Advances in Reliability, Safety and Security, Part 4 – Kołowrocki, Dąbrowska (eds.)
 ISBN 978-83-68136-16-6 (printed), ISBN 978-83-68136-03-6 (electronic)

Advances in Reliability, Safety and Security

ESREL 2024
Monograph Book Series

Towards Effective Hazard Analysis: Qualitative Modeling Approach For Diagnosing Control Function Failures Using Multilevel Flow Modeling

Jing Wu, Ruixue Li, Xinxin Zhang

Automation and Control, Department of Electrical and Photonics Engineering, Technical University of Denmark, Lyngby, 2800, Denmark

Abstract

Failures of control systems including wrong interactions with control systems by operators can lead to accidents. Model-based techniques can model control systems to diagnose such failures. However, traditional mathematical models of control systems do not consider the relationships between process and control on a system level. It also requires detailed information after the detailed design stage. Instead, functional models can be used for the early stage of system development. Multilevel Flow Modeling technique (MFM), as a representative functional modeling method, was applied to modeling control systems. However, the modeling of failure modes of control systems and reasoning rules regarding the control functions were not completely implemented. Consequently, it creates a problem when MFM Models are used for safety analysis, i.e., Hazard and Operability Study (HAZOP) for identification of hazards related to control functions and reasoning about their consequences. To enable MFM to diagnose such hazards, a modeling method for two typical input devices of control systems: switches and analogues is proposed in this paper. A process HAZOP study of a water injection system is used as a modeling input for examining consequences due to the failures of control systems. The scope of the paper is limited to diagnosing control function failures qualitatively for a single failure mode in one mode of operation, i.e., the normal operational mode.

Keywords: safety analysis, system control, process complexity, functional modeling, social-technical system

1. Introduction

Accidents may happen if control systems fail, including wrong interactions with control systems by operators (Zhen et al., 2022). A system(equipment) is under control shown in Figure 1. It can be seen clearly that if a controller is out of function or the wrong operator's commands are based on a misunderstanding of the system's status, all can affect the plant status. If the operating status of the system is beyond the safety limit, and there is no adequate response, accidents occur. To diagnose such failures, model-based techniques were proposed (Abid, Khan and Iqbal, 2021). However, traditional mathematical models of control systems do not consider the relationships between process and control on a system level (Heussen and Lind, 2012). It also requires detailed information after the detailed design stage. Instead, functional models can be used for the early stage of system development. Multilevel Flow Modeling technique (MFM) (Lind, 2014), as a representative functional modeling method, was applied to modeling of control systems.

The control system has a design intention. If a control system has a safety role, either as an integral part of the EUC or as a separate protection system, it will be a safety-related system to achieve safety-oriented control objectives. If a control system has a process role, to maintain a process to work in a normal operational range (between low and high states), it will be a process-related system to achieve process-oriented control objectives. MFM can distinguish the two types of objectives and they are treated as different functional concepts semantically in MFM. Zhang and Lind (2017) established causal reasoning through MFM control functions. These reasoning rules are given the sensors' information is correct, about the corresponding control actions influencing the states of the controlled element. These rules are not for diagnosing what are the causes of failures

of control systems. According to the analysis conducted by the Health and Safety Executive (Great Britain, 2003), the summarized reasons for the failures of control systems are as follows:

- Failures to cope with multiple failure modes;
- Inconsistent safety function specifications due to a number of design parties or when sub-systems are being designed concurrently;
- Inadequate safety integrity level, e.g., only a single channel design;
- Failures to cope with failures of the computer or programmable systems;
- Failures to cope with all modes of operation;
- Failures to consider the operator as part of the safety-related system;
- Failures to consider the guidelines or standards regarding safety-related systems;
- Lack of formal safety validation during the control systems' design or system modification.

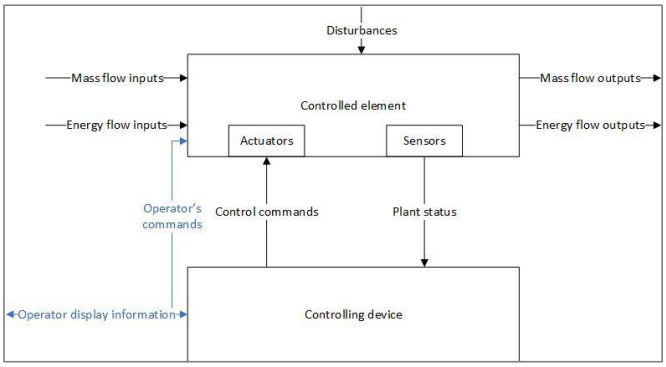

Fig. 1. Equipment under control (EUC).

