Proceedings of the 33rd European Safety and Reliability Conference (ESREL 2023)
Edited by Mário P. Brito, Terje Aven, Piero Baraldi, Marko Čepin and Enrico Zio
 Published by Research Publishing, Singapore.
doi: 10.3850/978-981-18-8071-1_P660-cd

Process hazard analysis: Proposing a structured procedure based on Multilevel Flow Modelling

Ruixue Li

Department of Electrical and Photonics Engineering, Technical University of Denmark, Denmark
E-mail: ruilia@dtu.dk

Jing Wu

Department of Electrical and Photonics Engineering, Technical University of Denmark, Denmark
E-mail: jinwu@dtu.dk

Xinxin Zhang

Department of Electrical and Photonics Engineering, Technical University of Denmark, Denmark
E-mail: xinz@dtu.dk

Ole Ravn

Department of Electrical and Photonics Engineering, Technical University of Denmark, Denmark
E-mail: oravn@dtu.dk

Process hazard analysis is significant in improving process safety in complex systems. Hazard and operability study (HAZOP) is one of the event-based methods of displaying hazards in the process industry, which can identify a wide range of hazards throughout the process life. However, HAZOP would repeat work on the same failure and lack a global view, as well as the result is not highly readable and reusable. Therefore, a hazard analysis procedure based on Multilevel Flow Modeling (MFM) is proposed. The procedure divides the system into sub-objectives and flow-based structures, subsequently analyzing and modeling hazard knowledge in terms of the objects and agents that realize the function. By comparing with a HAZOP report of the Minox process in a water injection system, it is demonstrated that MFM-based hazard analysis shows the potential for a more systematic and comprehensive representation of process hazards to improve process safety management.

Keywords: Process Hazard Analysis (PHA), HAZOP, Multilevel Flow Modelling, Process hazard procedure, Functional modeling, Process safety.

1. Introduction

Process hazards analysis is a set of structured assessments to identify potential hazards and evaluate the risks associated with a process or system, which includes management policies, procedures, and practices aimed at preventing or mitigating catastrophic incidents in industrial processes. There are several methods that can be used to conduct the process hazard analysis. The most commonly used methods are Hazard and Operability study(HAZOP), What-If analysis, Checklist, Failure Modes and Effects Analysis (FMEA), and Fault Tree Analysis (FTA)(Luo, 2010). A summary of how the different methods are chosen is in Wu et al. (2022).

In HAZOP, the identified hazards are guided by guide words and presented in the form of causes and effects of parameters/variables. The initial motivation for using the Multilevel Flow Modelling (MFM) for HAZOP automation study (Rossing et al., 2010) or MFM-assisted HAZOP studies (Wu et al., 2014) is its natural advantage in representing the results of HAZOP analysis, as it's a functional modeling approach of system information, mass and energy.

However, HAZOP study has its limitations in hazard identification as follows:

- Lack of a global view
- Duplication of work:1) for one deviation in different nodes, the causal analysis of the same

root cause is repeated; 2) for multiple deviations in one node, duplication of work occurs when different deviations are actually caused by one deviation
- Lack of level of details in cause-effect analysis
- Lack of utilization of the HAZOP results

As HAZOP initiates the analysis by dividing the entire system into equipment-based nodes, this results in the consideration of only local interactions within the nodes and ignores the entire process when analyzing the causes-consequences of deviations. Since hazards may propagate through the flow, upstream will affect downstream, leading to repeated analysis of the same deviation within different nodes, reducing the efficiency. Also, since flow-based deviations are also the cause of their pressure, temperature, and level deviations, analyzing all deviations within the same node without any skipping can also cause repetitive and inefficient work (Duhon, 2011).

HAZOP method is structured and systematic in identifying hazards because the analysis is based on the system layout itself, node by node, without missing a single element, which means that all components of the process are analyzed in a structured sequence. However, it is systematic in terms of the object of analysis, not at the stage of cause-and-effect analysis. On the contrary, because HAZOP is all about guide-word-driven causal analysis, it can make its results appear flatter and lack a clear hierarchical structure, namely, lack of the level of details in causal analysis. For example, when analyzing the same category of deviations for different nodes, some nodes will consider the mechanical integrity, such as whether there is a pipe rupture, but some nodes will only consider the functional aspect of the equipment. This reflects that HAZOP is not sound and clearly hierarchical when doing causal analysis for the same type of deviations for different objects.

