Barrier Identification by Functional Modeling of a Nuclear Power System

Jing WU[1], Morten LIND[1], Xinxin ZHANG[1] and Pardhasaradhi KARNATI[2]

1. Department of Electrical Engineering, Technical University of Denmark, Kongens Lyngby, 2800, Denmark (jinwu@elektro.dtu.dk; mli@elektro.dtu.dk; xinz@elektro.dtu.dk)

2. ELDOR Technology AS, Koppholen 19, 4313 Sandnes (karnati@eldor.no)

Abstract: The paper investigates application of functional modeling for independent protection layer analysis of risk assessment in complex industrial plant with special reference to nuclear power production.

Layer of Protection Analysis （LOPA）is a simplified semi-quantitative risk assessment method that typically builds on the information developed during a qualitative hazard evaluation such as HAZOP. LOPA typically uses order of magnitude categories for initiating event frequency, consequence severity, and the likelihood of failure of independent protection layers (IPLs) to approximate the risk of a scenario. Identifying the IPLs systematically is a fundamental challenge as a basis for estimating the probability of failure on demand of each IPLs and for evaluating the risk to a decision concerning the scenario. Functional safety is the main focus of this study, which shows the modeling and reasoning capability of functional modeling, e.g. Multilevel Flow Modeling (MFM) and its application in IPLs analysis of a design based accident scenario, e.g. Loss of coolant accident (LOCA). Previously, MFM has showed its potential to be used for safety barrier analysis and Defense in Depth.

The main contribution of the study is to explore a procedure using MFM to identify safeguards and then credit some of them as IPLs. Firstly, MFM modeling of the process system including control flow structures is presented. Secondly, the rule-based cause reasoning of MFM is used to identify initiating causes (chain of causes) of a specific consequence. Thirdly, safeguards are derived (safety functions in the system are designed represented by MFM functions) to prevent the consequence to happen. Fourth, judging the initiating causes and safeguards whether they can have common mode failure. If there is no common mode failure, then the safeguard is considered as an IPL. This procedure is demonstrated in a PWR LOCA accident scenario.

Keyword: Risk Assessment, Functional Modeling, Rule-based Reasoning

1 Introduction

Safety functions play an important role in preventing or mitigating accident consequences. Layer of protection analysis (LOPA) [1] provides a procedure for identifying safety functions and evaluating their effectiveness. Specifically, it is a semi—quantitative method that can be used to identify safeguards that meet the independent protection layer (IPL) criteria. Intrinsically, IPL are provided by safety systems.

Although the LOPA method has been developed for more than 20 years since 1993, it lacks a modeling tool of safety systems to analyze the interaction between safety and process systems, to visualize the propagation of the consequence of executing safety systems actions through the process system, and finally to credit those safety systems functioning as IPLs. Therefore, systematic identification of IPLs is a fundamental challenge as a basis for estimating the probability of failure on demand of each IPL and for evaluating the risk concerning the scenario. The present study shows the modeling and reasoning capability of Multilevel Flow Modeling (MFM) [2] applied in IPLs analysis for a design based accident scenario, e.g. Loss of coolant accident (LOCA) [3]. Previously, MFM has showed its potential to be used for safety barrier analysis and Defense in Depth [4].

2 Safety Functions and LOPA

2.1 Safety functions

Safety functions are exploited by safety systems to prevent or mitigate hazards harmful for a target. Among industries, sectors, and countries, different terms are used such as barrier functions [5], depth of defense [6], and protection layers [7]. Barrier theory in safety engineering research can be traced back to 1970s. The concept of barrier comes from the analysis of hazards concerning with environment, ecology and the public health. Haddon [8] proposed ten strategies for reducing the human and economic losses. The vital sixth strategy mentioned by Haddon is the use of material barrier to prevent energy reaching the targets rather than separation in space or time. Furthermore, the ten strategies represent a preference ordering of the barriers. Later in 1980, the Management Oversight and Risk Tree (MORT) [9] approach focus on organizational barriers. In 1989, barrier diagrams have been developed by Taylor et al. [10] in Denmark as a tool for risk analysis in the process industry and it was applied for installations [11-12]. Hollnagel has proposed a taxonomy of barriers including material and symbolic barriers [13]. However, there is no general consensus regarding on the concept of barrier in spite of its importance for safety engineering. Also, there is a lack of a modeling tool for supporting barrier identification.

