# An Integrated Qualitative and Quantitative Modeling Framework for Computer-Assisted HAZOP Studies

**Jing Wu**
Dept. of Safety Engineering, College of Mechanical and Transportation Engineering, China University of Petroleum-Beijing, Beijing 102249, China

State Key Laboratory of Heavy Oil Processing, China University of Petroleum-Beijing, Beijing 102249, China

**Laibin Zhang and Jinqiu Hu**
Dept. of Safety Engineering, College of Mechanical and Transportation Engineering, China University of Petroleum-Beijing, Beijing 102249, China

**Morten Lind and Xinxin Zhang**
Dept. of Electrical Engineering, Technical University of Denmark, 800 Lyngby, Denmark

**Sten Bay Jørgensen and Gürkan Sin**
CAPEC-PROCESS, Dept. of Chemical and Biochemical Engineering, Technical University of Denmark, 2800 Lyngby, Denmark

**Niels Jensen**
Safepark, Kannikestræde 14, 3550 Slangerup, Denmark

*DOI 10.1002/aic.14593*
*Published online August 27, 2014 in Wiley Online Library (wileyonlinelibrary.com)*

*The article proposes a novel practical framework for computer-assisted hazard and operability (HAZOP) that integrates qualitative reasoning about system function with quantitative dynamic simulation in order to facilitate detailed specific HAZOP analysis. The practical framework is demonstrated and validated on a case study concerning a three-phase separation process. The multilevel flow modeling (MFM) methodology is used to represent the plant goals and functions. First, means-end analysis is used to identify and formulate the intention of the process design in terms of components, functions, objectives, and goals on different abstraction levels. Based on this abstraction, qualitative functional models are constructed for the process. Next MFM-specified causal rules are extended with systems specific features to enable proper reasoning. Finally, systematic HAZOP analysis is performed to identify safety critical operations, its causes and consequences. The outcome is a qualitative hazard analysis of selected process deviations from normal operations and their consequences as input to a traditional HAZOP table. The list of unacceptable high risk deviations identified by the qualitative HAZOP analysis is used as input for rigorous analysis and evaluation by the quantitative analysis part of the framework. To this end, dynamic first-principles modeling is used to simulate the system behavior and thereby complement the results of the qualitative analysis part. The practical framework for computer-assisted HAZOP studies introduced in this article allows the HAZOP team to devote more attention to high consequence hazards.* © 2014 American Institute of Chemical Engineers *AIChE J*, 60: 4150–4173, 2014

*Keywords: hazard analysis, multilevel flow modeling, dynamic simulation, computer-assisted HAZOP, knowledge-base*

## Introduction

Hazard and operability (HAZOP) study is a well-accepted method for hazard identification of process designs and for planned modifications, which initially was developed for analyzing chemical process hazards.[1] The approach is a structured brainstorming using guidewords and is performed by a multidisciplinary team during a set of meetings to derive the records of causes and consequences of deviations.[2] An effective HAZOP ensures that all potential deviations from design intentions are identified and process hazards are revealed. Based on the brainstorming sessions, mitigating actions can be planned against unacceptable process consequences or actions for improvement of the system safety integrity level. It is important that records of the brainstorming sessions and documentation of planned actions are available for review by management and authorities.[3]

Conventional HAZOP study is time-and-cost consuming and suffers from lack of completeness.[4,5] By investigation,[6] for the installation of an oil and gas unit on an existing site,

Correspondence concerning this article should be addressed to J. Wu at wj87811 @126.com.

each P&ID (Piping & Instrumentation Diagram) might take 5 or 6 h depending on the scale of the project. For the installation of a major new unit on an existing refinery or of the topsides on an oil platform, 6–8 weeks may be required. Consequently, HAZOP studies may benefit significantly from development of computer-aided technology, for example, through the use of knowledge-based techniques, combining multiple models to improve the quality of the hazard analysis in terms of consistency, coverage, and so forth.

During the last three decades, many studies have focused on developing improved HAZOP methods. There are two promising research trends to develop effective hazard analysis: automating HAZOP using qualitative models and reasoning in expert systems and HAZOP supported by quantitative dynamic simulation. According to Dunjó et al.,[7] almost 40% of published literature in HAZOP improvement work concerns the development of expert systems intended to automate HAZOP. Some of these expert systems are model based. Vaidhyanathan and Venkatasubramanian[8] proposed HAZOP Digraph-based models for representing causal models of process systems, and developed an expert system, named HAZOPExpert, for performing HAZOP analysis. The expert system was implemented is in an object-oriented architecture using the expert system shell G2. Srinivasan and Venkatasubramanian[9] described the architecture of a prototype expert system based on the use of Petri net-digraph models. A Functional HAZOP assistant proposed by Rossing et al.[10] is based on multilevel flow modeling (MFM) representing functional knowledge providing a very efficient paradigm for facilitating HAZOP studies and for enabling reasoning about potential hazards in safety critical operations. Briefly, the purpose of the above mentioned different qualitative models is to represent systems and reproduce the reasoning in expert system during the HAZOP analysis searching for the causes and consequences of process variable deviations. The qualitative models play an important role in increasing the efficiency, coverage, consistency, and accuracy of HAZOP analysis. Conversely, for deviations with potentially high risk and hazardous consequences, researchers try to use quantitative dynamic simulation to validate the effects of deviations on plant. Dunjó et al.[7] found that only up to 5% of published literature in the research area of HAZOP has been supported by quantitative dynamic simulation. 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.

The aim of this article is to develop tools to assist with hazard identification in the proposed integrated qualitative and quantitative modeling framework, 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 remainder of this article is organized as follows. The Methods and Tools section introduces the qualitative and quantitative modeling approaches and the simulation software used in the study. Next, the proposed integrated qualitative reasoning and quantitative process simulation framework is explained in detail followed by the proposed integrated HAZOP procedure explained step by step. In the case study, the proposed qualitative and quantitative modeling framework is applied in computer-assisted HAZOP studies. Finally, a discussion of the result follows and conclusions are drawn.

## Methods and Tools

System modeling methodologies developed in process safety engineering (PSE) are primarily driven by two considerations. One is the interest in a quantitative representation of system behavior as a whole from the physical laws point of view while the other has an emphasis on investigating how the functions of the plant components, the structures, and their interactions contribute to fulfillment of the overall goals of the system.[11] We call these two system modeling methodologies the physical modeling approach and the functional modeling approach. The purpose of this section is to present the two approaches and the associated reasoning and simulation software we used in this study.

### *Quantitative modeling*

A mathematical model describes the plant involving physical, chemical, and/or biological processes and control couplings by the laws of physics, chemistry, biology, mechanical, and electrical engineering.[12] To achieve quantitative analysis, a set of mathematical equations are developed from knowledge of physical, chemical, and biological mechanisms (i.e., first-engineering principles modeling or mechanistic modeling) and used to simulate system behavior. However, obtaining the necessary information to formulate a 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

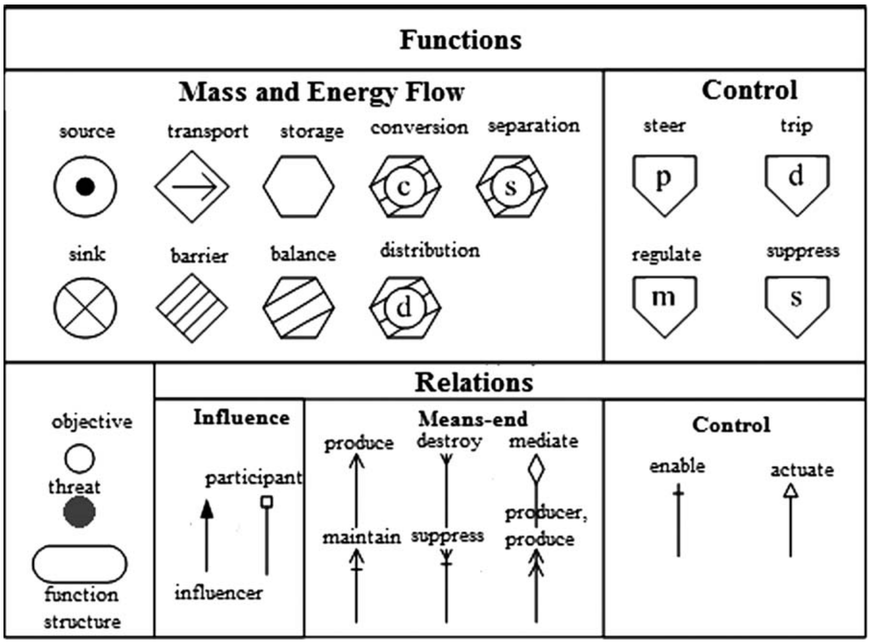



Figure 1. The basic MFM symbols.

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[13,14] 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 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. System models must represent system features and capture system knowledge about design intention.

### *Qualitative modeling*

The functional modeling of a system is one representative qualitative modeling framework, which aims at covering the problems described above. Functional modeling uses the concepts of goal and function to describe system functionality at multiple abstraction levels. This modeling concept has demonstrated its potential to resolve challenges in modeling operating modes, control modes, and failure mode analysis in the domains of nuclear power system,[15,16] oil/gas facilities,[17] and so forth. MFM is a widely used knowledge-based functional modeling methodology. MFM modeling applies means-end and parts-whole decomposition and aggregation techniques to handle the complexity of PSE systems.[18] A means-end relation links the target state of a process with means provided by the plant designer for reaching it. In MFM modeling, means-end relations link the objective 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 1) 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. We take the separator in the case study presented later as an example to illustrate these fundamental concepts. The function of transport of mixed feed of crude oil, water, and gas from upstream to the separator is realized by means of pipelines and valves that have the potential behavior to fulfill one of the objectives that is to maintain the separator feed flow condition to achieve the goal

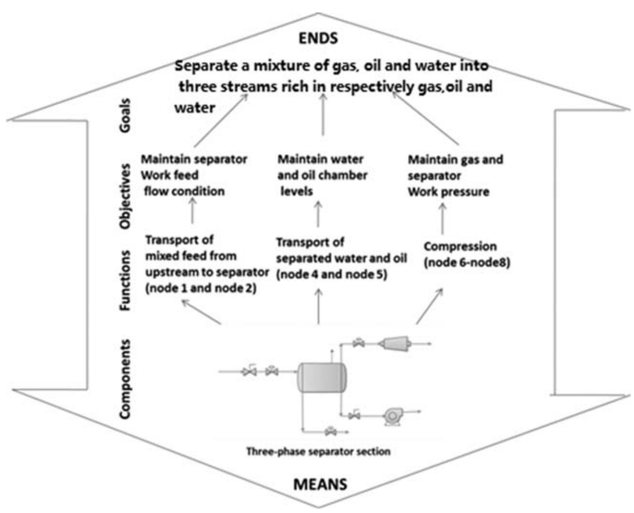



Figure 2. Means and ends of the three-phase separator subsystem.