In addition, HAZOP findings are often underutilized in subsequent risk assessment analysis and operational support for online decision-making (Mu and Venkatasubramanian, 2003). Firstly, it's because HAZOP reports presented in list form are stored in a relatively isolated way after completion and are not integrated into online use or ranking of identified risks through other quantitative methods (Fuentes-Bargues et al., 2016), apart from being used for offline risk identification and corrective recommendations. Namely, it's not treated as part of online abnormal event management or as part of subsequent risk management; secondly, due to the lack of standardization requirements for language expressions, the understanding of the guide words may cause ambiguity due to unclear analysis objects, and thus unclear descriptions of the defined deviations. For example, when people who did not attend the HAZOP analysis workshop read the report, they may need to determine the specific reference of deviations, compromising the report's readability and usability.

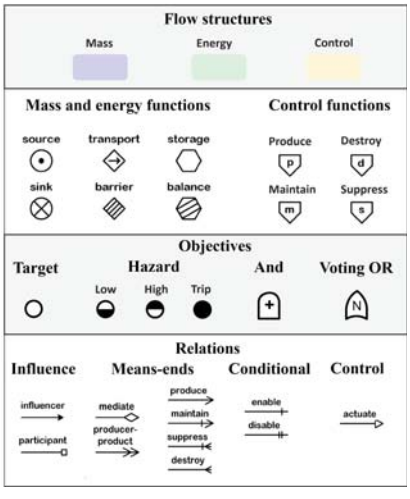


Fig. 1. Basic symbols of MFM method

Owing to these limitations, it becomes clear that treating the MFM approach simply as an aid or automation of HAZOP studies is not sufficient. MFM is based on a hierarchical decomposition of the whole system's function, from the plant level to the component level, with a clear and complete hierarchical structure and a perspective on the whole picture(Lind, 2017). And the powerful reasoning function can quickly locate the root cause and end consequence of deviations, not only analyze the local impact but also trace the

global scope of causality. Plus there is a formal model language to transfer the contained hazard information without errors and ambiguities(Wu et al., 2021), which is of practical significance for the reuse and regular update of the model.

Therefore, we propose a procedure for process hazard analysis based on the MFM approach that addresses these limitations and provides a clear hierarchical structure in the causal analysis for more structured knowledge acquisition and representation. Thus it enables a more comprehensive and systematic identification of process hazards, as well as laying the foundation for building a database of hazard information and creating the possibility of establishing a library of equipment-related hazards based on functional classification.

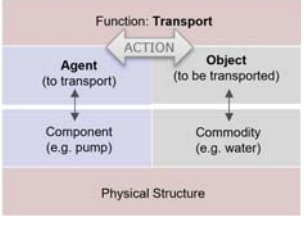


Fig. 2. Interpretation of objects and agents in the function and structure semantics

2. Process hazards analysis procedure

2.1. *MFM method*

MFM is a functional modeling method that models the objectives and functions of the system by examining the interaction of mass, energy, and information (Lind, 2011). MFM modeling is a top-to-bottom decomposition from system purpose to function to component, which is a decomposition of the system from means-ends and part-whole dimensions. Through the intention and causality contained in the means-end relations, the MFM model's inference capability allows for efficient applications in fault diagnosis (Nielsen et al., 2018) and alarm analysis. The meaning of the MFM symbol can be found in Fig. 1. More details on interpreting model notation and building models through knowledge acquisition and representation can be found in Wu et al. (2021).

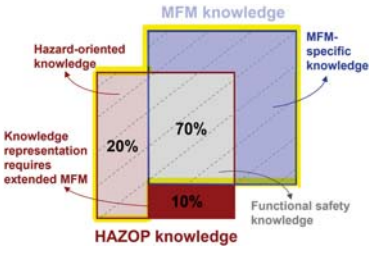


Fig. 3. Knowledge coverage of the proposed procedure

In the study of failure analysis of physical components, roles are presented as a representation of the function-structure relation(Lind, 2010). A function always has roles associated with it as the support for the realization of the function, and this role includes objects and agents. Shown in Fig. 2, for the function of transport, in order to achieve this function, i.e. successful transport, an agent (pump) is needed to provide the action (to transport) and an object (water) is needed to guarantee the conditions under which this action can occur (to be transported).

2.2. *MFM-based process hazard analysis procedure*

HAZOP and MFM methods share a common nature of being knowledge intensive. HAZOP requires piping and instrumentation diagrams (P&IDs) and process flow diagrams (PFDs) as the most basic input for the process, while MFM models also store functional model knowledge of system intention and means-ends relations. Therefore, for the use of the proposed MFM-based procedure for hazard analysis, it is necessary to explain the scope of knowledge that it can cover compared to HAZOP.