To enable MFM to diagnose the failures of control systems, one key element is to represent those different failure patterns in MFM. In this paper, a modeling method for two typical input devices of control systems: switches and analogues, for implementing control functions is considered. A Process HAZOP study of a water injection system is used as a modeling input for examining consequences due to the failures of control systems. The scope of the paper is limited to diagnosing control function failures qualitatively for a single failure mode in one mode of operation, i.e., the normal operational mode.

The paper has the following sections, Section 2 introduces the challenges of understanding control functions from the process and its safety perspective. In Section 3, the literature on the functional modeling of controls is reviewed and summarized. Then, the modeling method of control failure modes is proposed in Section 4. The case study of safety analysis of a water injection system is used for demonstration in Section 5. In the end, the conclusions are given.

2. Understanding control functions from the process and its safety perspective

In the safety research domain, control functions are seen as one barrier function to reduce the possibility/ for a hazard to occur or limit its harm/disadvantages. Control functions can work individually or collectively. Safety is about avoiding hazards. From the energy control perspective, a hazard is seen as an energy source. Control functions are to separate in time and space, the victims from the energy being released. One typical example is the Energy Barrier Analysis (Rahimi, 1986), which analyzes the means of controlling the levels and the transfer of potential unwanted energy. From the situation control perspective, a hazard is seen as an unwanted situation. Control functions are to control abnormal operations and detect failures. The typical examples are the defense of depth and layer of protection. From the accident control perspective, a hazard is seen as a possible source or cause of an accident. Control functions are to control hazardous events. A typical example is the risk assessment of machinery, which identifies all the relevant hazardous events and identifies relevant means to prevent such events. In this paper, control functions are to control normal operations from the process perspective and protect the systems from the safety perspective.

3. The literature review of functional modeling of controls

Based on the previous understanding propositions, there were several pieces of literature research for investigating how to model controls from function views.

STAMP (Systems-Theoretic Accident Model and Processes) (Leveson, 2004) was proposed on the assumption that accidents occur due to inadequate control systems. It views that the goal of controls is to enforce constraints on system development and on system operation that result in safe behavior. The function of controls is an adaptive feedback function that maintains safety as performance changes over time. Classification of control failures is given into three categories: (1) Inadequate enforcement of constraints; (2) Inadequate execution of control action; (3) Inadequate or missing feedback. However, one challenge in this method is to identify the right process model that is controlled by the controller. The whole paradigm of the STAMP is based on the traditional control theory, so the causality between the process and control is not obvious. For example, the influence of one control action failure cannot obviously be examined on another part of the system. Because the three categories of control failures are examined on a single control loop. This may lead to disabilities by diagnosing system-level failures.

GTST (Goal tree-success tree) and MLD (Master Logic Diagram) (Modarres, 1999) were proposed to decompose a system in terms of functions into two parts: main functions and support functions. For each part, it can further decompose into different levels: objective, generalized functions, physical functions, and components. Physical functions can be described according to a formalized structure composed of functional primitive, variable, object or classobject and context. The dynamic features can be considered if necessary. The cause-effect between the main functions and support functions can be found in the interdependency matrix. The mapping relations between structures and functions are explicit. However, the disadvantage of the method is the model is described using natural language. The model can be extremely scaled up when modeling complex systems, even if it is impossible. The relations in the GTST model are defined based on mathematical relations which are difficult to interpret when they are applied to expressions of relations of functions. The relation between process functions and control functions is not clear.

To support the interface design of automatic control systems, a set of functional primitives (Liu, Nakata and Furuta, 2004) was proposed to describe the functions of control systems: “control”, “generate”, “transform”, “set”, “select”, “calculate”, “limit” and “delay”, and their graphical representations. However, this work simply considers the control functions describing signal flow information of control systems. In this way, it may help operators to identify the operating mode of a system because of the certain patterns of control functional representations, but still, it is difficult for operators to understand the causes of control failures. Because the causality is not in control signals.

Based on action theories, a set of control functions was proposed in MFM: “maintain”, “produce”, “destroy”, and “suppress”. As mentioned previously, control systems may have two types of objectives: process-oriented control objectives and safety-oriented control objectives. MFM can distinguish the two types of objectives and they are treated as different functional concepts semantically in MFM. However, the internal functions of a control system are not specifically described in MFM. The consequence effect of the control actions through the process model is included but not the causes of control function failures. The biggest advantage of MFM is having clear relations between process and control functions, and it can be used for system-level analysis for different applications, even for complex systems. In the next section, the failures of four conditions for establishing control functions are represented by MFM for explicit modeling of control failures.