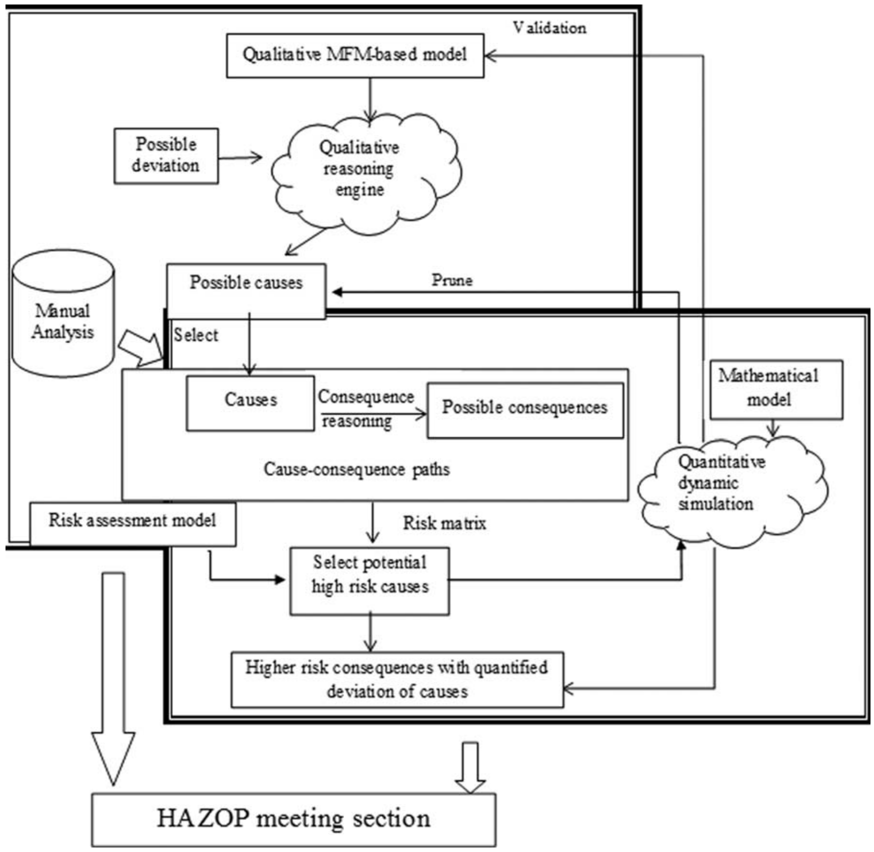



**Figure 3. The proposed integration of qualitative and quantitative process simulation frameworks: qualitative analysis highlighted in upper left box and quantitative analysis is highlighted in lower right box.**

(the end) to separate the mixture of gas, crude oil, and water as shown in Figure 2. The MFM modeling languages provide formalized concepts for the description of the systems and as such serve as a modeling languages which as pointed out by Stephanopoulos and Reklaitis[11] is an important research effort. The graphical symbols used in MFM as shown in Figure 1 support multilevel representation in terms of mass and energy flow structures and control structures.[19] Detailed definitions for each graphical symbol can be found in an introduction to MFM.[20] 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.[21,22]

In this study, a graphical editor based on the Java-based ShapeShifter framework supporting MFM modeling (called the MFM Editor) developed by the Institute for Energy Technology in Norway is used.[23,24] 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.

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 displayed nor communicated when quantitative models are developed and presented. Consequently, there is a direct connection from a qualitative (functional) model to a quantitative (mathematical) 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.

### *Integrated qualitative and quantitative process simulation framework*

This section describes the purpose of the integrated qualitative and quantitative process simulation framework. It is well known that, in general, no single method is sufficient for a wide range of problem-solving tasks.[25] For example, a quantitative dynamic simulation cannot simulate emergency situations.[26] A qualitative model-based approach for HAZOP is often needed for full understanding the complexity of real industrial systems. But the integration of qualitative and quantitative methods is quite rare. However, qualitative and quantitative methods for facilitating hazard analysis can supplement each other in several aspects.

- At early system design stage, there are still no detailed numerical data about the physical process phenomena, equipment specification, controllers, and so forth, which are necessary for quantitative process simulation. However, by providing general information about the process, such as mass and energy balances qualitative reasoning concerning cause and consequence of hazards can be carried out before a detailed design has been done.
- Qualitative methodologies for facilitating hazard analysis, such as MFM model-based methods, can explore both causes as well as consequences of deviations from design

Table 1. Risk Matrix Showing Likelihood (Frequency) on Horizontal Axis, and Consequences (Severity) on Vertical Axis

| | | | | Likelihood | | | | |
|---|---|---|---|---|---|---|---|---|
| | Scale | | | Improbable | Remote | Occasional | Probable | Frequent |
| | | Quant. | | <0.0001 | 0.001 | 0.01 | 0.1 | 1 |
| | | | Qual. | Rare | Unlikely | Probable | Likely | Certain |
| **Consequences** | Catastrop. | 50 M$ | Very high | | | | | |
| | Critical | 5 M$ | High | | | | | |
| | Moderate | 0.5 M$ | Medium | | | | | |
| | Minor | 0.05 M$ | Low | | | | | |
| | Negligible | <0.005 M$ | Very low | | | | | |

intention of the process components or equipment. A quantitative dynamic simulation can only be triggered by an initial abnormal event and track the corresponding consequences. There is no direct means in a quantitative dynamic simulation to search for the initial abnormal event, in other words, to find possible causes for a given consequence.

• Conversely, some inherent limitations for some hazard analysis purposes exist in qualitative hazard analysis methodologies. There is insufficient information to examine how the system reacts to deviations with respect to accurate response time for resetting affected variables back to the normal range. Also, even if the possible consequences can be inferred by the qualitative reasoning, a quantitative value on how far the system will move away from the critical situation cannot be answered. Obviously, quantitative dynamic simulation can handle such limitations. At the same time, the consequences obtained from quantitative dynamic simulation can be helpful with pruning and validation of the possible consequences deduced from qualitative reasoning engine.

Generally speaking, integration of the qualitative 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[27] 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 3. Based on the qualitative MFM model of the process system, one can perform qualitative simulations 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,[28] 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.

The benefits for the performance of HAZOP studies in the integrated framework are:

1. The qualitative MFM-based functional representation of the process is based on deep knowledge about system goals,

Table 2. Predefined Matches of Functions and Failure Modes to Generate Failure Scenarios in Quantitative Dynamic Simulator

| Parts/Components | Possible Functions | Function States | Possible Failure Modes | Quantitative Input Variables |
|---|---|---|---|---|
| Valve | Mass transport | {low, normal, high} | {Open failure, Close failure} | Stem position [0, default, 1] |
| | Mass balance | {leak, normal, fill} | {Leakage, Stick} | Leakage fraction [0, 1]<br>Stem position [0, default, 1] |
| Pipe | Mass transport Energy transport | {low, normal, high} | Plugging | Plugging fraction [0, 1] |
| Separator | Mass storage | {lowvol, normal, highvol} | {Open failure, Close failure} | Water-oil interface level 23LV0001 Stem position [0, default, 1]<br>Water level 23LV0002 Stem position [0, default, 1] |
| | Energy storage | | | Temperature/K [0, 315.15, 333.15]<br>Pressure /MPa [0, 2.4, 6] |
| Motor | Energy source | {lowvol, normal, highvol} | Machine failure | Voltage fraction [0, 1] |
| Compressor | Mass transport | {low, normal, high} | Reduction of polytrophic efficiency | Reduction fraction [0, 1] |
| Heat exchanger | Mass storage Energy storage | {lowvol, normal, highvol} | {Open failure, Close failure} | 23TV0003 stem position [0, default, 1] |
| | Mass balance Energy balance | {leak, normal, fill} | {fouling, plugging} | Fouling factor [0, 1]<br>Plugging [0, 1] |

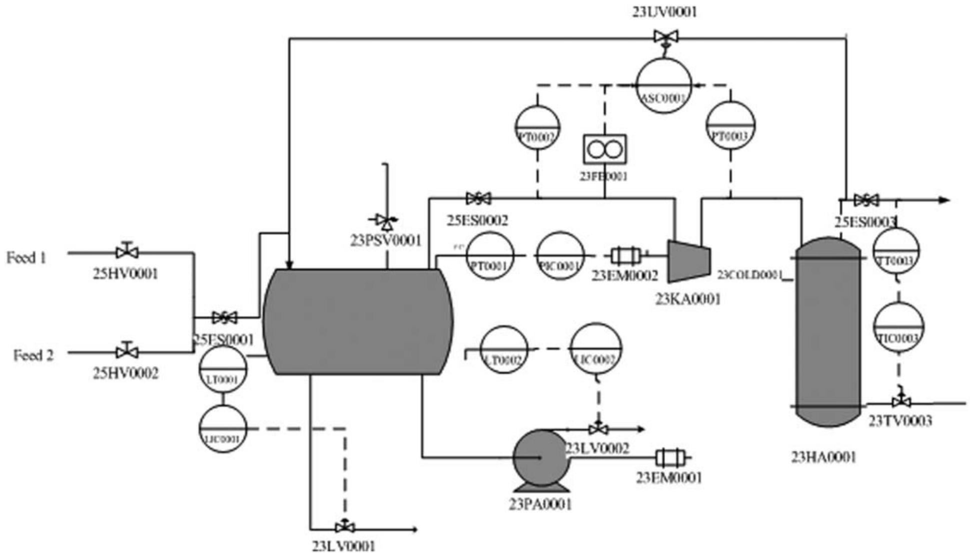



**Figure 4. Simplified P&ID of three-phase separation process.**

function, and structure rather than heuristic knowledge such as the deduction from expert evidence. The deep knowledge reasoning about HAZOP result is more consistent, universal, and suitable for engineering application, which could be beneficial for improving the quality of HAZOP;

2. The functional models capture much of the tacit knowledge, which normally is neither displayed nor communicated when quantitative models are developed and presented. For example, the precondition for proper working of a centrifugal pump is that it has to be filled with a suitable amount of fluid. The failure of such condition fulfillment is also one type of potential hazard. The qualitative functional model can represent and detect such potential hazards (i.e., by examining whether the enablement relation between flow structure and objective/function is fulfilled or not). Conversely, quantitative modeling is rooted in first principles and physical/chemical laws underpinning phenomena in engineering system (e.g., in off-shore oil and gas industries, that would include phenomena such as transport, reaction, separation, thermodynamics, input-output dynamics, and so forth, which will be explicitly mathematically described) where the connection to the goal of the system and the conditions required for their fulfillment are implicit. Hence the two modeling approaches enhance the breadth and scope of modeling the system. Therefore, integrating qualitative and quantitative methods can be potentially beneficial for revealing a larger set of possible scenarios.

3. The feedback from the quantitative model can be used to prune the possible cause paths and enhances the MFM model reasoning as indicated in Figure 3.