MFM modeling acquirers knowledge of process objectives and functions from documents containing PFD, P&ID, Standard Operational Procedures (SOPs), System Control Diagrams (SCDs), Process Descriptions, and Cause-effect diagrams (CEDs), etc., and of safety objectives and functional knowledge including safety standards and requirements, etc (Wu et al., 2021). Since the MFM model was originally used for operational support purposes, the use of the MFM

Table 1. Object-based hazard knowledge: consideration for mass or energy

Hazards of properties		Hazards of quantity / state	
Chemical properties	Physical properties	Variable	Guide word
toxic, corrosive, explosive, combustible, flammable, etc	fouling, sharp/high hardness damage, thermal damage, hydraulic damage, pneumatic damage, etc	flow, phase, composition	no, more, less, other than, as well as, part of, reverse

model for process hazard analysis only contains functional safety knowledge compared to HAZOP, and lacks hazard-oriented knowledge (Li et al., 2023). To allow a comprehensive view of the MFM-based process hazard analysis approach, the knowledge coverage of the proposed procedure is MFM knowledge and hazard-oriented knowledge, as shown in Fig. 3.

From the perspective of MFM, hazards are triggered in terms of abnormal function states, whereas abnormal function states are determined by the roles that support the realization of the function, and roles are divided into objects and agents. Therefore, the process of analyzing hazards in MFM is to analyze the objects and agents of the function to determine whether they can cause the function to be abnormal. The form of hazard and analysis of roles are shown below:

- Trigger of a hazard: abnormal function state
- Forms of a hazard: abnormal function state + cause-effect propagation path
- Object: Consider the impact of the Physico-chemical properties of the object and its quantity/state on the function realization
- Agent: FMEA, consider the impact of failure modes of agent on functional realization

2.2.1. *Trigger and forms of hazards*

Since MFM is naturally characterized by causal reasoning, the hazard is still represented in the form of abnormality + causality. The abnormal function state can be understood semantically as function failure resulting from role failure. So from the perspective of model language means: 1) for energy flow, high or low state of temperature and pressure; 2) for mass flow, high or low state of level, flow, and pressure.

2.2.2. *Object*

The failure of an object leads to the failure of its function, and the object is either a material entity or an energy. Therefore, to analyze the hazards that cause the failure of an object is to consider the hazards of the properties of mass and energy themselves, as well as the anomalies caused by anomalies in their quantity or state. Table 1 shows the sources of hazards for object failure. Chemical properties consider common properties in the Chemical Hazard Database. One of the common thermal damage is the overpressure of thermal expansion. For quantity or state, the failure of the object is described by the variable and the corresponding guide word:

- Flow: no/more/less/reverse/other than.
- Phase: more/less/other than.
- Composition: as well as/part of/other than.

2.2.3. *Agent*

The failure of an agent also leads to the failure of its function. The agent is mass when the object is energy, and the agent is a physical structure when the object is mass. To identify more comprehensive agent-based hazards, the failure modes of the agents are modeled from the FMEA approach perspective. Common failure modes considered in MFM include the following:

- Mechanical integrity failure: The physical structure is leaked, ruptured, or damaged.
- Environmental failure: The conditions/environment needed to realize the function are not reached.
- Maintenance failure: The agent has problems due to improper or erroneous maintenance.
- Component failure: Failure of a single component results in the failure of the agent.