The term of protection layer was proposed in chemical industry in the late 1980s, the published Responsible Care ®Process Safety Code of Management Practices included “sufficient layers of protection” as one of the recommended components of an effective process safety management system. In the late 1990s, to comply with the emerging international standards emerged for computer based control systems in the process industry, LOPA was introduced to define the necessary safety integrity levels (SILs) for automated safety functions in production facilities in the chemical industry. It was promoted by Center for Chemical Process Safety (CCPS) in 1993. The LOPA method is an “onion” that has several skins from the core. These layers of protection are provided by safety measures built into:

- Process design
- Basic process control systems (PCS)
- Critical alarms and human intervention (PSD, ESD)
- Safety instrumented function(SIF)
- Physical protection relief devices (PSV, HIPPS)
- Post-release physical protection (F&G, Fire hydrant system)
- Plant emergency response (PA)
- Community emergency response

Process design ensures inherently safer systems [14]. Basic process control systems, critical alarms and human intervention, safety instrumented function and physical protection relief devices ensure functional safety. Post-release physical protection, plant emergency response and community emergency response belongs to emergency response. Functional safety is the main focus of the present study.

Safety functions in nuclear industry mainly have three purposes: 1) controlling the reactors, 2) cooling the fuel and 3) containing radiation. Safety functions embedded representation in the process flow can provide insight for safety critical systems which indicate explicit causal relations between safety functions and failure scenarios. And analyzing such causal relations is of great importance in failure analysis, which may give an advantage to improve integrated safety level of systems. Plant operators can also get training from visual representation of safety functions in by understanding how to prevent accidents by making sure that layers remain in function. This is also recognized to be important and is emphasized in the Three-Mile Island (TMI-2) accident report [15]. Here it is stated that dealing with combinations of minor equipment failures require operators and supervisors who have a thorough understanding of the functioning of the plant and who can respond to.

2.2 Independent protection layer in LOPA

An IPL is a device, system or action that is capable of preventing a scenario from proceeding to its undesired consequence independent of the initiating event or the action of any other layer of protection associated with the scenario. A qualified IPL has to be with effective, independent, auditable characteristics. It is a key step in LOPA as shown in Figure 1. However, in order to achieve it, three steps should be accomplished: 1) select a scenario, 2) identify possible initiating causes and 3) safeguards.

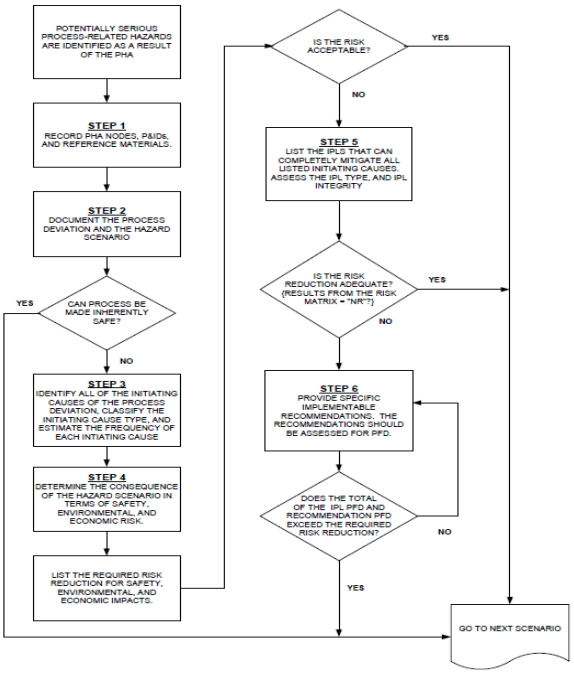

Fig.1 A procedure of LOPA method (adopted from [16])

Researchers have used several approaches for achieving the three steps. Most of them used qualitative process hazard analysis such as HAZOP for defining the scenarios and to minimize the overlooking of the potential scenarios, which are sequences of events that lead to undesired consequences [17]. Then the safeguards or protection layers are found by using techniques such as the bow-tie method [18-19]. For evaluations of the protection layer with respect to independence and efficiency with regard to risk reduction, approaches or rules are put forward by CCPS [20], Stack [21], and Dowell [22].