4. The current MFM modeling of control functions and its reasoning

For a typical control loop, to effect control over a system requires four conditions (Ashby, 1973):

- the controller must have a goal or goals;
- the controller must be able to affect the state of the system;
- the controller must be (or contain) a model of the system;
- the controller must be able to ascertain the state of the system.

MFM can represent the four conditions in terms of control objectives and functions. For example, the Glycol Flash Drum in Figure 2 is a horizontal three- phase separator with the function of providing sufficient retention time for any entrained hydrocarbons to separate from the rich glycol. Any hydrocarbon gas which is liberated from the rich glycol solution in the Glycol Flash Drum is routed to the LP Flare. The hydrocarbon condensate floats on the surface of the glycol and is skimmed off into an internal open-topped catchment chamber. Excess hydrocarbons are discharged to the closed drain. The controllers of the flash drums are shown in Table 1.

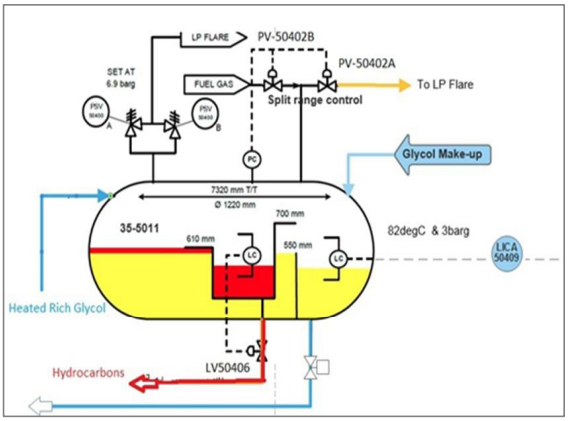

Fig. 2. A glycol flash drum process.

Table 1. Setpoints and alarms for the flash drum.

Controller Tag	Set Point	Low Alarm	High Alarm
LICA-50406 (Condensate Level)	On/Off Control 500 On 375Off	375mm	500mm
LICA-50409 (Glycol Level)	500mm	400mm	600mm
PICA-50402	3barg	2barg	5barg

For example, a controller LICA-50409 is to regulate the Glycol level in the flash drum. In the MFM model, Figure 3, the state of the material storage sto19_GlycolPh is linked to the target state Obj2_GlycolLvl. The value of Obj2_GlycolLvl indicated by the level sensor is the glycol level of the flash drum (condition 4). The state of the fulfillment of Obj2_GlycolLvl influences the control function mco-GlycolLevel (condition 3) to act upon the actuated transport function LV-50409 implemented by the control valve LV-50409 (condition 2). The controller has its objective, which is to maintain the state of the control performance (condition 1).

In MFM, there are 4 control functions shown in Table 2. The other controllers' functions are exemplified in the MFM model in Figure 3.

Table 2. MFM control related concepts and symbols.

Type	Name	Symbol
Control function	Produce	p
	Maintain	m
	Destroy	d
	Suppress	s
Objective state	Target	○
	Hazard	High ◓ Low ◒ Trip ●
Means-end relation	Produce	→
	Maintain	→+
	Destroy	→−
	Suppress	→⊣
Control relation	Actuate	⇢