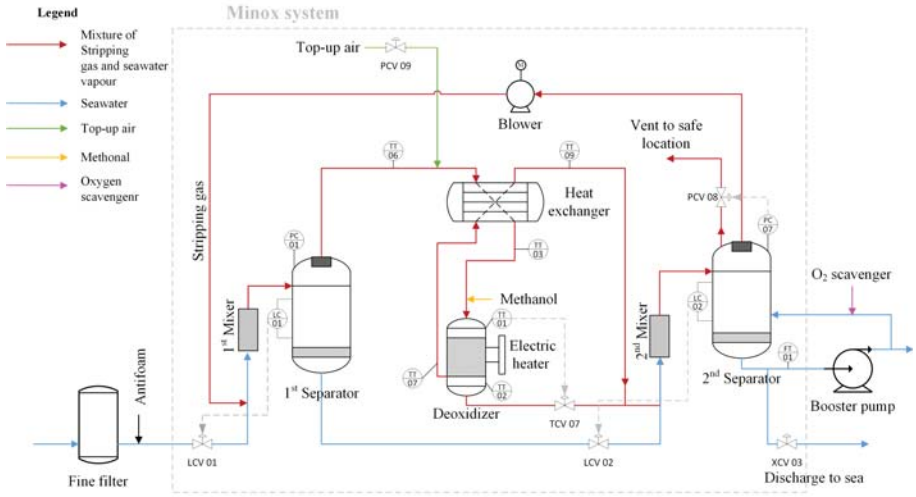


Fig. 4. The Minox system in a water injection system flow chat

- Aging failure: Agent fails due to prolonged use.
- Electrical failure: Component circuits malfunction or lack power supply.
- Performance degradation: The agent cannot work at the expected level of performance due to hidden hazards.

2.2.4. *Steps for MFM-based hazard analysis*

For the total intention of a system, it is decomposed into sub-objectives from top to bottom, and then the functions are identified from each sub-objective, and then hazards are identified in terms of what affects the successful realization of each function. Such a means-end, whole-part analysis process is the MFM-based hazard analysis process, which models the hazards of the objects or agents that can cause function failure and thus represents the hazard-oriented knowledge. The causal inference capability of the MFM approach allows the identification of the path of hazard occurrence and evolution with the input of a trigger, thus supporting the management of process safety. The steps are as follows:

(i) Identify the overall intention of the system.
(ii) Decompose into sub-objectives.
(iii) Identify the mass and energy flows involved in the sub-objectives and divide them into flow-based structures.
(iv) Identify the functions contained in the flow-based structure. The functions can be described as actions to achieve sub-objectives, like transporting fluid, reacting with gas, etc.
(v) For each function, analyze the roles, i.e. objects and agents, required to realize the function. Analyze whether the roles carry any risk of failing the function. Object-based hazards are identified by Table 1 and agent-based hazards are identified from the failure modes.
(vi) The system model is built through the MFM workbench (Rossing et al., 2010) to represent the knowledge of the role-based hazards and other knowledge (Wu et al., 2021).
(vii) For each function, the trigger of hazard is specified. The cause-consequence analysis is performed on the MFM workbench.

3. MFM-based hazard analysis for Minox system

The flow diagram of a Minox system in a water injection system is shown in Fig. 4. The seawater passes through two separators in sequence and mixes with the stripping gas to reduce the oxygen content of the seawater Wu et al. (2021).

The overall intention of Minox system is to reduce the oxygen content in seawater below a required value. The sub-objectives, flow-based structures, and functions are defined in Table 2.

Table 2. Sub-objectives, flow-based structures, and functions for Minox system

Sub-objectives	Flow-based structures	Functions
Strip oxygen from seawater	Seawater flow	Separating oxygen
	Booster pump energy flow	Moving the seawater
	Oxygen flow	Removing oxygen by reaction
		Removing oxygen by separation
	Stripping gas flow	Stripping oxygen
		Exchanging heat
		Maintaining pressure by top-up air
		Maintaining pressure by vent valve
	Blower energy flow	Circulating stripping gas
	Methanol flow	Removing oxygen by reaction
	Methanol pump energy flow	Providing methanol
	Catalyst flow	Removing oxygen by reaction
	Temperature flow	Providing heat for reaction
	Pressure flow	Maintaining pressure for separation
Oxygen scavenger works when oxygen is still higher than required	Oxygen scavenger flow	Scavenging oxygen
	Oxygen flow	Removing oxygen by scavenger

After completing the first 4 steps, the hazard knowledge of the role corresponding to the function is analyzed. The role-based hazards are analyzed using methanol flow as an example. Methanol reacts with oxygen in stripping gas at a certain temperature with a catalyst thus removing oxygen. Therefore, for the basic function of methanol flow, i.e. the reacting, the object is methanol and the agent is the deoxidizer.

3.1. *Object-based hazard knowledge*

Considering the object-based hazards in terms of properties, methanol is highly flammable in a high-temperature and aerobic environment; from the quantity aspect, both less and more methanol flow cause the function to fail. So the object-based hazards of methanol flow and other related flows are denoted as follows:

- Quantity: flow more/no. Related to methanol pump energy flow.
- Properties: flammable. Related to temperature and oxygen flows.