4. After searching for hazards based on the functional model, the more hazardous events of considerable interest are scrutinized by performing quantitative dynamic simulations of the corresponding abnormal scenarios to explore details such as response time and quantified degree of deviation in order to improve the analytic depth.

### *Integrated HAZOP methodology procedure*

In this section, the integrated HAZOP methodology procedure used by the presented framework are described and explained in detail.

The main steps of the integrated HAZOP methodology procedure include:

1. MFM model building. In this step, given system information such as process flow diagram and P&ID, a functional model of the physical system is developed by following the MFM model building procedure:

   a. Knowledge acquisition: collect supporting documents from design plant such as P&ID diagram and operational manual.
   Then analyze comprehensively the production system to fully understand the purpose (-s) of the system;

   b. Decompose the process system into subsystems and analyze their goals;

**Table 3. Function Nodes in Section 1**

| Node Number | Function | Structure |
|---|---|---|
| 1 | Fluid transport | Line from Feed 1 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 | Antisurge control loop |

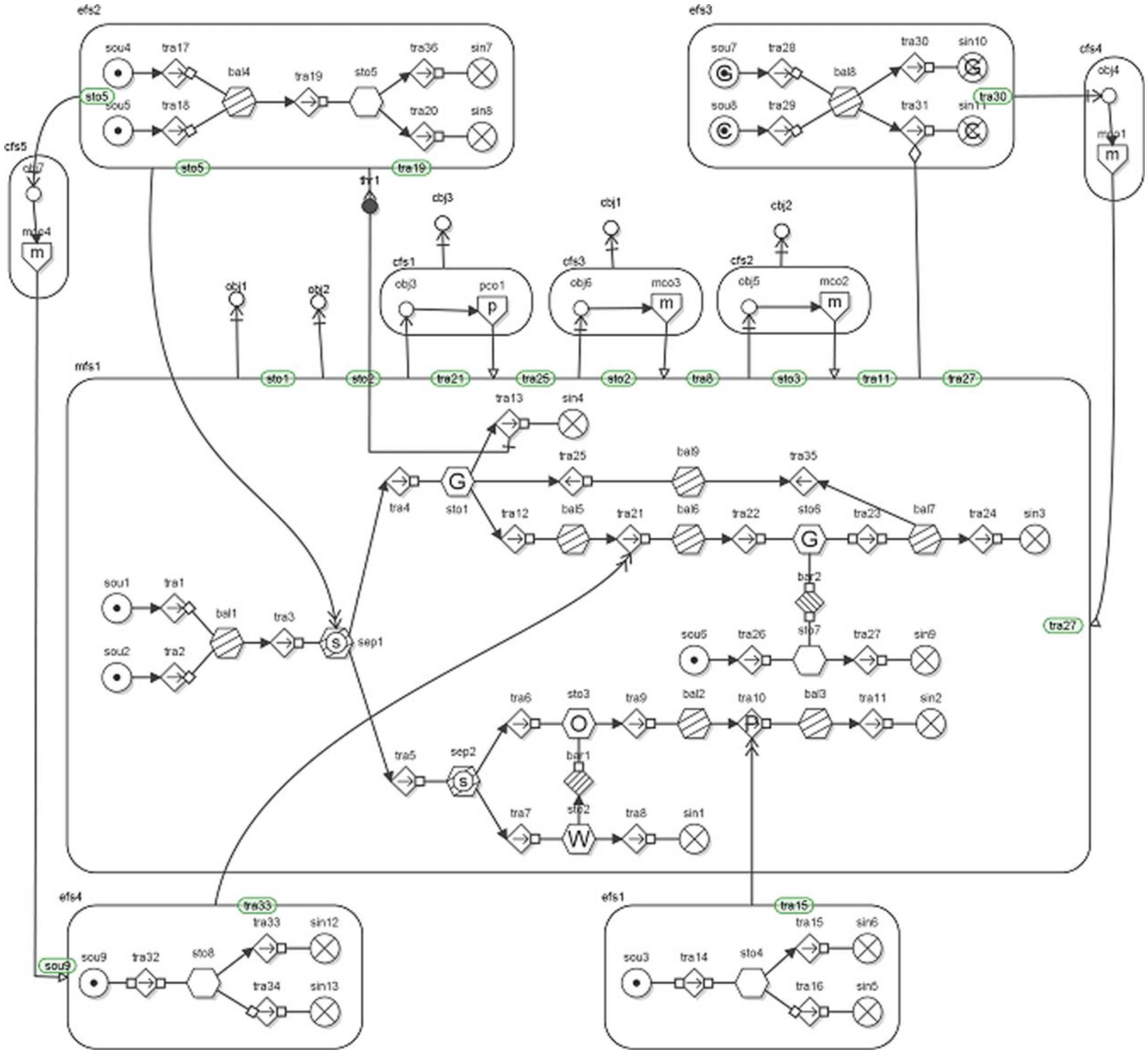



**Figure 5. MFM model of three-phase separation process (higher level abstraction).**

[Color figure can be viewed in the online issue, which is available at wileyonlinelibrary.com.]

c. Each subsystem is further decomposed into functional nodes;

d. Means-end analysis in terms of components, functions, objectives, and goals;

e. Build MFM model based on the means-end analysis;

f. Model verification and validation.

2. Qualitative HAZOP analysis for process. In this step, each column of the traditional HAZOP table is filled and the former P&ID diagram is modified by following the qualitative HAZOP analysis for process procedure:

2.1. Traditional HAZOP

Carry out a traditional HAZOP procedure to fill in the traditional HAZOP parts of the qualitative HAZOP worksheet[1]

2.2. MFM-based HAZOP

a. Set abnormal state of any function to trigger deviation of selected parameter so as to generate a failure scenario;

b. Run the cause analysis and consequence analysis to generate cause tree and consequence tree for the deviation;

c. Interpret each function state of cause tree and consequence tree and record it in the corresponding column of the HAZOP worksheet of MFM-based causes and MFM-based consequences;

d. Existing safeguards for each consequence are filled in and required mitigating action (-s) are proposed;

e. Modify the P&ID diagram.

3. Select potentially high risk hazard. In this step, the higher unacceptable risk hazard with cause–consequence paths is selected by following the select potentially high risk hazard procedure.

a. Evaluate the likelihood and severity of each cause–consequence path using a risk matrix. Two metrics: severity and frequency (or likelihood) is taken into account. Table 1 shows the risk matrix, showing likelihood (frequency) on horizontal axis, and consequences (severity) on vertical axis. Risk = severity × frequency and the low risk zone (generally acceptable risk) is marked by light gray color, medium risk zone is marked by white color, high risk zone is marked by dark gray color[26];

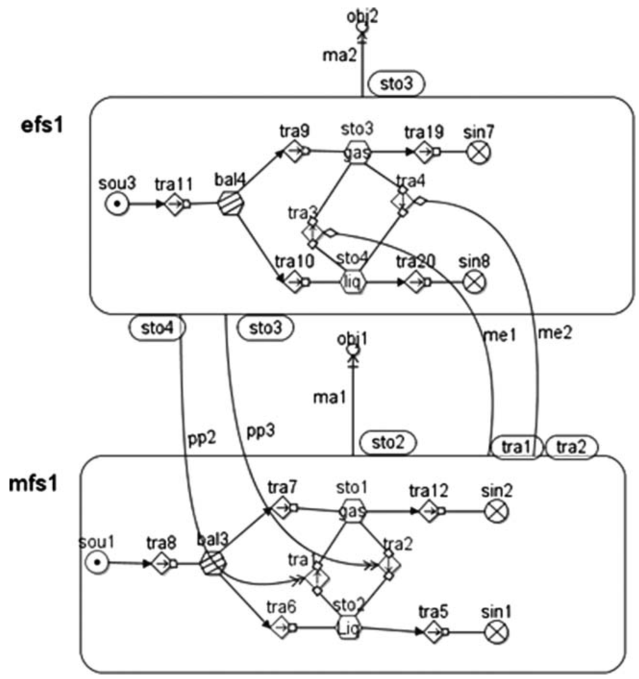



**Figure 6. MFM model of three-phase separator section (lower level abstraction of separation function).**

b. Select potentially high risk hazard marked by dark gray color as input for the quantitative dynamic simulation in quantifying the process hazard.

4. Validation of the qualitative analysis using quantitative dynamic simulation. In this step, the quantitative model could be simulated by commercial dynamic simulation software (HYSYS, K-Spice®, and so forth), and the highly unacceptable failure scenarios identified by qualitative analysis are simulated in the quantitative dynamic simulator. In this task, the following workflow is typically involved:

a. Configure the process in quantitative dynamic simulation software;

b. Implement the highly unacceptable qualitative scenarios with quantitative dynamic simulation; the possible failure scenarios can be generated from qualitative analysis matching the quantitative parameters in the quantitative dynamic simulator according to the Table 2.

c. Analyze the quantitative simulation output.

5. Further detailed analysis for highly unacceptable consequences is done for further mitigating suggestions.

## Case Study: Three-Phase Separation Process

In this section, 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. The process schematic is shown in Figure 4 and is explained as part of the MFM model building section below. 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.

### *Development of the MFM model*

To build a MFM model of the separation process, according to the procedure proposed above, the first step is knowledge acquisitions of the process followed by a comprehensive analysis of the production system and fully understand the purpose of the system. The purpose of the separation system is to separate two feed flows with mixtures of crude oil, water, and gas stream. Both feed flows have a nominal flow rate of 1 kg/s, pressure of $5.6 \times 10^6$ Pa and temperature of 323.15 K. The components of the feed flows are water, lower hydrocarbons, methanol, carbon dioxide, nitrogen, isobutene, isopentane, MEG, and four pseudo components representing higher hydrocarbons.

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 antisurge controller loop (23UV0001) is installed to protect the compressor from entering a surge condition. More details about the process can be found elsewhere.[29]

Initially starting with Step 1 a for knowledge acquisition, the supporting document of the designed process such as P&ID diagram and quantitative simulating models are obtained to support understanding of the process.

According to Step 1 b in MFM model building, based on the design intentions of the system, we divide the process system into two subsystems:

• 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.

To illustrate the Step 1 c, we take Section 1, for example, which is further divided into the functional nodes listed in Table 3.