3 Functional modeling

3.1 Modeling technique

MFM [2] is a network structured hypergraph, where the connection between function nodes (flow functions and control functions) is constrained by syntax rules. Connections represent casual relation (influencer and participate) as shown in Fig.2.and Fig.3. The set of function primitives are defined on the basis of a theory of action types applied for process systems. States of the function nodes are defined by possible failure modes of the specific function. MFM provides facilities for semantic distinctions between different functional abstractions of a system and gives guidelines of how to decompose and aggregate system functions, and how to relate them to objectives using means-end relations [23]. Terminologies of MFM can be found in tutorial [24]. The MFM models presented in the following are built using a model builder called EGolf developed by ELDOR Technology, Norway.

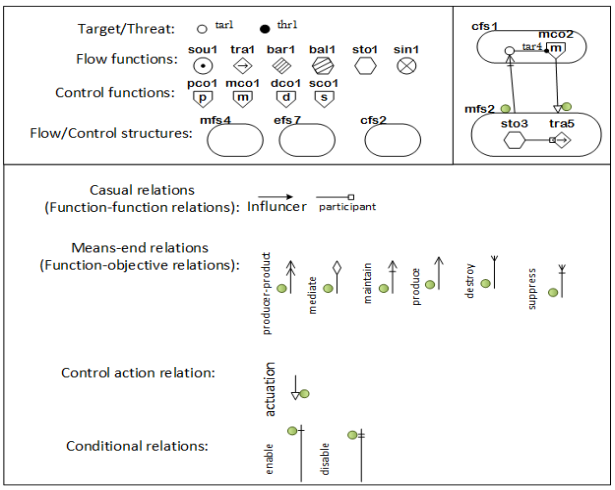

Fig. 2 MFM symbols

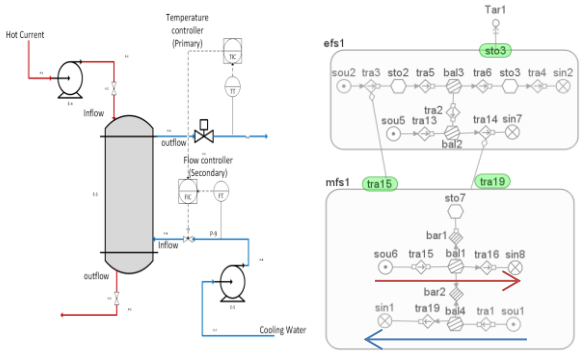

Fig.3 MFM Modeling of a heat exchanger

An objective in MFM represents a situation or state which should be produced, maintained, destroyed or suppressed. Targets are situations or states which are being promoted by the decisions of the process designer or the actions of a control agent. Threats are situations or states which imply a risk or are undesirable by being in conflict with the values of the designer or operators. Targets and threats are related to functions in mass or energy flow structures by means-end relations which are attached with mass or energy flow structures and labeled by the name of the related flow function. Due to syntax restrictions, targets can be attached with produce and maintain means-end relations (production objective), while threats can be attached with destroy and suppress means-end relations (protection objective) as shown in Fig. 4. The protection objective could be to suppress a potential new state or to destroy an actual state. For example, in Fig.4, if the state of storage function sto4 is high i.e. high temperature in the reactor core then the state of threat thr3 is true. Consequently, it disables the barrier function bar2 deployed by fuel cladding in mass flow structure mfs4, which means the fuel enters the reactor coolant.