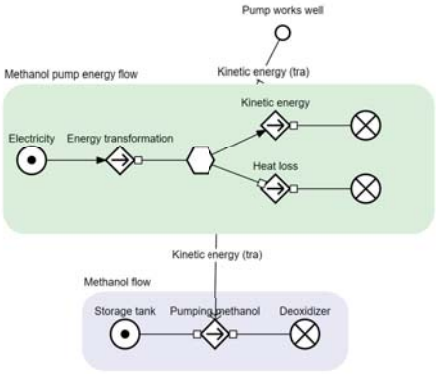
After identifying the object-based hazards of methanol, the hazard knowledge and the associated flow structures need to be represented in the system model. According to step 6, an MFM model of the entire system is developed by representing the knowledge acquired from process and safety aspects. The whole model can be found in (Li et al., 2023). The modeling of the methanol flow is shown in Fig. 5. Fig. 5a indicates the relation between the quantity deviation of the methanol flow and the methanol pump. Fig. 5b shows how the preconditions for methanol explosion are represented by OR logic gate.

3.2. *Agent-based hazard knowledge*

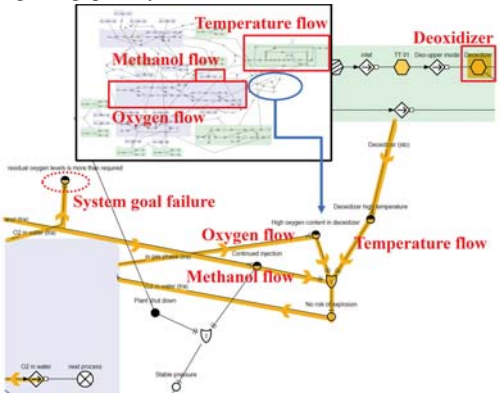
The agent deoxidizer's structural integrity determines the realization of the function(reacting). Since the function is considered for the methanol flow, the structural damage caused by the methanol flow is considered. The realization of the function also has environmental requirements, where the reaction needs to take place at a certain temperature. So the agent-based hazards of methanol flow and other related flows are denoted as follows:

- Mechanical integrity failure: Rupture due to vessel overpressure. Related to pressure and oxygen flows.
- Environmental failure: Temperature failed. Related to temperature and oxygen flows.

As above, Fig. 6 illustrates the model for the methanol flow section, where the reacting func-



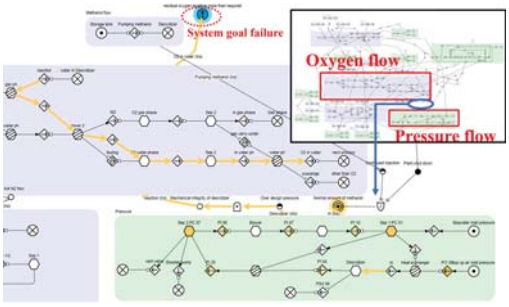
(a) Representing object-based hazard knowledge regarding quantity



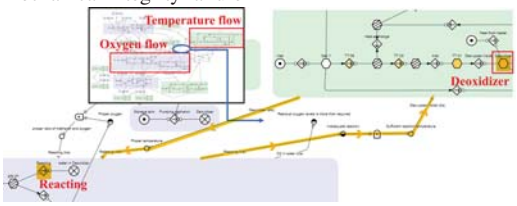
(b) Representing object-based hazard knowledge regarding properties

Fig. 5. Modeling of methanol flow

tion is represented by a transport symbol over the oxygen flow, indicating the fraction of the total oxygen flow that is eliminated by the deoxygenation reaction. As hazard knowledge directly affects the failure of the function, the two above failure modes are related to the oxygen flow when modeling. Fig. 6a depicts through logic gates, targets, and hazards that excess methanol in the deoxidizer can cause vessel damage and reaction termination, thus causing system goal failure due to overpressure. Fig. 6b shows how the temperature in the deoxidizer affects the performance of the deoxygenation reaction, because the reaction heat is also one of the sources of heat supply, so there is a cyclic influence structure as shown.



(a) Representing agent-based hazard knowledge regarding mechanical integrity failure



(b) Representing agent-based hazard knowledge regarding environmental failure

Fig. 6. Modeling of methanol flow

4. Discussion

4.1. *Continuous and non-repetitive representation*

For the built Minox model, the hazard trigger for the function reacting is low flow representing a low amount of oxygen eliminated by the reaction. Through the MFM workbench reasoning, 25 root causes and 2 end consequences can be found. In the HAZOP report corresponding to this Minox system, a total of 7 deviations related to methanol reaction, there are two deviations as follows:

- Malfunctional methanol pump →Flow No →Reduced deoxygenation capacity
- Methanol supply failure →Low Temperature →Deoxygenation reaction interrupted

However, these two deviations are actually continuous and lie on the same causal path of the root cause (pump failure). Rossing et al. (2010) and Wu et al. (2014) demonstrate that the MFM model has the capability to infer a complete causal path from the root cause to the end consequence, indicating the multi-level causes and consequences

of a hazard trigger. This shows that discontinuous identification and analysis are covered in the inference results of the MFM, avoiding repetitive work.