In the Case Study section of the article, the relevant process parameters and deviations will be applied to identify hazards in each functional node. For example, for the Node 3 "function of separator" will be: Level: {higher, lower}

Flow: {more, less, reverse, no}

Temperature: {more, less}

Pressure: {more, less}

**Table 4. Control Objectives**

| Number | Measurements | Actuator |
|---|---|---|
| Cbj1 | Oil level in the separator | Dump oil 23LV0002 to next unit |
| Cbj2 | Water level in the separator | Dump water 23LV0001 |
| Cbj3 | 23PT0002, 23PT0003 and the value of flow element 23FE0001 | Antisurge valve 23UV0001 |
| Cbj4 | Temperature of output gas flow | Pipe valve 23TV0003 output gas flow |
| Cbj5 | Pressure of the separator | Motor EM0002 speed |

Table 5. 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<br>2. Compressor possibly surge<br>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<br>4. A low oil level causes gas to exit via the oil output causing high pressure down-stream (pressure builds up on pump)<br>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<br>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<br>2. Compressor can possibly surge<br>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<br>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<br>2. Add high pressure alarm<br>3. Install a manual bypass valve V-2<br>4. Line design pressure higher than pump deadhead pressure<br>5. Install kickback line to pump<br>6. Install relief valve 23PSV0002 for pump<br>7. Install stand-by pumping system |
| | | | Polytropic efficiency of compressor is degrading | 4 | 1. Pressure builds up on separator 23VA0001<br>2. Compressor surge<br>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<br>2. Compressor possibly surge<br>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<br>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<br>2. Ensure regular motor maintenance |

It should be noted that when we simulate failure scenarios in the MFM reasoning engine, the "no" guideword is not covered by the presently existing version. However, the manual HAZOP includes the "no" guideword to complete HAZOP results and required actions.

To achieve the goals of the process system, following the Step 1 d, we need to associate the objectives with the goals to be satisfied. What is more, every objective is achieved by functions which are realized by related system components. The principle of an MFM model represents system relations by such means-ends analysis. To illustrate the means-ends structure, we take Section 1 as an example as shown in Figure 2 and discussed earlier in the Methods and Tools section.

In the Step 1 e, the MFM model is built using the MFM editor as shown in Figures 5 and 6. The explanations of elements in (flow structures, objectives, relations, and functions) in Figures 5 and 6 are presented in Appendix A.

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 5 is a higher level abstraction of the three-phase separation process. Figure 6 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. In Figure 5, the mass flow structure (mfs1) of the three-phase separator represents the mixture of gas, crude oil, and water flowing from the wells to the three-phase separator followed by the heat exchange of gas for model completeness. The first separator function (sep1) represents the separation of the gas phase and the liquid phase via means-end relation (pp2: producer-product) driven by the energy storage (sto5) in separator in the higher level abstraction. In lower level abstraction, this separation is coupled to the energy structure (efs1) in Figure 6 via means-end relation, which drives the mixed flow in mass structure (mfs1) in Figure 6 flowing from the liquid (sto2 Liq) to the gas (sto1 Gas) phase within the three-phase separator following the evaporation (tra1) and, inversely, the liquefaction (tra2) processes. Afterward, the liquid phase of mixed flow of crude oil and water will be separated (sep2) due to the density difference of water and crude oil stored in the water storage (sto2) and oil storage (sto3). The weir plate between the water room and oil room in the tank is represented as a barrier (bar1). A barrier in MFM is a special flow functions, which often is used to express a safety purpose in a system. Here it is used to represent subfunctions of the separation function. The separated oil will be pumped out (tra10) supported by the energy structure of the pump (efs1) via outlet pipeline (tra11) to the downstream facilities. The objective of the three-phase separator from the mass flow perspective is to separate the mixture of gas, crude oil, and water, explicitly obj1 (two-phase gas/liquid separation) and obj2 (crude oil/water separation). There is also a threat (i.e., an undesired situation or a hazard) represented in MFM by a black circle (thr1 related to an operation condition /temperature and pressure represented by the energy storage function sto5), the pressure relief safety valve (23PSV0001) represented by the transport function (tra19) destroying the threat is represented by the means-end relation (de1), and enables (en1) the mass flow and transport function (tra13) to flow away from the over pressurized separator. In detail, representing the gas-liquid equilibrium phenomena in Figure 6, the objective of the separator from the energy perspective is to maintain the right pressure (obj2), that is, the right amount of energy in storage (sto3) and the objective of the two phase (gas/liquid) separation process is from the mass flow perspective to maintain the right liquid level, that is, the right amount of mass in storage Liq (sto2). The separated gas will be transported out and pressurized by compressor (tra21) via means-end relation (pp3: producer-produce) driven by the energy flow structure of the compressor (efs4) to the heat exchanger. By regulating the outlet cooler flow (tra27) to mediate (me1: mediate relation) the energy taken away (tra31) and to maintain the temperature of the discharge gas of the heat exchanger tube (obj4).

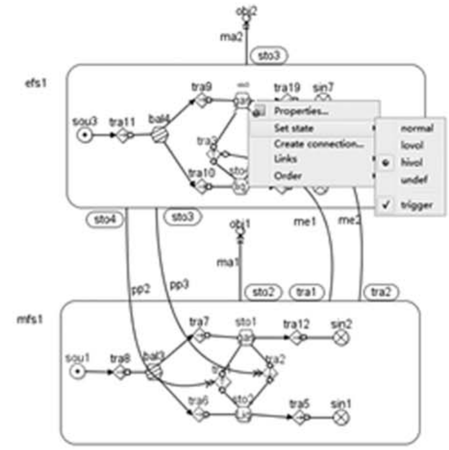
It should also be noted that some control objectives are related to control flow structures. In Figure 5, there are five control flow structures. The related control objectives and actuators are explained in Table 4. Specifically, in the antisurge control loop including a comparison between the set point of 23ASC0001 set by measurement of 23PT0002, 23PT0003 and the value of flow element 23FE0001 to actuate the antisurge valve 23UV0001 (tra25). It can be seen that in a functional model, such antisurge loop can be represented and included in the qualitative reasoning.

Step 1 f for 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[22]; (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. Then a validation procedure for an MFM model should be followed to accomplish the validation task. This article is not dealing with the MFM model validation issue in detail. If readers are interested this subject, please refer to Wu et al.[30]

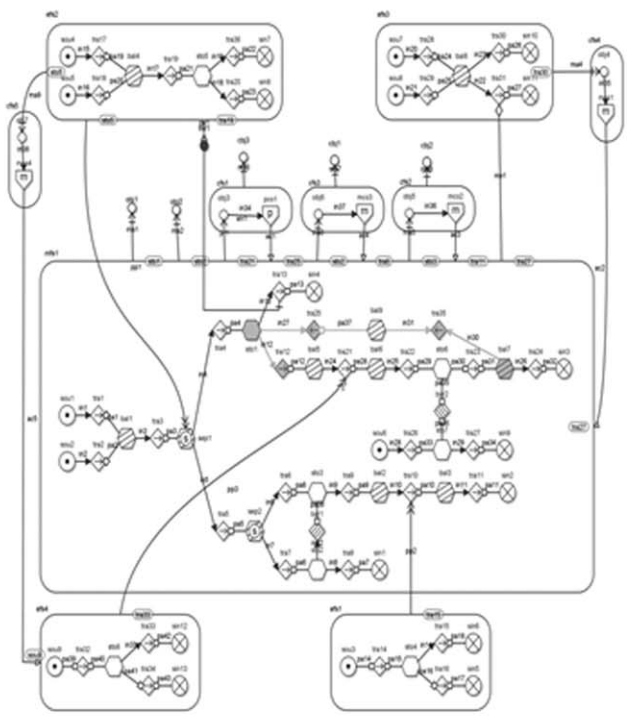
### *Qualitative HAZOP analysis*

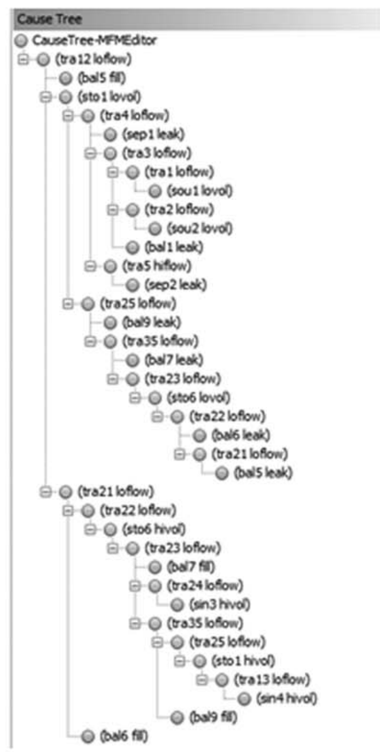
To demonstrate the feasibility of the methodology for qualitative hazard analysis, we applied related deviations for the nodes of Section 1. According to the Step 2.1, we carried out a traditional HAZOP procedure to fill in the traditional HAZOP parts of the qualitative HAZOP worksheet. The result of 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 5. It should be noted that the consequences occur in Table 5 are in condition of the safety valve 23PSV0001 failure to open.

In Table 5, 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




(a) Simulation of a deviation in MFM editor for higher separator pressure in reasoning engine






(b) One wrong cause path (bal7 leak , filled and marked by grey) visualized in MFM Editor

(c) Cause tree of higher pressure of separator (underlined causes are possible root causes)

**Figure 7. Qualitative simulation results with MFM editor for simulating the causes and consequences for higher separator pressure: (a) MFM editor interface for setting the deviation, (b) One wrong cause path (bal7 leak , filled and marked by gray), and (c) cause tree generated by the reasoning engine.**

consequences for the deviation in third column, respectively. The explanations of numbers in MFM-based causes and consequences refer to Tables 8 and 9. The gas out pipeline of the separator blocked as a cause for a deviation of higher pressure in Table 5 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

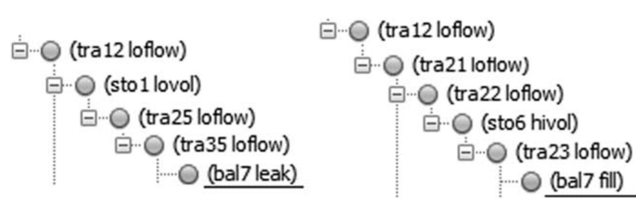



**Figure 8. Two conflicting results displayed in cause tree: the left possible root cause, bal7 leak, is wrong whereas the right possible root cause, bal7 fill, is right.**

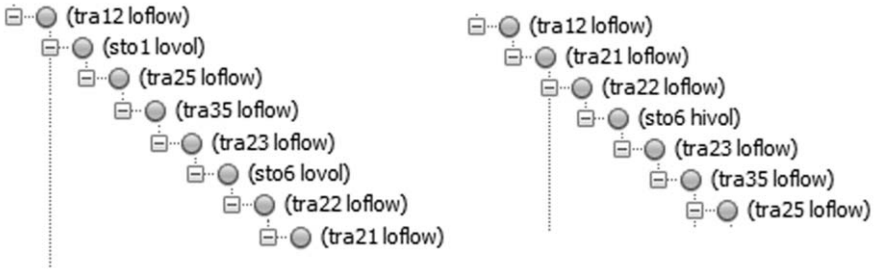



**Figure 9. Example of two causes (low flow rate in tra25 and tra22) leading to low value in tra12 which requires quantitative simulation to determine which cause has the major influence on tra12.**

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 5 can also be compared in this way.