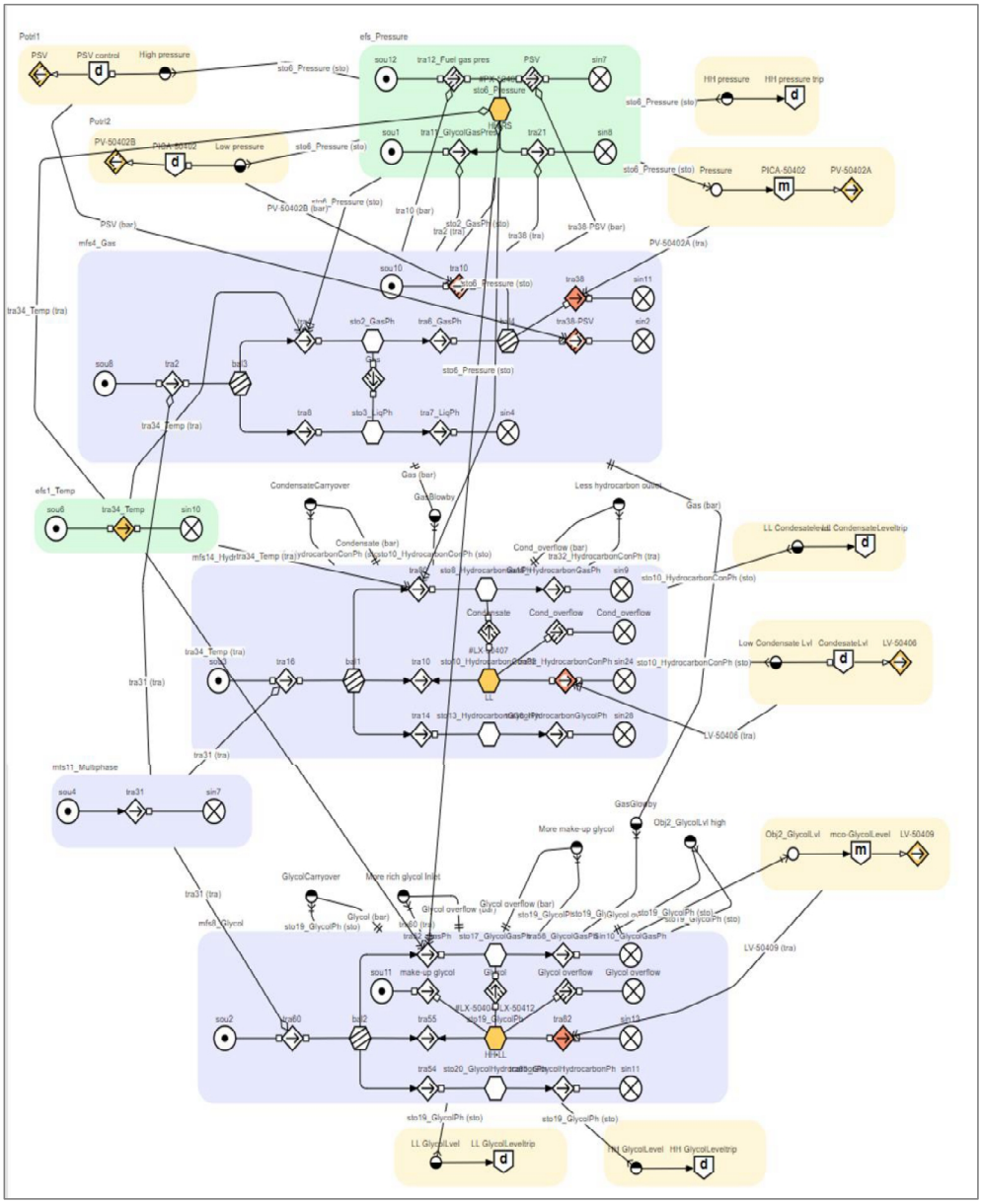

Fig. 3. An MFM model of the flash drum process.

Based on the current MFM consequence reasoning rules, if the inlet flow rate of the flash drum is low, then one of the consequences colored by blue is the opening percentage of the level control valve LV-50409 will decrease given the level control function is normal as shown in Figure 4. Based on the current MFM cause reasoning rules, the root causes colored green are shown in Figure 5. One of the causes is the glycol level control function fails in a way that it decreases its output. However, it does not specify which conditions lead to the failure of the glycol level control function. If the root cause can be identified, then the counteraction plans can be made to prevent undesired events, e.g., the high-high level of the glycol leading to shutdown situations shown in Figure 6. In the next section, the functional modeling of control failure modes is introduced.