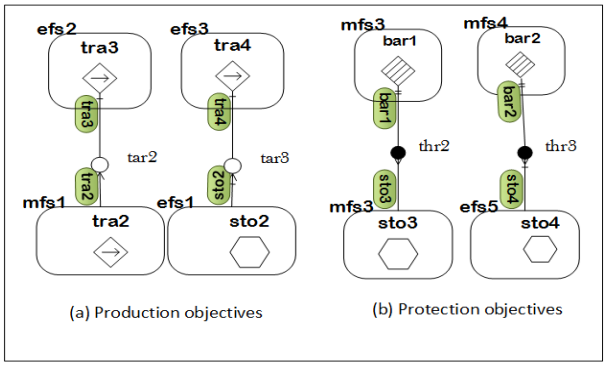

Fig. 4 Targets and threats combined with means-end relations and conditional relations. Combinations are constrained by the MFM syntax

Safety functions are categorized into prevention, control, protection and mitigation. The barrier function in MFM represents the prevention such as bar 1 and bar 2 shown in Fig. 3. Bar 1 represents the function of the shell to prevent the transfer of hot current to surroundings. Bar 2 represents the function of tube and shell to prevent the mass transfer of cooling water and hot current into each other. The functions associated with targets and actuated/enabled functions in MFM are control. The control functions associated with threats and actuated/disabled functions in MFM are protections. The mitigation are the safety functions after the accidental events happen such as emergency response. They are not included in MFM. Those can be handled by QRA for calculating safety zone after accident, i.e. loss of containment to make an emergency plan [25].

3.2 MFM reasoning

Reasoning with MFM models is based on the cause effect relations associated with the function–function and function–objective relations [26]. These casual-effect relations are general, i.e. independent from the concrete systems to be modelled. MFM model reasoning is based on a fixed set of cause-effect inference rules defined by MFM model patterns. The MFM reasoning engine developed at Technical University of Denmark implements the inference rules in a rule-based reasoning shell. The reasoning system propagates state information of each function and can derive possible cause and consequence paths of a given deviation in a functional state. Observations or other evidence is used by the reasoning system to select cause-consequence paths consistent with the given evidence.

The state of barrier function in MFM is either normal, breach-us or, breach-ds. Breach-us means a leak of the barrier from its downstream to its upstream direction and breach-ds means a breach of the barrier from its upstream to its downstream direction. Cause and consequence reasoning patterns for barriers are shown in Fig.5 and Fig.6. For example, if transport function upstream connected with balance function has a low or low-low state then there is a leak of the barrier from its downstream direction. It is equivalent to a leak of balance function.

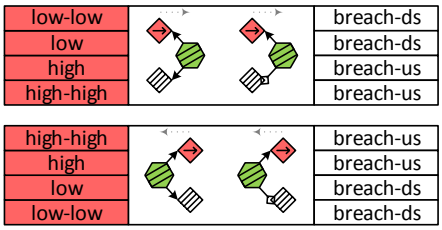

Fig.5 Cause reasoning for a barrier

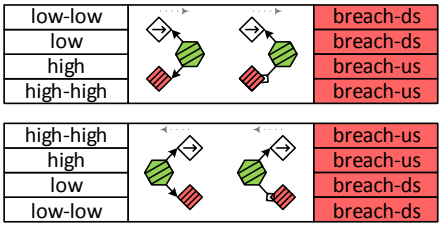

Fig.6 Consequence reasoning for a barrier

Deviations may also be caused by transmitter failure or the control system malfunction. Some accidents report point out that such cause can lead to a disaster. Therefore, cause-effect reasoning about control actions and relations should also be included in MFM to explain why a certain control function is triggered and to explain the control actions which are deployed. Explicit rules for reasoning about control in MFM are descried by Zhang and Lind [27]. The reasoning about barriers and control functions are also implemented and applied in the LOCA accident scenario described below.

4 A new approach for barrier identification

The first step in the approach is to get and analyze process documentations so that the process knowledge acquisition is achieved. Process knowledge is held within the organization in a variety of forms, including systems and procedures, standards and codes, design manuals and other forms of process documents.