Here we describe how we obtain the result of functional HAZOP, which includes pruning the possible causes and validation with the aid of quantitative simulation. We simulated one deviation, higher pressure of the separator in node 3 in Table 3. To do this, we set the state of function sto3 in Figure 7a to hivol (high volume). The transportation function tra12 is the same function in both abstraction level of the MFM models (Figures 5 and 6), therefore, it is a key function to propagate the effect of high volume state of function sto3 from lower abstraction level to higher abstraction level of models. Continuously, by using postdiction (i.e., searching backward toward causes in the same or lower structure) based on the reasoning rules in the MFM reasoning engine, it is feasible to find all possible cause paths (a complete cause tree) are shown in Figure 7c.

One of the observations that can be made from the reasoning result is that some of the reasoning paths are invalid due to the nature of the process. For example, two conflict results can be seen from the cause tree that is generated by the reasoning engine. One states that a balance bal7 leak can be a root cause of low flow in tra12, while the other states that bal7 fill can be a possible root cause shown in Figure 8.

A further observation can be made that low flow rate in tra25 and tra22 along the two paths can cause the low value in tra12 shown in Figure 9, and they can also be the cause for each other. This indicates that a dynamic situation and the influence forces must be considered quantitatively to evaluate which one of the functions has a major influence on tra12. This can be easily determined by the quantitative simulation model. The major and minor cause paths determined by the simulation are shown below in Figure 10. The bal7 leak is deleted from root cause list, because in this cause path on left side of Figure 8, sto1lovol is in conflict with the higher pressure of the separator. The simulation process will be explained further in the section on validation of the qualitative analysis. The complete cause tree generated from the reasoning engine is shown in Figure 7c and all valid cause paths are summarized in Table 6.

By prediction (searching forward in the same or higher structure) to find consequences, we take root cause sou9lovol as an example, there are seven consequence paths for this root cause as follows as shown in Table 7.

According to Step 2.2 c, each root cause is interpreted from the structural failure aspects as summarized in Table 8. By consequence analysis for each root cause, all possible

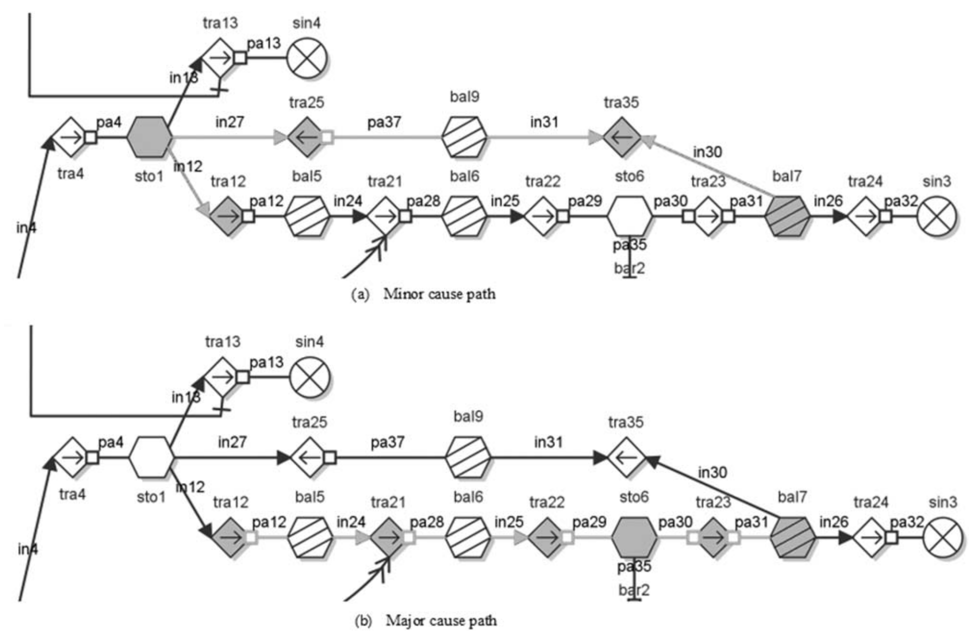



**Figure 10. Minor and major cause paths determined by quantitative simulation displayed by MFM reasoning engine.**

Table 6. Cause Paths for Higher Pressure Deviation in Node 3 "Function of Separator"

| ID Number | Cause Paths |
|---|---|
| 1 | sto3hivol → tra9hiflow → tra10loflow → sto4hivol → tra3loflow → tra10loflow → sto1hivol → tra12loflow → tra21loflow → tra22loflow → sto6hivol → tra23loflow → bal7fill |
| 2 | sto3hivol → tra9hiflow → tra10loflow → sto4hivol → tra3loflow → tra10loflow → sto1hivol → tra12loflow → tra21loflow → tra22loflow → sto6hivol → tra23loflow → tra35loflow → bal9fill |
| 3 | sto3hivol → tra9hiflow → tra10loflow → sto4hivol → tra3loflow → tra10loflow → sto1hivol → tra12loflow → bal5fill |
| 4 | sto3hivol → tra9hiflow → tra10loflow → sto4hivol → tra3loflow → tra10loflow → sto1hivol → tra12loflow → tra12loflow → tra21loflow → tra33loflow → sin12hivol |
| 5 | sto3hivol → tra9hiflow → tra10loflow → sto4hivol → tra3loflow → tra10loflow → sto1hivol → tra12loflow → tra21loflow → tra33loflow → sto8lovol → tra32loflow → sou9lovol |

Table 7. Consequence Paths for Root Cause (sou9lovol) in Node 3 "Function of Separator"

| ID Number | Consequence Paths |
|---|---|
| 1 | sou9lovol → tra32loflow → sto8lovol → tra34loflow → sin13lovol |
| 2 | sou9lovol → tra32loflow → sto8lovol → tra33loflow → sin12lovol |
| 3 | sou9lovol → tra32loflow → sto8lovol → tra33loflow → tra21loflow → sto1hivol |
| 4 | sou9lovol → tra32loflow → sto8lovol → tra33loflow → tra21loflow → sto1hivol → tra4loflow → tra3loflow → tra1oflow → sou1hivol |
| 5 | sou9lovol → tra32loflow → sto8lovol → tra33loflow → tra21loflow → sto1hivol → tra4loflow → tra3loflow → tra2loflow → sou2hivol |
| 6 | sou9lovol → tra32loflow → sto8lovol → tra33loflow → tra21loflow → tra12loflow → obj3 false |
| 7 | sou9lovol → tra32loflow → sto8lovol → tra33loflow → tra21loflow → tra22loflow → sto6lovol → tra23loflow → tra24loflow → sin3lovol |

consequences are found and filled into Table 5. The possible consequences are explained in Table 9.

According to Steps 2.2 d and 2.2 e, we fill 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 11. From a means-end relation perspective, Figure 11 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 8 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

Table 8. Interpretation of Each Root Cause

| ID number | Root causes | Interpretations |
|---|---|---|
| 1 | Bal7fill | Pipeline joint is blocked |
| 2 | Bal9fill | Antisurge 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 9. 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 |

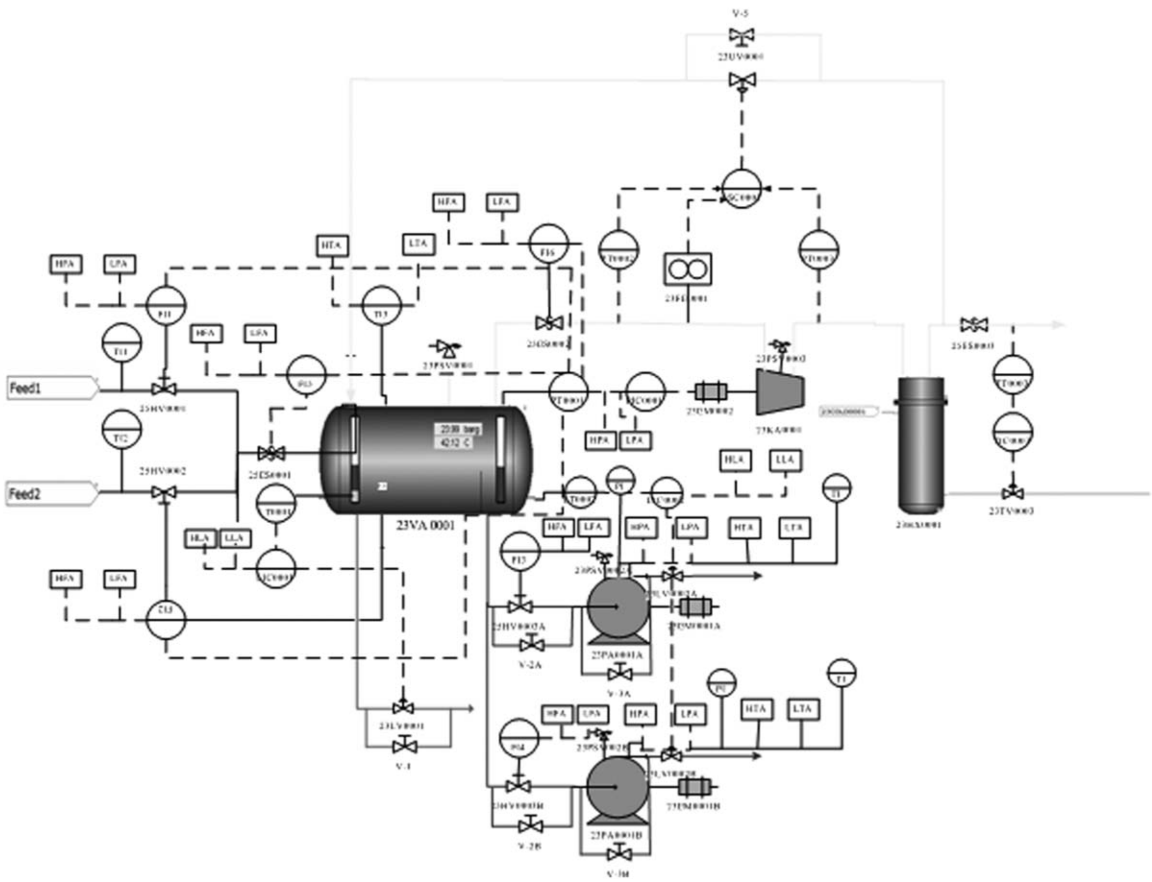



**Figure 11. Modified P&ID diagram for Section 1.**

strategy is improvement of system independence level. This strategy used in Figure 11 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 11. Alternatively the gas or turbine driven pump could be provided in addition to the electric motor driven pump as shown in Figure 11.