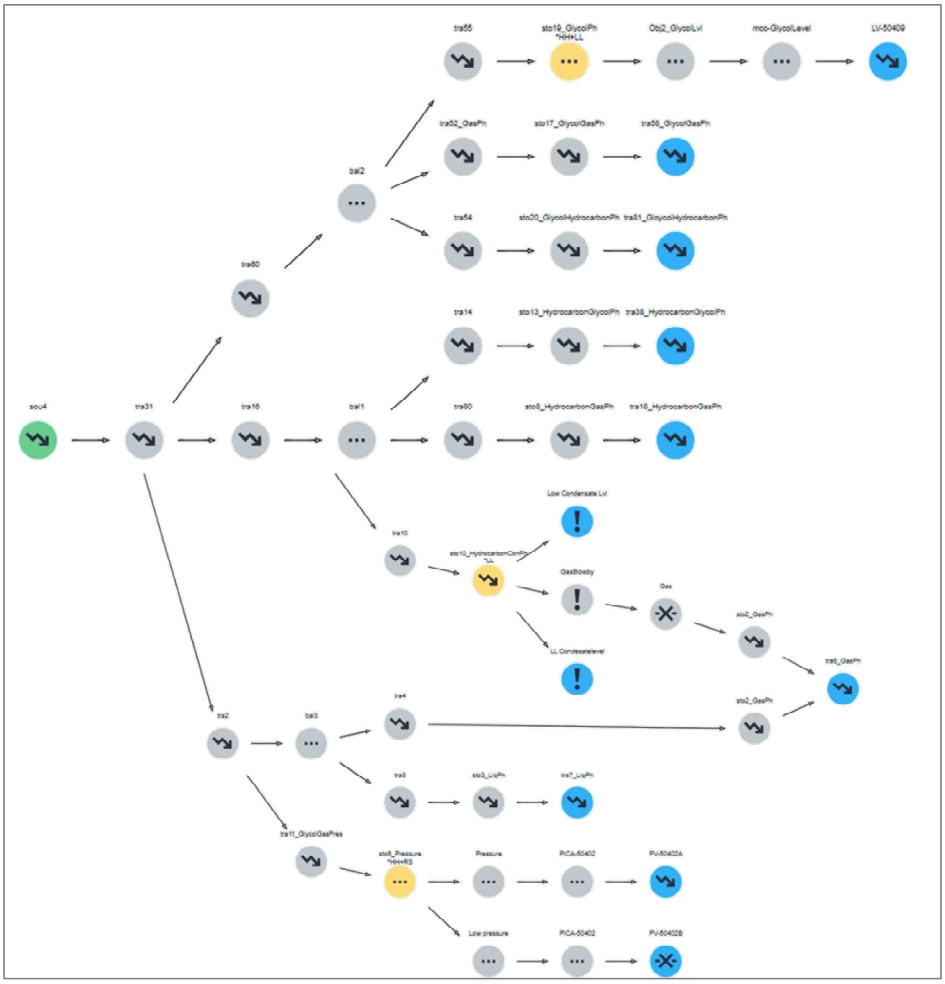

Fig. 4. An MFM model of the flash drum process.

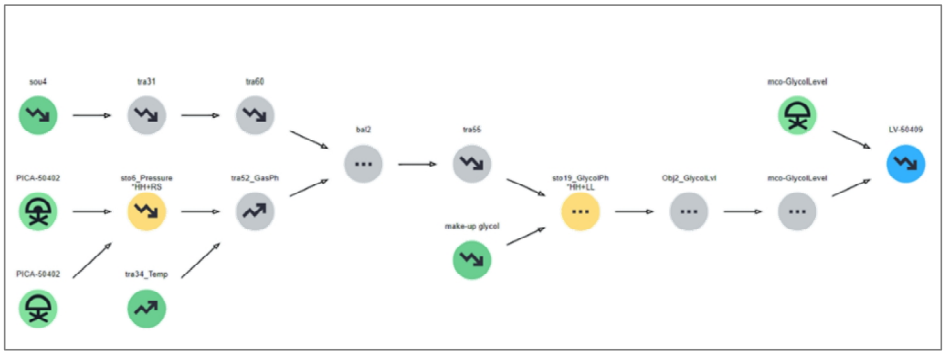

Fig. 5. The causes of the decreasing opening percentage of level control valve LV-50409.

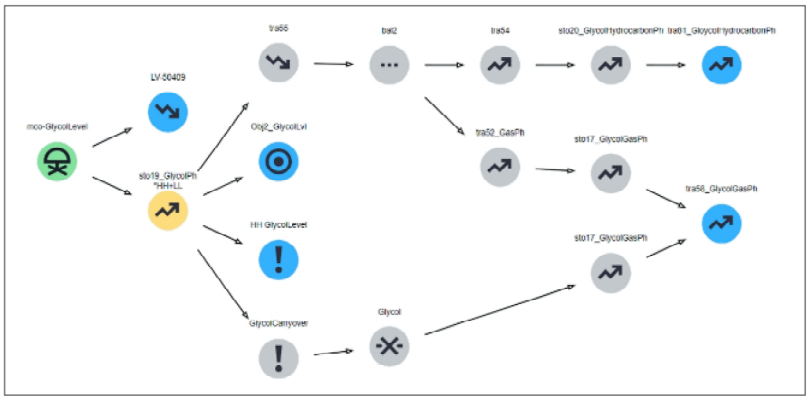

Fig. 6. Flash drum process shutdown due to the failure of the glycol level control function.