The second step is to interpret knowledge by objective-function-structure decomposition (OFS), in a means-ends manner based on existing system documents and experts' knowledge on the operational abstraction level. Learnt from previous modeling experience of the authors, it takes a major effort to create such an MFM model since it requires both configuration and operation knowledge. Therefore, the OFS-decomposition is used as a preliminary step to facilitate the MFM modeling.

Thirdly, the MFM is built including safety functions.

The fourth step is model verification and validation. It is validated that the desired safety targets are met and the undesired threats are destroyed. A validation procedure can be found in Wu [28].

The fifth step is to select a scenario from a HAZOP study.

The sixth step is to search for safeguards and identify initiating causes. Advanced by MFM reasoning rules, safeguards and initiating causes can be found.

Seventh step is IPLs determination. According to the judgment rule sets [20] it is assessed whether the safeguards are qualified to be IPLs.

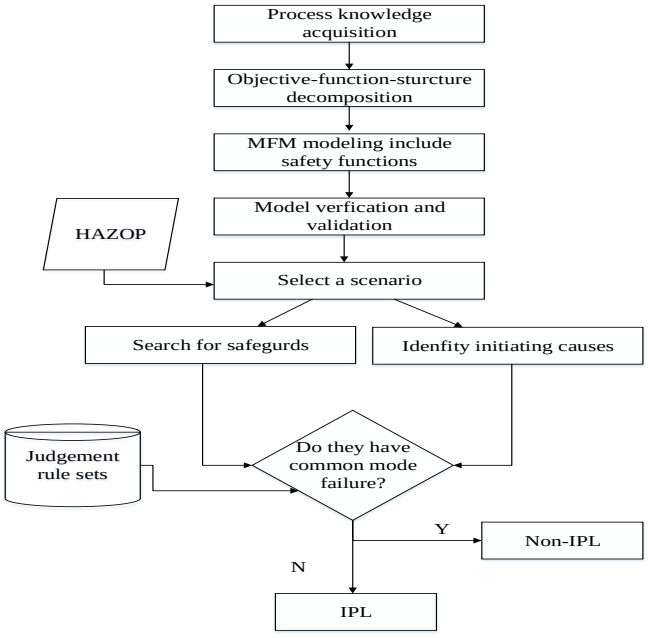

Fig. 7 A procedure for identifying IPLs

5 An application for a LOCA

A loss-of-coolant accident (LOCA） is a mode of

failure for a nuclear reactor. If the engineered safety functions (ESFs) are not actuated effectively, the results of a LOCA could in the worst situation result in reactor core damage. It is a design basis accident (DBA) for the PWR. A LOCA can be categorized into small-break, medium-break and large-break. In essence, the LOCAs are categorized according to the number of trains of emergency core cooling needed to accomplish the safety function, the approximate timing of critical evolutions in an accident scenario, the ability of control room operators to initiate manual back-up actions in case of failed auto-initiation of a safety function, etc.

A small LOCA is an event where the high pressure safety injection system (or equivalent system) is required to maintain coolant inventory, but the heat removal through a cracked or ruptured pipe would not be sufficient to remove decay heat. At the TMI-2 accident, it was such a small break equivalent LOCA which was originally caused by a malfunction of a feed pump in secondary loop.

The TM2 plant diagram is shown in Fig. 8, the plant description can be found in Reference [29]. The reactor coolant system (RCS) with safety functions will be modeled for the LOCA accident. We will investigate whether IPLs exist for preventing such accident if only the process design and basic control systems are considered.

5.1 Modeling of RCS

5.1.1 Decomposition of objectives

From a safety perspective, the overall objective of the RCS is to transfer heat from the fuel to the steam generator. The objective can be further decomposed into mainly three elements: 1.Produce heat by fission process; 2. Remove heat from the reactor core produced by fission process; 3. Prevent radioactive material exposure. The end-means decomposition of RCS safety objectives are shown in Fig. 9.