**Table 10. Measured and Monitored Variables List (Refers to Figure 3)**

| ID Number | Measured Variables | Units |
|---|---|---|
| 1 | 23VA0001:Temperature | K |
| 2 | 23VA0001:Pressure | Pa |
| 3 | 23KA0001:mass flow | kg/s |
| 4 | pf_23LV0001:mass flow | kg/s |
| 5 | pf_25ES0002:mass flow | kg/s |
| 6 | pf_25HV0001:mass flow | kg/s |
| 7 | pf_25HV0002:mass flow | kg/s |
| 8 | pf_25MV0003:mass flow | kg/s |
| 9 | 23VA0001:level overflow liquid | m |
| 10 | 23VA0001:level feed side weir | m |
| 11 | 23VA0001:level heavy phase feed side weir | m |
| 12 | 23KA0001:inlet pressure | Pa |
| 13 | 23KA0001:outlet pressure | Pa |
| 14 | 23KA0001:polytropic head | m |
| 15 | 23PA0001:inlet pressure | Pa |
| 16 | 23PA0001:outlet pressure | Pa |
| 17 | 23PA0001:volume flow | $m^3/s$ |

### *Using the risk matrix for qualitative risk assessment*

Following Step 3 of the methodology, the likelihood and severity of each cause–consequence path is evaluated using the risk matrix as shown in Figure 12. 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 gray color. The total number of high potential risk paths is 20. Among them, the consequences of higher pressure in separator, compressor working condition toward 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.

### *Development of quantitative model*

For the case study presented here, the quantitative model of the three-phase separation process is based on the three conservation equations of momentum, energy, and mass together with the Soave–Redlich–Kwong equilibrium state equation as the thermodynamic model, as described in Cameron et al.[14] The implementation of the three-phase separation system in the commercial dynamic simulation software K-Spice® was performed in the following five stages:

Table 11. **Normal Operating Conditions for the Three-Phase Separation Process**

| ID Number | Flow/Equipment | | Parameter | Normal value |
|---|---|---|---|---|
| 1 | Feed flow | | Flow rate | 1 kg/s |
| | | | Temperature | 323.15 K |
| | | | Pressure | $5.6 \times 10^6$ Pa |
| 2 | Three-phase separator | | Temperature | 315.15 K |
| | | | Pressure | $2.4 \times 10^6$ Pa |
| | | | Total level | 0.156 m |
| | | | Oil-water interface level | 0.05 m |
| | | | Oil level | 0.15 m |
| 3 | Compressor | | Suction pressure | $2.38 \times 10^6$ Pa |
| | | | Discharge pressure | $5.03 \times 10^6$ Pa |
| | | | Mass flow rate | 0.41 kg/s |
| | | | Compressor rotation speed | 139 Hz |
| | | | Suction temperature | 315.05 K |
| | | | Discharge temperature | 380.15 K |
| | | | Polytropic efficiency | 73.4 % |
| 4 | Motor for Compressor 23EM0002 | | Control signal | 0.90 fract |
| | | | The speed of the machine's own rotor | 139 Hz |
| | | | Machine power | $5.95 \times 10^6$ W |
| | | | Machine torque | $6.80 \times 10^3$ Nm |
| | | | Norminal Torque | $3.5 \times 10^4$ Nm |
| | | | Nominal synchronous speed | 157 Hz |
| 5 | Pump 23PA0001 | | Pump speed | 49 Hz |
| | | | Inlet suction pressure | $2.41 \times 10^6$ Pa |
| | | | Outlet pressure | $5.32 \times 10^6$ Pa |
| | | | Pump suction temperature | 315.25 K |
| | | | Pump discharge temperature | 316.95 K |
| | | | Pump volumetric flow rate | 0.11 $m^3/s$ |
| | | | Consumed pump power | $0.48 \times 10^6$ W |
| 6 | Motor for pump 23EM0001 | | Control signal | 1 fract |
| | | | The speed of the machine's own rotor | 49 Hz |
| | | | Machine power | $0.49 \times 10^6$ W |
| | | | Machine torque | $1.59 \times 10^3$ Nm |
| | | | Nominal torque | $2.00 \times 10^3$ Nm |
| | | | Nominal synchronous speed | 50 Hz |
| 7 | Heat exchanger | Tube | Inlet temperature | 379.15 K |
| | | | Outlet temperature | 318.15 K |
| | | | Flow rate | 40.6 kg/s |
| | | Shell | Inlet temperature | 288.15 K |
| | | | Outlet temperature | 350.15 K |
| | | | Flow rate | 21.7 kg/s |

(1) feed source stage-define the feed; (2) flow pressure stage-setup the piping/fitting network; (3) separation stage-build the separator; (4) heat exchanger stage-build the heat exchanger; (5) compressor antisurge stage-implement the antisurge control. The model parameters are presented in Cameron et al.[14]

### *Validation of the qualitative analysis*

Step 4 of the integrated methodology is applied in this section, to demonstrate the validation methodology for the qualitative analysis. Configuration of the process (Step 4 a) is done using the quantitative dynamic simulation software K-spice®. To implement Step 4 b, the measured variables list is shown in Table 10. The normal operation condition of the three-phase separation process is obtained and shown in Table 11. The linking of the qualitative analysis outputs in Table 9 as input for quantitative dynamic simulation is shown in Table 12, where each root cause is represented by a corresponding failure scenario. The detailed quantitative analysis is represented in Table 13 for one of the failure scenarios in Table 12, namely the failure of the control function of the antisurge valve (UV0001). The consequences of the other root causes are summarized in Appendix B. The normal valve fractional position in the antisurge pipeline is 0.5.

Table 12. **Generation 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 | Antisurge 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 13. Consequences of Antisurge Valve Stuck at 0.9 Fractional Position Failure Scenario**

| Failure Scenario | | | | Process Parameters | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Cause ID Number | Failure Mode | Parameter Value | Equipment | T (K) | Lw (m) | Lo (m) | Lt (m) | P ($10^6$ Pa) | F (kg/s) | Consequences |
| | | | | Failure value | | | | | | |
| 2 | Antisurge valve stuck at 0.9 fractional position | 0 0.9 | Pf_25HV0001 | 318.15 | | | | 2.98 | 61.11 | The pressure of the separator rises up from 2.4 to 2.84 MPa within 180 s. 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 |
| | | | Pf_25HV0002 | 317.55 | | | | 2.98 | 53.33 | |
| | | | Separator | 317.25 | 0.05 | 0.15 | 0.156 | 2.84 | 114.72 | |
| | | | Heat exchanger tube | 318.15 | | | | 5.00 | 84.17 | |
| | | | Export oil | 315.35 | | | | 2.85 | 73.89 | |
| | | | Export gas | 313.95 | | | | 2.84 | 84.44 | |
| | | | Export water | 316.15 | | | | 2.85 | 73.89 | |
| | | | Pump | 317.15 | | | | 5.73 | 73.89 | |
| | | | Compressor | 369.25 | | | | 5.04 | 84.44 | |
| | | | Antisurge loop | 308.85 | | | | 2.85 | 47.77 | |

In this failure mode, the valve position was assumed to be stuck at 0.9 fractional position. This means that the normal antisurge loop mass flow (pf_25ES0006) is 1.94 kg/s, while when the antisurge valve get stuck at 0.9 fractional position the mass flow increases to 47.22 kg/s.

The failure scenario of 0.9 fraction leakage of the antisurge valve (cause 2) is introduced after the simulator has been running in normal state runs for 900 s. The failure scenario trend time is 2700 s, and the simulation results are recorded for every 8 s. The simulation results are shown in Figures 13–15. The pressure of three-phase separator rises from 2.4 to 2.84 MPa within 3 min. 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 316.65 K and comes down to another stable state at approximately 315.55 K, which has little impact on the separator (Figure 13). 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 40.55 to 84.44 kg/s (Figure 14). Accordingly, the inlet volume flow rate for the compressor increases from 1.98 to 3.6 $m^3/s$, and the head-flow rate performance curve of the compressor in Figure 15 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 12 summarized in Appendix B, validate the cause–consequence paths in highly risk area in the risk matrix in Figure 12. 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 shutdown 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.

### *Real-time simulation of transient behavior and quantification of deviation scenarios*

In this section, quantitative analysis is carried out for serious failure scenarios. The purpose of the analysis 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 are also introduced. The trend/lasting time for each

| | Scale | Quant. | Qual. | Likelihood: Improbable | Remote | Occasional | Probable | Frequent |
|---|---|---|---|---|---|---|---|---|
| | | Quant. | | <0.0001 | 0.001 | 0.01 | 0.1 | 1 |
| | | | Qual. | Rare | Unlikely | Probable | Likely | Certain |
| Consequences | Catastrop. | 50 M$ | Very high | | | | | |
| | Critical | 5 M$ | High | | | | (1,6) | (1,3),(1,4),(1,5),(1,7),(2,7),(2,8),(3,3),(3,4),(3,5),(3,7) |
| | Moderate | 0.5 M$ | Medium | | | | (4,6),(4,9),(5,6) | (4,3),(4,4),(4,5),(4,7),(5,2),(5,3),(5,4),(5,5),(5,7) |
| | Minor | 0.05 M$ | Low | | | | | |
| | Negligible | <0.005M$ | Very low | (5,1) | | | | |

**Figure 12. Risk matrix for higher pressure deviation of separator.**

plugging change is shown in Table 14. The results are sampled every 48 s. It is assumed that the other equipment state is normal at the beginning of the simulation.

We monitor the same variables as listed in Table 10 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 Figures 16–19. Along with the successive changes of separator outlet gas pipeline plugging fraction with time in Figure 16, 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 17. At a pipeline plugging fraction of 0.9, the separator pressure dramatically rises to 4.8 MPa. 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 18. 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 19. By investigating the other parameters, it can be seen in Figure 18, that the water level is almost 0. In other words, since the pressure rises

