure builds up the separator.
				Separator	317.15	0.05	0.15	0.156	3.00	114.17	
				Heat exchanger tube	318.15				5.00	42.78	
				Export oil	315.15				2.4	73.1	
				Export gas	315.15				2.4	42.78	
				Export water	315.15				2.4	4.44	
				Pump	316.85				5.32	73.06	
				Compressor	381.15				5.14	42.78	The working condition of the compressor is normal but is approaching a blocking state.
				Antisurge loop	305.95				3.28	3.89	
4	Compressor polytrophic efficiency deterioration is 0.8 fraction	0	0.8	Pf_25HV0001	316.55				2.56	53.06	Less inlet flow.
				Pf_25HV0002	315.95				2.56	45.83	
				Separator	320.15	0.05	0.15	0.156	4.10	98.61	The pressure and temperature increases sharply.
				Heat exchanger tube	318.15				5.00	42.78	
				Export oil	315.15				2.4	73.06	
				Export gas	315.15				2.4	42.78	
				Export water	315.15				2.4	4.44	
				Pump	316.85				5.32	73.06	
				Compressor	381.15				5.14	42.78	Antisurge compressor valve opens more.
				Antisurge loop	305.95				2.41	108.06	
5	Motor (23EM0002) machine failure	false	true	Pf_25HV0001	322.95				5.35	19.72	The inflow of mixed crude oil is prevented from flowing into the separator.
				Pf_25HV0002	322.95				5.35	17.2	The separator losses the separation opportunity due to no object (feed flow) needs to be separated. The pressure of the separator rises dramatically from 2.4MPa to 5.4 MPa within only 100s. Temperature of the separator has the same increasing trend from 315.15K to almost 323.15 K.
				SeparatorHeat	323.15	0	0.079	0	5.40	36.67	The water-oil interface level, oil level and the total level Oil and water level falls rapidly.
				exchanger tube	288.15				5.00	3.89	Heat exchanger tube outlet stream temperature decreases a lot. Less export gas.
				Export oil	322.75				5.35	0	The low oil level causes gas to exit via the oil output causing high pressure downstream. The outlet pressure of centrifugal pump (23PA0001) accordingly goes up.
				Export gas	372.35				5.35	3.89	Compressor surging. The gas recirculation surge control loop failed to handle with the compressor surging situation.
				Export water	372.35				5.34	0	
				Pump	372.35				8.26	0	
				Compressor	282.85				5.01	3.89	
				Antisurge loop	322.75				5.34	−32.5	