The AND/OR branches in Fig.9 can be seen as an end/means decomposition structure for the overall objectives and should be read from the end (round dot) towards the means (square dots). The process design and basic process control systems are represented by black boxes. The threats against the safety objectives are represented by the yellow boxes. The safety functions (ESD, SIF, PSV and HIPPS) in abnormal situations are represented by orange boxes. The post-release physical protections are represented by red boxes. The objectives are decomposed from the protection layers strategies by means-ends relations, which is different from the safety objectives developed from accident management information needs point of view [30].

The safety systems include Core Flood System (CF), High Pressure Injection, Makeup, and Purification System (HPI), Low Pressure Injection System (LPI), Reactor Coolant Pressure Control system (RCPCS), Reactor Building Cooling System (RBCS), Reactor Building Sump System (RBSS). The purification system has less to do with the LOCA scenario considered and is therefore not included in the modeling.

5.1.2 MFM models

The MFM model of primary loop of the PWR in TMI under normal operation is shown in Fig. 10. The mass flow structure mfs1 represents the primary coolant mass flow. The storage function sto7_RC represents the storage of water which is heated up in the reactor vessel. The function tra5 represents the transportation of water from the reactor to the steam generator by hot leg which is represented by the storage function sto5_HotWater. The water is transported through the steam generator to the cold leg represented by the storage function sto3_ColdLeg and further transported (tra4) back to the reactor. The transport function tra32 represents the reactor coolant pump. The barrier function bar1 is to prevent the hot water in the RCS leaks to the steam generator secondary side.

In order to keep sufficient coolant in the circuit and maintain its overall system temperature and pressure, facilities are installed include the core flood tank, pressurizer which is equipped with PORV connecting with tail line to the drain tank ,heating rod and the volume-compensation nozzle