5. The current MFM modeling of control functions and its reasoning

In this section, the proposed functional modelling of control failure modes is introduced, where the control hazards of the level controller for a water tank are used as an example in Figure 7. The controller function is modeled as a barrier function in MFM, which means a controller works as a safety function to prevent or suppress the water level in deviating from its set point by either opening or closing the inlet flow control valve. Therefore, there are two working modes for the controller function. One is when the water level is higher than the set point, the controller should decrease the position of the control valve (the left labelled "Decrease"), while the other one is when the water level is lower than the set point, the controller should increase the position of the control valve (the right labelled "Increase"). The modeling of the failures of the two working modes is modelled in two separate energy flow structures. The three working conditions are modelled as hazards, any one of which fails will lead to a failing in the control function. The hazards modeling and reasoning can refer to the work (Wu, Lind and Zhang, 2022). In extreme cases, the left box means that the inlet control valve is supposed to be fully closed but not closed at all while the right box means that the inlet control valve is supposed to be fully opened but not open at all. The modeling method can be applied to two typical input devices of control systems: switches and analogues.

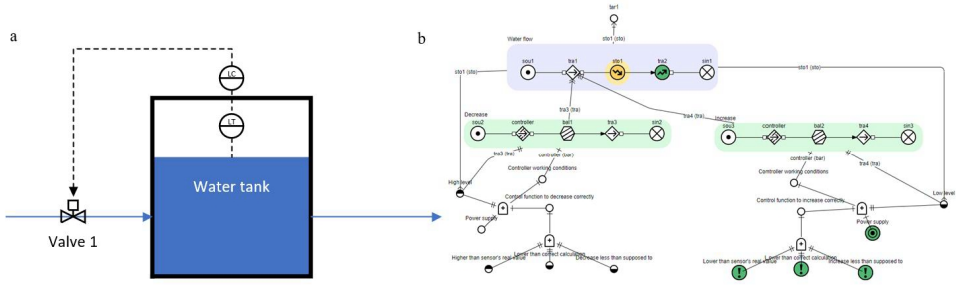

Fig. 7. (a) A water tank is controlled by a level controller; (b) Modelling control hazards for the water tank by MFM: the green nodes highlighted are the possible root causes for low level of the water tank.

6. The case studies

The application of the functional modeling method of control function failures is demonstrated in the safety analysis, i.e., the HAZOP study of a water injection system for examining consequences due to the failures of control systems. In the water injection system, there is a minox system to remove the dissolved oxygen in the seawater. The process diagram is shown in Figure 8. A detailed description of the process can be found in Wu et

al. (2021). The original purpose of the study was to use MFM to support the HAZOP study. The manual HAZOP report is used as a comparison study to examine the effectiveness of the MFM-based HAZOP study. However, during the study, the modeling of control function failures becomes a challenge to deal with the hazardous scenarios due to the failures of controls. Here, the demonstration shows that the proposed modeling method can solve the problem. The developed MFM models focus on the water mass balance of the minox system, and two deviations: no level and more level of the 2nd separator due to the failure of the inlet control valve are used as the case studies. Therefore, the oxygen mass balance is not relevant for this demonstration purpose, which is omitted in the paper. The HAZOP analysis of the two deviations is shown in Table 3.

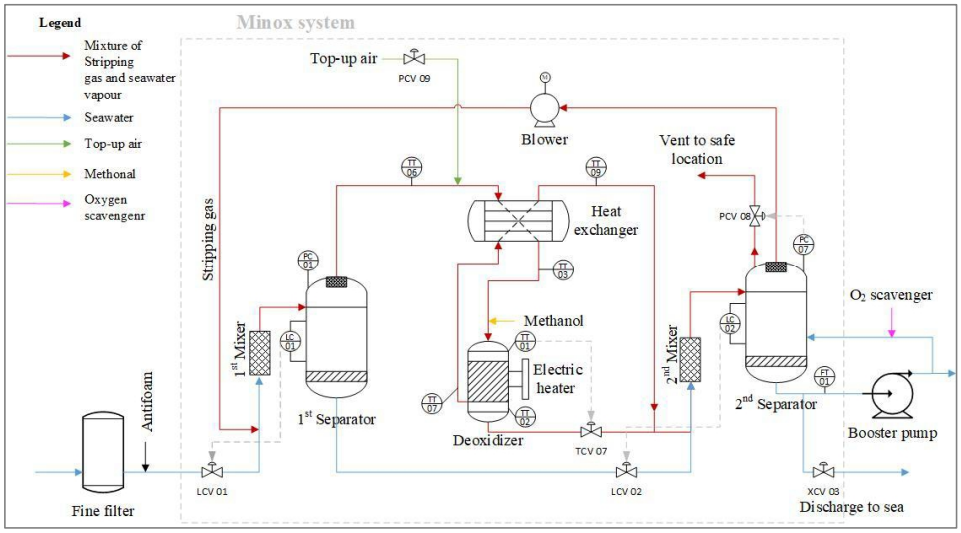

Fig. 8. A process diagram of the minox system in a water injection system.