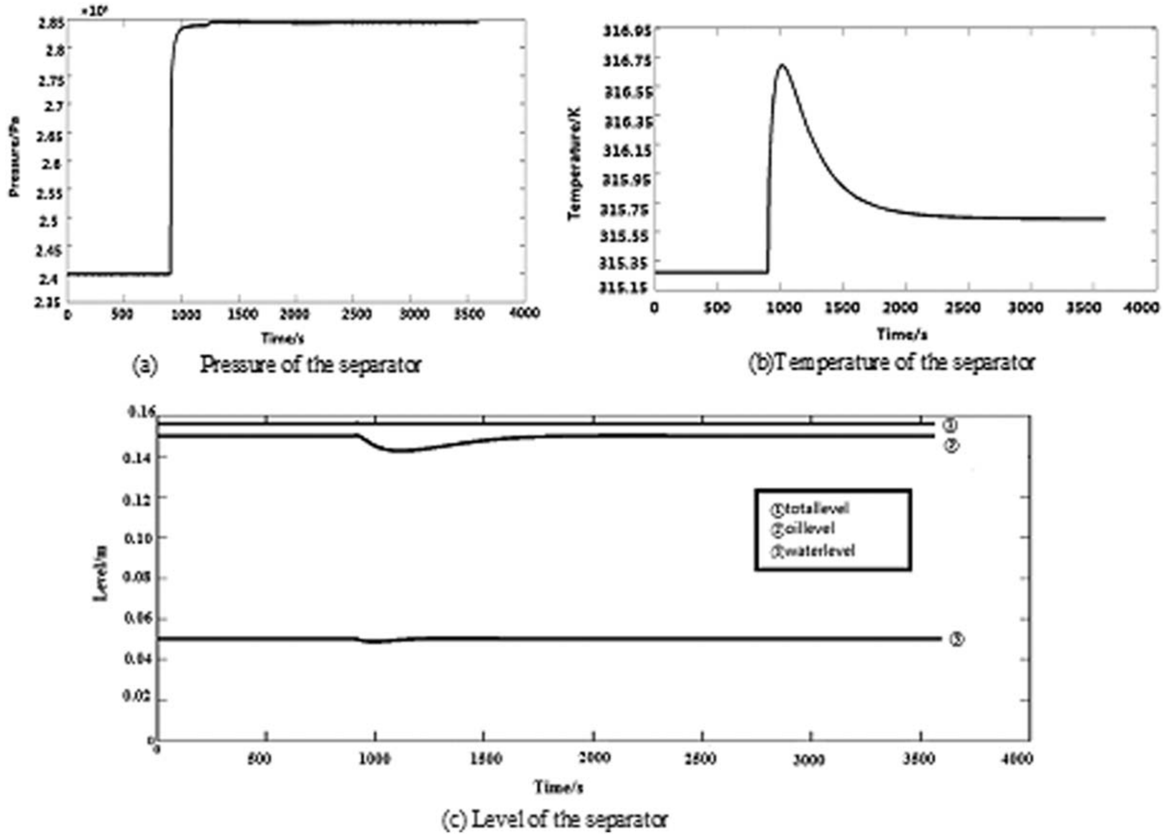



**Figure 13. Changes in operating condition of the three-phase separator when antisurge valve is stuck. (a) Pressure changes, (b) Temperature changes, and (c) Level changes.**

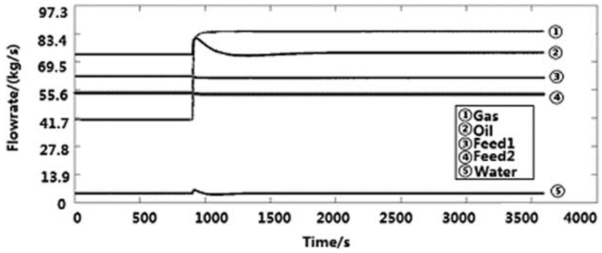



Figure 14. Mass flow rate changes of feed flows, separated oil, water, and gas flows when antisurge valve is stuck.

above the safety relief pressure limit, the three-phase separation process is at a catastrophic state (referring to Table 15). 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 15. 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 are 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.

## Discussions and Perspectives

From the case study results, some significant features of the framework for computer-assisted HAZOP studies are discussed below:

First, only a systematic, creative, and imaginative examination by the HAZOP team can yield a high quality HAZOP report. This means that the traditional HAZOP is limited by the expertize and experience within the team which may not guarantee identification of every possible hazard or operability problem that could arise during the actual operations. The MFM-based HAZOP presented here provides a complementary tool to the traditional HAZOP as it can support the process of brain-storming explicit by being a tool for identification, elaboration, and discovery of possible failure scenarios. Thereby, the MFM-based tool assists HAZOP team to carry out HAZOP studies and provides quality of the study and enables identification of more complex possible scenarios.

Second, another demonstration of the methodology has linked functional modeling to HAZOP.[9] Also, it is the first time an MFM model of a three-phase separation process in the specific oil and gas production field has been presented in the literature. The possibility offered by a functional modeling could track causes and consequence paths from node unit to whole system level.

**Table 14. Trend Time for each Plugging Change**

| Plugging Fraction | Trend Time (s) |
|---|---|
| 0 | 300 |
| 0.1 | 300 |
| 0.2 | 300 |
| 0.3 | 300 |
| 0.4 | 600 |
| 0.5 | 600 |
| 0.6 | 900 |
| 0.7 | 1200 |
| 0.8 | 1200 |
| 0.9 | 1200 |
| 0.95 | 1200 |
| 0.98 | 1200 |

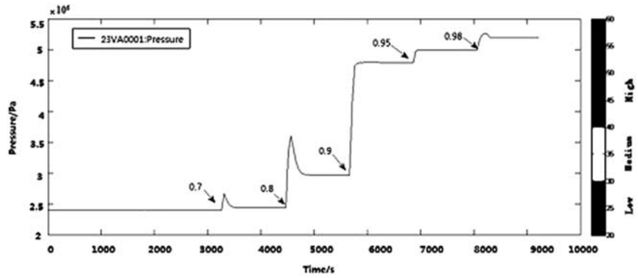



Figure 16. Pressure changes of the separator along with the changes of separator outlet gas pipeline plugging fraction.

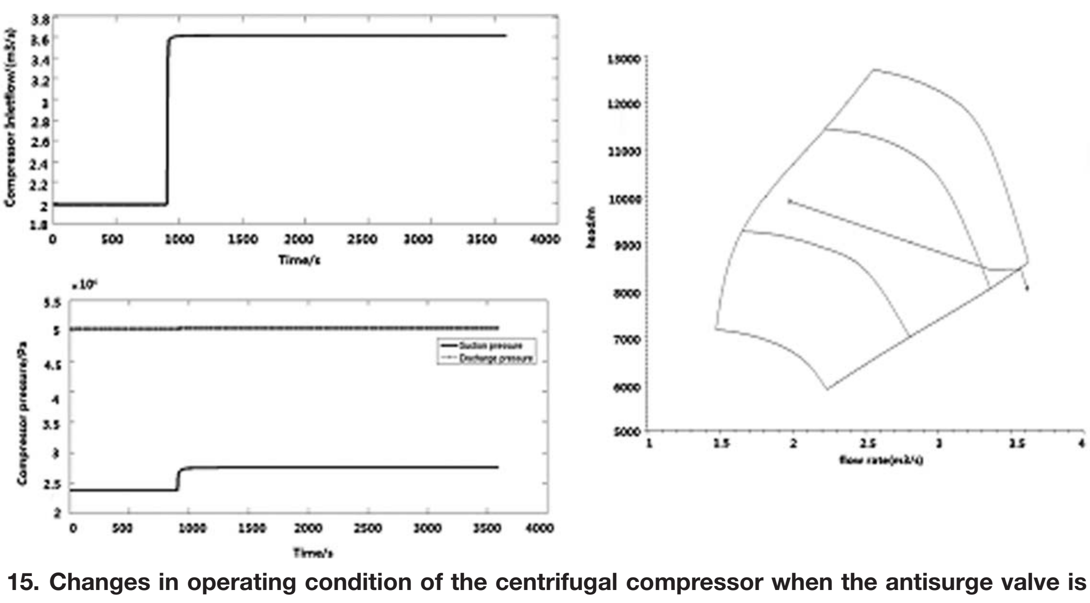



Figure 15. Changes in operating condition of the centrifugal compressor when the antisurge valve is stuck.

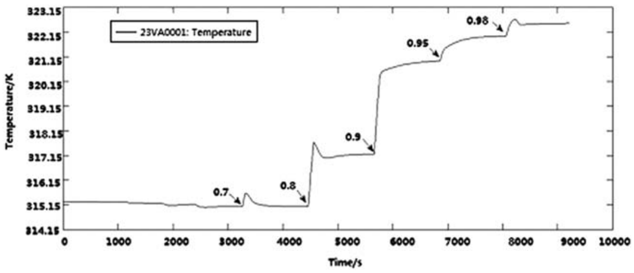



**Figure 17. Temperature changes of the separator along with the changes of separator outlet gas pipeline plugging fraction.**

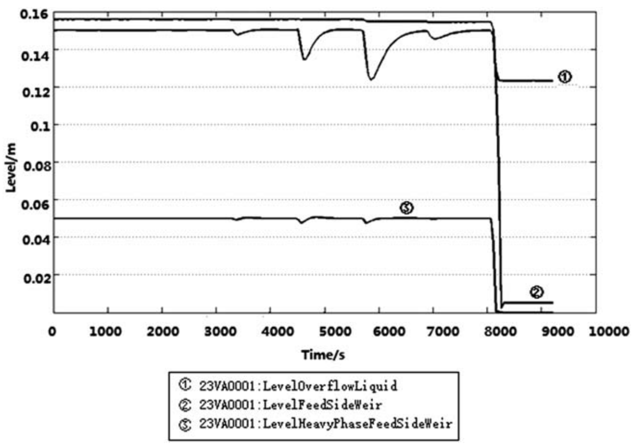



**Figure 18. Level changes of the separator along with the changes of separator outlet gas pipeline plugging fraction.**

Third, the output of the qualitative part of the integrated methodology is the modified HAZOP worksheet. By comparison of results from the traditional HAZOP with those of MFM-based HAZOP, it is demonstrated that we can find potential causes and consequences systematically by MFM-based HAZOP, and the results are in accordance with the traditional HAZOP. However, the coverage of guide words in MFM based HAZOP should be improved by introducing the concept of roles and additional reasoning rules.[31] 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

**Table 15. 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 |

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. Reasoning about the realization relations of roles between structure and function makes it possible to consider consequences of component failure in MFM and the extension of MFM with roles also support the representation of and reasoning about redundancy. Therefore, the expressivity and reasoning ability of extending MFM with information of the plant structure will make it possible to deal with the myriad of plant details, that is, design data and specification. Addition of the further guide words "no," "part of," "as well as" would be directly possible, but will require further development of the MFM reasoning engine.

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. However, it also should be noted that some catastrophes, with low probability but high consequence, will be in the right bottom corner in the risk matrix even though they also may lead to significant loss consequences. Those consequences should not be ignored, such as the nuclear leakage in Japan resulting from the recent tsunami. Once a low probability event with high consequences occurs, it may expand into a huge disaster leading to environmental, human, and economic catastrophes such as the Macando well blowout in Gulf of Mexico in 2010. Therefore, based on this different understanding of the concept of risk, some companies pay much more attention on such scenarios when HAZOP studies are performed.