4.2. *Potential for operational support*

Since both operational and hazard information is contained in the MFM model, the results of process hazard analysis can be integrated for online decision support by including sensor signals into the model as hazard triggers.

5. Conclusion and future work

As functional modeling MFM has an explicit hierarchy and strong inference, this paper proposes a process hazard analysis procedure based on MFM, aiming to realize the transformation of MFM from a HAZOP assistant into an independent analysis method. The procedure divides the system into sub-objectives and flow-based structures, uses abnormal functions as hazard triggers, and analyzes and models hazard information from the object and agent perspectives that realize the functions so that more hazard-oriented knowledge can be included in the MFM model. Object-based hazard knowledge is analyzed from properties and quantity/state, and agent-based hazard knowledge is analyzed from failure modes. Finally, the procedure is demonstrated with the Minox system, which not only reduces the repetitive work of identifying more hazard information compared to HAZOP reports but also has the potential to apply the analysis results to online decision-making, solving the HAZOP pain points.

Future work is to investigate how hazard knowledge identified based on failed function can be represented through more unified model language. Develop a function-based classification of equipment and form a corresponding hazard database.

Acknowledgement

The authors would like to thank The Danish Offshore Technology Centre for supporting the research.

References

Duhon, H. J. (2011). Stream-based hazop: A more effective hazop method. In *SPE Americas E&P Health, Safety, Security, and Environmental Conference*. OnePetro.

Fuentes-Bargues, J. L., C. González-Gaya, M. C. González-Cruz, and V. Cabrelles-Ramírez (2016). Risk assessment of a compound feed process based on hazop analysis and linguistic terms. *Journal of Loss Prevention in the Process Industries 44*, 44–52.

Li, R., J. Wu, X. Zhang, and O. Ravn (2023). Integrating hazard-oriented knowledge representation for multilevel flow modelling in process hazard identification. Unpublished manuscript.

Lind, M. (2010). Knowledge representation for integrated plant operation and maintenance. In *Seventh American Nuclear Society International Topical Meeting on Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies*. American Nuclear Society.

Lind, M. (2011). An introduction to multilevel flow modeling. *Nuclear safety and simulation 2*(1), 22–32.

Lind, M. (2017). Knowledge acquisition and strategies for multilevel flow modelling. In *International Symposium on Future Instrumentation and Control for Nuclear Power Plants*.

Luo, H. (2010). The effectiveness of u.s. osha process safety management inspection – a preliminary quantitative evaluation. *Journal of Loss Prevention in The Process Industries - J LOSS PREVENT PROC IND 23*, 455–461.

Mu, F. and V. Venkatasubramanian (2003). Online hazop analysis for abnormal event management of batch process. In *Computer Aided Chemical Engineering*, Volume 14, pp. 803–808. Elsevier.

Nielsen, E. K., S. Jespersen, X. Zhang, O. Ravn, and M. Lind (2018). On-line fault diagnosis of produced water treatment with multilevel flow modeling. *Ifac-papersonline 51*(8), 225–232.

Rossing, N. L., M. Lind, N. Jensen, and S. B. Jørgensen (2010). A functional hazop methodology. *Computers & chemical engineering 34*(2), 244–253.

Wu, J., M. Lind, X. Zhang, K. Pardhasaradhi, S. K. Pathi, and C. M. Myllerup (2021). Knowledge acquisition and representation for intelligent operation support in offshore fields. *Process Safety and Environmental Protection 155*, 415–443.

Wu, J., M. Song, X. Zhang, and M. Lind (2022). Safeguards identification in computer aided hazop study by means of multilevel flow modelling. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability*, 1748006X221086341.

Wu, J., L. Zhang, J. Hu, M. Lind, X. Zhang, S. B. Jørgensen, G. Sin, and N. Jensen (2014). An integrated qualitative and quantitative modeling framework for computer-assisted hazop studies. *AIChE journal 60*(12), 4150–4173.