Table 3. The HAZOP analysis of the two deviations: no level and more level of the second separator.

Deviation	Cause	Consequence	Protection
Level No	Failure closed of LCV-02 at the inlet of the 2nd Separator	Loss of level in the 2nd Separator which may lead to loss of NPSH and cavitation in the booster pumps.	LALL-02 on the 2nd Separator which shuts down the downstream pumps and ESDV-04 at the inlet of the 1st Separator. Protection is considered adequate. No action is required.
Level More	Fail closed of LCV-02 at the inlet of the 2nd Separator	Potential overflow of seawater to N2 stripping system. This would reduce the efficiency of the catalyst.	LCV-01 at the inlet of the 1st Separator will close. If that works, the pumps will be tripped by low low level in the 2nd Separator. If LCV-01 fails, LAHH-02 on the 2nd Separator will shutdown the downstream pumps and close ESDV-04 at the inlet of the 1st Separator. Protection is considered adequate. No action is required.

6.1. Functional models of the water mass balance of the minox system

The function-stream diagram of the water mass balance of the minox system is shown in Figure 9. There are two level control functions, one for the first separator, and another for the second separator. The MFM model is shown in Figure 10. The model consists of one mass flow structure to model the seawater mass balance as described in Figure 9. The model failure patterns of the control functions in Figure 7 are associated with the two level control functions. The process objective is to maintain the seawater flow rate to the injection wells. The two control objectives are to maintain the 1st separator seawater level and the 2nd separator seawater level.

6.2. HAZOP analysis based on the MFM model with reasoning

The two deviations: no level and high level, can be indicated by the states of the storage function labeled LC05, which is associated with the level sensor.

The causes of no level after manual screening based on the MFM model are shown in Table 3. The result shows that one of the causes is that the controller's working conditions are violated. One of the controller's working conditions is that the inlet valve LCV-02 is supposed to open more but it is fully closed. After the causes for no level are identified, by consequence reasoning, the consequences can be obtained. Take the cause: the inlet valve LCV-02 is fully closed; for example, the consequences are shown in Figure 10. The orange-colored highlighted consequence is no flow to the booster pump, which means the loss of NPSH.

If the position of the inlet valve is decreasing less than it is supposed to be, the consequences are shown in Figure 11. The orange-colored highlighted consequence is the seawater overflow to the N2 stripping system.

In this way, the MFM model can support the identification of failures of control functions and their consequences, which are needed for safety analysis, i.e., a HAZOP study.

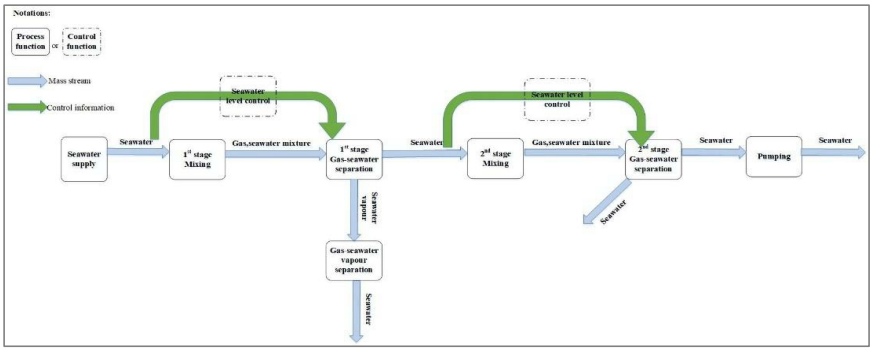

Fig. 9. The function-stream diagram of the water mass balance of the minox system.

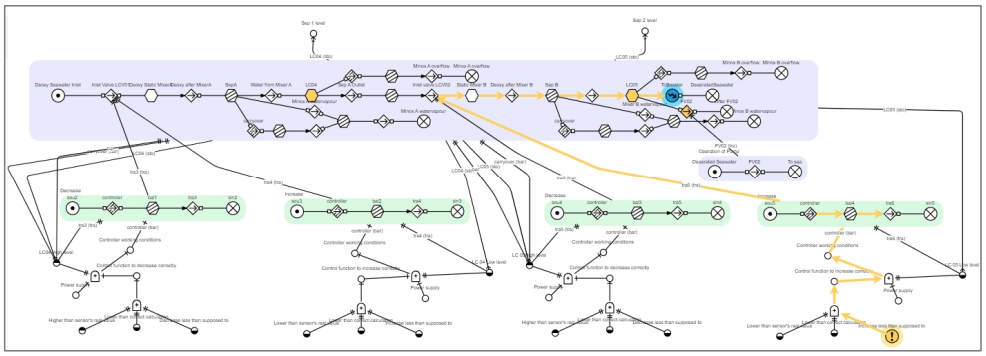

Fig. 10. The consequences of the failure closed of LCV-02.