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

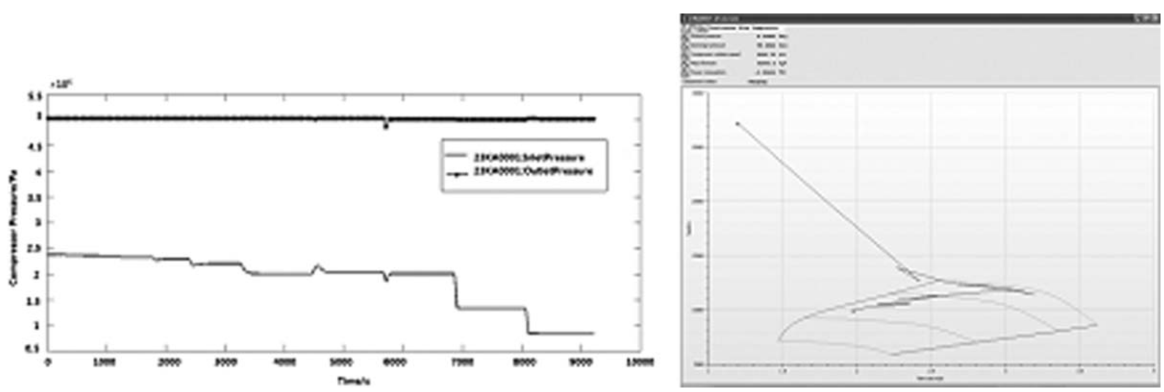



**Figure 19. Changes in operating condition of centrifugal compressor along with the changes of separator outlet gas pipeline plugging fraction.**

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 reducing 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 topic for future work.

Sixth, in industrial practice HAZOP studies are carried out at various stages during the plant life cycle. The integrated methodology developed in this article could be best suitable for FEED stage, where it makes the most sense to invest time and resources for a comprehensive hazard identification and risk analysis. It is common industry practice to divide FEED stage into three stages with typical deliverables: material and energy balance, preliminary equipment design, and layout, purchase-ready major equipment specifications and preliminary three-dimensional (3-D) model, and so forth. For the FEED 1 stage, functional modeling is suitable for qualitative process modeling. For the dynamic modeling, FEED 3 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 technique. The knowledge-based reasoning system developed here demonstrates a promising potential and feasibility for automating some of the tasks involved in HAZOP analysis. The tool complements the HAZOP team in completing a comprehensive analysis as well as in better use of their time and resources that comes with the model-based assistance.

## Conclusions

An integrated qualitative and quantitative modeling framework for HAZOP studies that uses MFM and knowledge-based reasoning system, risk matrix, and quantitative dynamic simulation for verification and validation risks has been proposed. The integrated framework is successfully applied to a realistic three-phase separation process system. To this extent it provides 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 application case provides a reasonable basis for demonstrating the integrated methodology. Here the qualitative functional modeling supports the HAZOP analysis team in formulating the goal-function relationships for the system and enables qualitative reasoning about the cause–consequence paths for selected deviations. Furthermore, the more critical process hazards can be directly evaluated through quantitative dynamic simulation. The results demonstrate the importance of the formulation of MFM models to represent the physical system for acquisition of HAZOP knowledge in the qualitative part of the overall methodology. From this point of view, the quantitative analysis obtained from the dynamic simulation complements and enhances the MFM model based process safety analysis of the system in particular regard to the transient dynamics of the system.

The methodology generates a HAZOP worksheet, which resembles quite closely that obtained from a traditional HAZOP. This research demonstrates a promising potential and feasibility of functional knowledge-based tool to assist some of the tasks involved in HAZOP and as such contributes to better use of resources and time for a HAZOP team. The outcome of the tool is cause–consequence paths with high potential hazard risks. These potential high risks are used as input for quantitative framework to analyze in detail the operability issues and validate the cause–consequence paths with high potential hazard risk using a dynamic process simulation.


## Acknowledgments

The first author is thankful to China Scholarship Council (CSC), Ministry of Education (File No. 201206440002) for the grant of a scholarship for 1 year and the support from the research groups at Dept. of Electrical Engineering and Dept. of Chemical and Biochemical Engineering at DTU. This work is also supported by the Natural Science Foundation of China (Grant No. 51104168), the Excellent Doctoral Dissertation Supervisor Project of Beijing (Grant YB20111141401), the Program for New Century Excellent Talents in University (NCET-12-0972), Beijing Natural Science Foundation (3132027) and also by Science Foundation of China University of Petroleum (No. YJRC-2013-35).


## Notation

### *Acronyms*

HAZOP = Hazard and Operability Studies
MFM = Multilevel Flow Modeling
P&ID = Piping & Instrumentation Diagram
PSE = Process Safety Engineering

## Literature Cited


1. Kletz TA. *Hazop and Hazan: identifying and assessing process industry hazards. Institution of Chemical Engineers*, 2001.
2. Nolan DP. *Safety and security review for the process industries [electronic resource] : application of HAZOP, PHA and What-If reviews*. William Andrew, 2008.
3. Crawley F, Preston M, Tyler B. *HAZOP: Guide to best practice: guidelines to best practice for the process and chemical industries*. IChemE, 2008.
4. Khan FI, Abbasi SA. OptHAZOP—an effective and optimum approach for HAZOP study, *J Loss Prev Process Ind*. 1997;10:191–204.
5. Enemark RR, Cameron D, Angelo PB, Sin G. A simulation based engineering method to support HAZOP studies, vol. 31. In Karimi IA, Srinivasan R, editors. *Proceedings of the 11th International Symposium on Process Systems Engineering (Computer-Aided Chemical Engineering)*. Elsevier Science, 2012:1271–1275.
6. Khan FI, Abbasi SA. Mathematical model for HAZOP study time estimation. *J Loss Prev Process Ind*. 1997;10(4):249–257.

7. Dunjó J, Fthenakis V, Vílchez JA, Arnaldos J. Hazard and operability (HAZOP) analysis. A literature review. *J Hazard Mater*. 2010; 173:19–32.
8. Vaidhyanathan R, Venkatasubramanian V. Digraph-based models for automated HAZOP analysis. *Reliab Eng Syst Saf*. 1995;50:33–49.
9. Srinivasan R, Venkatasubramanian V. Petri net-digraph models for automating HAZOP analysis of batch process plants. *Comput Chem Eng*. 1996;20:719–725.
10. Rossing NL, Lind M, Jensen N, Jørgensen SB. A functional HAZOP methodology. *Comput Chem Eng*. 2010;34:244–253.
11. Stephanopoulos G, Reklaitis GV. Process systems engineering: from Solvay to modern bio-and nanotechnology.: a history of development, successes and prospects for the future. *Chem Eng Sci*. 2001; 66:4272–4306.
12. Garcia HE, Vilim RB. Combining physical modeling, neural processing, and likelihood testing for online process monitoring. *IEEE International Conference on Systems, Man, and Cybernetics*, San Diego, CA, USA, 1998.
13. Komulainen TM, Enemark RR, Sin G, Fletcher JP, Cameron D. Experiences on dynamic simulation software in chemical engineering education. *Educ Chem Eng*. 2012;7:153–162.
14. Cameron D, Clausen C, Morton W. Dynamic simulators for operator training. *Comput-Aided Chem Eng*. 2002;11:393–431.
15. Lind M, Yoshikawa H, Jørgensen SB, Yang M. Modeling operating modes for the Monju nuclear power plant. *Int J Nucl Saf Simul*. 2012;3:314–324.
16. Gola G, Lind M, Zhang X, Heussen K. *A multilevel flow model representation of the operation modes of the control systems in a PWR pressurizer*. OECD Halden Reactor Project Report, Institute for Energy Technology, Halden, Norway.
17. Wu J, Zhang L, Liang W, Hu J. A novel failure mode analysis model for gathering system based on multilevel flow modeling and HAZOP. *Process Saf Environ Prot*. 2013;91:54–60.
18. Lind M. Modeling goals and functions of complex industrial plants. *Appl Artifi Intell*. 1994;8: 259–283.
19. Lind M. Means and ends of control. *IEEE International Conference on Systems, Man, and Cybernetics*, The Hague, Holland, October 10–13, 2004.
20. Lind M. An introduction to multilevel flow modeling. *Int J Nucl Saf Simul*. 2011;2:22–32.
21. Lind, M. *Reasoning about causes and consequences in multilevel flow models. In: Advances in Safety, Reliability and Risk Management – Proceedings of the European Safety and Reliability Conference, ESREL 2011*. European Safety and Reliability Association. 2012:2359–2367.
22. Zhang X, Lind M, Ravn O. Consequence reasoning in multilevel flow modeling. In *Proceedings 12th IFAC Symposium on Analysis, Design and Evaluation of Human-Machine Systems*, Las Vegas, August 11–15, 2013.
23. Thunem HP-J, Thunem AP-J, Lind M. Using an agent-oriented framework for supervision, diagnosis and prognosis applications in advanced automation environments. In: *Advances in Safety, Reliability and Risk Management – Proceedings of the European Safety and Reliability Conference, ESREL 2011*. European Safety and Reliability Association. 2012: 2368–2375.
24. Thunem HP-J. The development of the MFM Editor and its applicability for supervision, diagnosis and prognosis. In: *Proceedings of ESREL* 2013, Amsterdam.
25. Chittaro L, Guida G, Tasso C, Toppano E. Functional and teleological knowledge in the multimodeling approach for reasoning about physical systems: A case study in diagnosis. *IEEE Trans Syst Man Cybern*. 1993;23: 1718–1751.
26. Eizenberg S, Shacham M, Brauner N. Combining HAZOP with dynamic simulation—applications for safety education. *J Loss Prev Process Ind*. 2006;19:754–761.
27. Searle JR. *The construction of social reality*. The Free Press, A Division of Simon and Schuster, 1995.
28. International Standards Organization, *Space Systems Risk Management*, ISO 17666.
29. KONGSBERG K-Spice® Tutorial, Training Manual, May 2012 © Kongsberg Oil & Gas Technologies AS.
30. Wu J, Zhang L, Jørgensen SB, Jensen N, Zhang X, Lind M. Procedure for validation of a functional model of a central heating system. In: *The 5th World Conference of Safety Oil and Gas Industry*. June 8–11, 2014, Okayama, Japan.
31. Lind M. Knowledge representation for integrated plant operation and maintenance. In: *Proceedings of Seventh American Nuclear Society International Topical Meeting on Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies*, November 7–11, 2010, Las Vegas.

## Appendix A. The Explanations of Elements in (Flow Structures, Objectives, Relations, and Functions) in Figures 5 and 6 are Presented in Detail as Below

| Flow structure | Objective | Function name | Function | Structure |
|---|---|---|---|---|
| Elements explanation in MFM model in Figure 5 | | | | |
| 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 |

**Appendix A. Continued**

| Flow structure | Objective | Function name | Function | Structure |
|---|---|---|---|---|
| | | 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 | Antisurge 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 flow 1 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 |

**Appendix A. Continued**

| Flow structure | Objective | Function name | Function | Structure |
|---|---|---|---|---|
| | | 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 6 | | | | |
| 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 from energy flow perspective | obj2:maintain the right pressure (obj2), i.e. the right amount of energy in storage (sto3) | sou3 | Gathered feed flow energy source | Gathered feed flow |
| | | tra9 | Transport the energy of gas | Temperature and pressure of the gas |
| | | 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 12 (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 | The working condition of the compressor is normal but is approaching a blocking state. |
| | | | | Compressor | 381.15 | | | | 5.14 | 42.78 | |
| | | | | 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 | |

*Manuscript received Nov. 19, 2013, and revision received Aug. 4, 2014.*