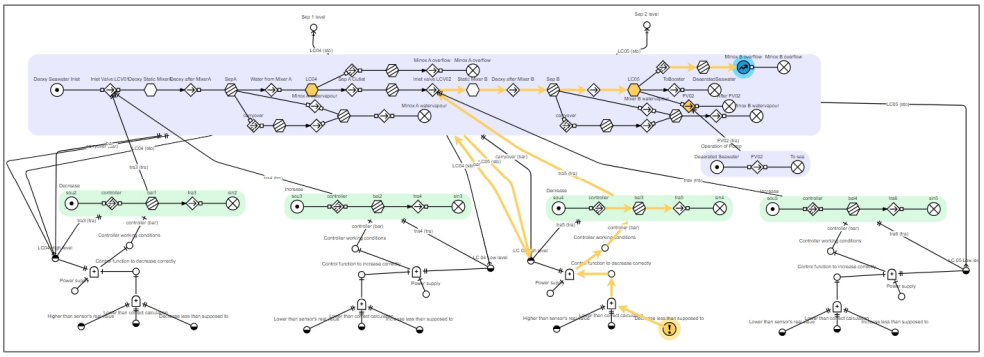

Fig. 11. The consequences of the inlet valve LCV-02 decrease less than it is supposed to be.

7. Conclusions

This paper tackled the challenges of how to model control functions by using the MFM method to enable the functionality of the model for the identification of control functions' failures and their consequences. This is useful for using MFM for the automation of HAZOP study. A modeling method is proposed for control functions. The case studies show that the method applies to a real industry use case. Because the fulfillment of the controller's conditions is modeled by using an AND gate, the cause of the specific failure of its condition requires signal information to confirm. The scope of the paper is limited to diagnosing control function failures qualitatively for a single failure mode in one mode of operation, i.e., the normal operational mode.

Acknowledgements

We would like to thank you for the funding support from DTU Offshore.

References

Abid, A., Khan, M.T., Iqbal, J. 2021. A review on fault detection and diagnosis techniques: basics and beyond. Artificial Intelligence Review 54(5), 3639–3664.

Ashby, W.R. 1973. An introduction to cybernetics. Chapman & Hall, London.

Health and Safety Executive (HSE). 2003. Out of control : why control systems go wrong and how to prevent failure. HSE Books, London.

Heussen, K., Lind, M. 2012. Understanding control function and failure from a process perspective. 2012 IEEE Workshop on Complexity in Engineering, COMPENG 2012 - Proceedings, 22–27.

Leveson, N. 2004. A New Accident Model for Engineering Safer Systems. Safety Science 42 (4), 237-270.

Lind, M. 2014. Functional Modeling of Complex Systems.P. Millot (ed.) Risk Management in Life Critical Systems. Wiley-IEEE press, 95–114.

Liu, Q., Nakata, K., Furuta, K. 2004. Making control systems visible. Cognition, Technology & Work 6(2), 87–106.

Modarres, M. 1999. Functional modeling of complex systems with applications. Proceedings of the Annual Reliability and Maintainability Symposium. IEEE, 418–425.

Modarres, M., Cheon, S.W. 1999. Function-centered modeling of engineering systems using the goal tree-success tree technique and functional primitives. Reliability Engineering and System Safety 64(2), 181–200.

Mokhtarname, R., Safavi, A.A., Urbas, L., Salimi, F., Zerafat, M.M., Harasi, N. 2020. Toward HAZOP 4.0 Approach for Managing the Complexities of the Hazard and Operability of an Industrial Polymerization Reactor. IFAC-PapersOnLine 53(2), 13593–13600.

Rahimi, M. 1986. Systems safety for robots: An energy barrier analysis. Journal of Occupational Accidents 8(1), 127–138.

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

Wu, J., Lind, M., Zhang, X. 2022. Functional Modeling and Reasoning about Hazards. 2022 6th International Conference on System Reliability and Safety (ICSRS), Venice, Italy, 2022, 217-225.

Zhang, X., Lind, M. 2017. Reasoning about Cause-effect through Control Functions in Multilevel Flow Modelling. International Symposium on Future Instrumentation and Control for Nuclear Power Plants. Gyeongju, Korea, 1–8.

Zhen, X., Vinnem, J.E., Han, Y., Peng, C., Huang, Y. 2022. Development and prospects of major accident indicators in the offshore petroleum sector. Process Safety and Environmental Protection, 160, 551–562.