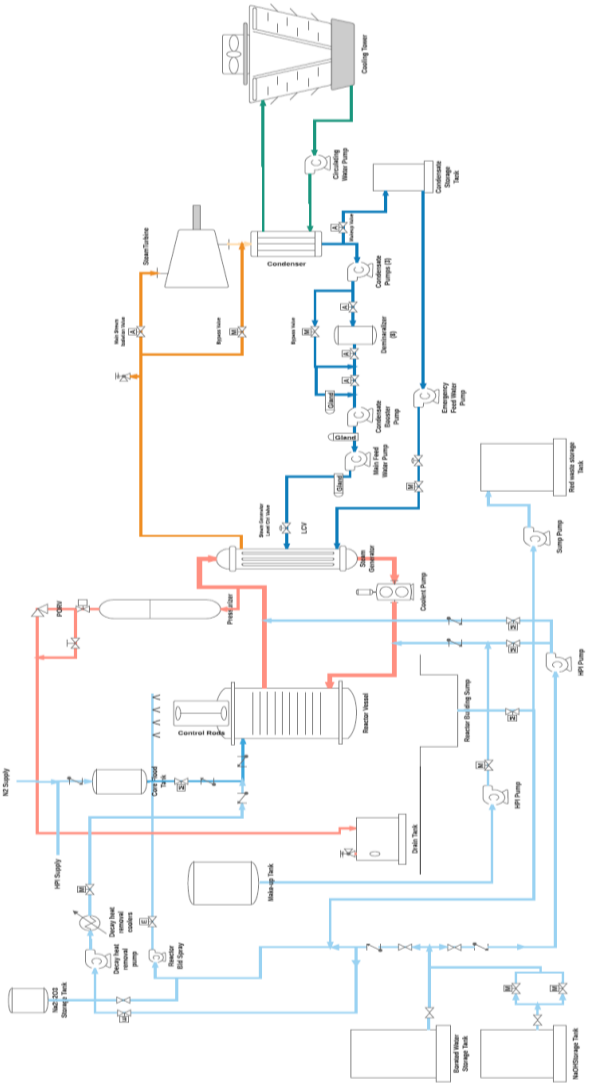

Fig. 8 TMI 2 plant stream diagram

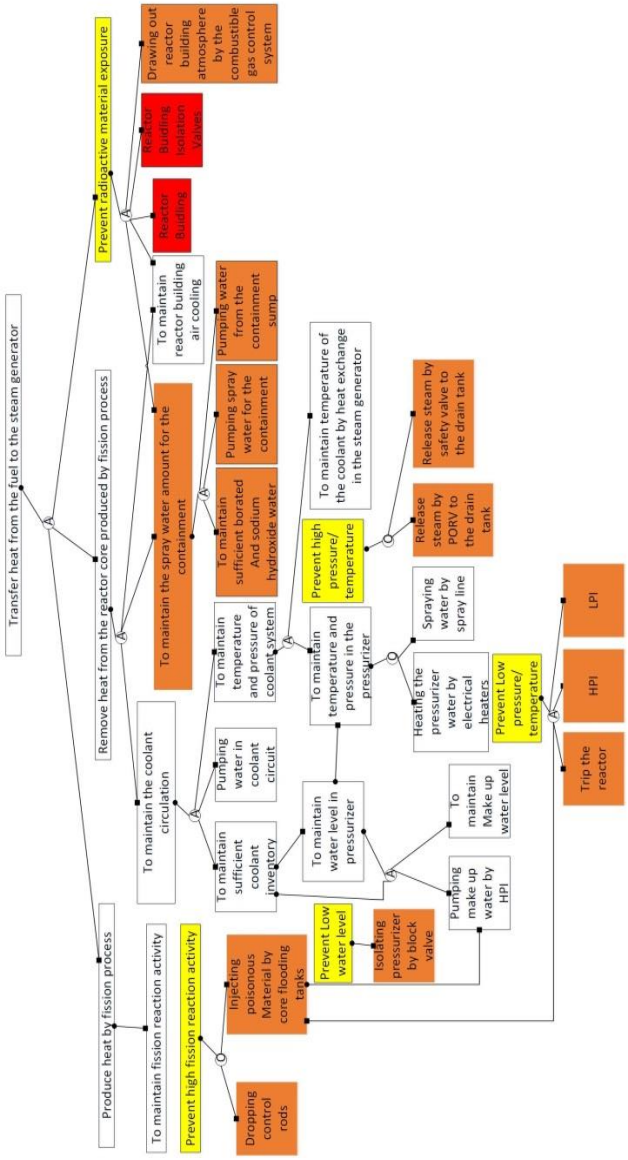

Fig.9 Decomposition of RCS objective

The storage function sto4 represents the storage of water in the core flood tank to keep mass balance (bal1) between its water storage in reactor. The storage function sto9_PZ represents the storage of water inside the pressurizer, and above the water is a bubble, or cushion of steam represented by the storage function sto10_Steam. The storage function sto6 is realized by drain tank. The water volume in the pressurizer can be compensated represented by a storage function sto8. It is connected directly to influence the level in the RCS. Additionally, another water source can be considered, which is the function of borated water storage tank (sto2).

The pressurizer and its associated control systems have the function of controlling the pressure of the whole primary system, so the energy flow structure efs1 is representing the energy balances in the whole primary system. Since MFM represents flow of mass and energy, pressure and its effects are expressed in the models via energy concepts. It is modelled separately in efs 5 by the energies storage in the pressurizer vapor phase (sto1) and liquid phase (sto13) and represents in this way thermal dynamic aspects. The functions of the pressurizer

represented in the mass flow structure mfs1 are also decomposed into vapor storage and liquid storage. The transport function tra9_Spray mediates the energy transport tra3 out of the pressurizer and the mass storage function sto9_PZ mediates the energy storage function sto13 (see [2] for an explanation of the mediation relation).

There are five production objectives of the primary loop. The energy storage function sto13 maintains the liquid phase pressure in the pressurizer (tar1) by actuating the heat transport function tra27 to maintain control objective 1. The energy storage function sto13 maintains the steam pressure in the pressurizer (tar2) by actuating the tra3 to maintain control objective 2. The mass storage function sto9_PZ maintains the water level in the pressurizer (tar3). The mass transport function tra5 maintains the coolant inventory (tar5). The mass storage function sto8 maintains the make-up tank level by actuating the tra8 to maintain control objective 3.

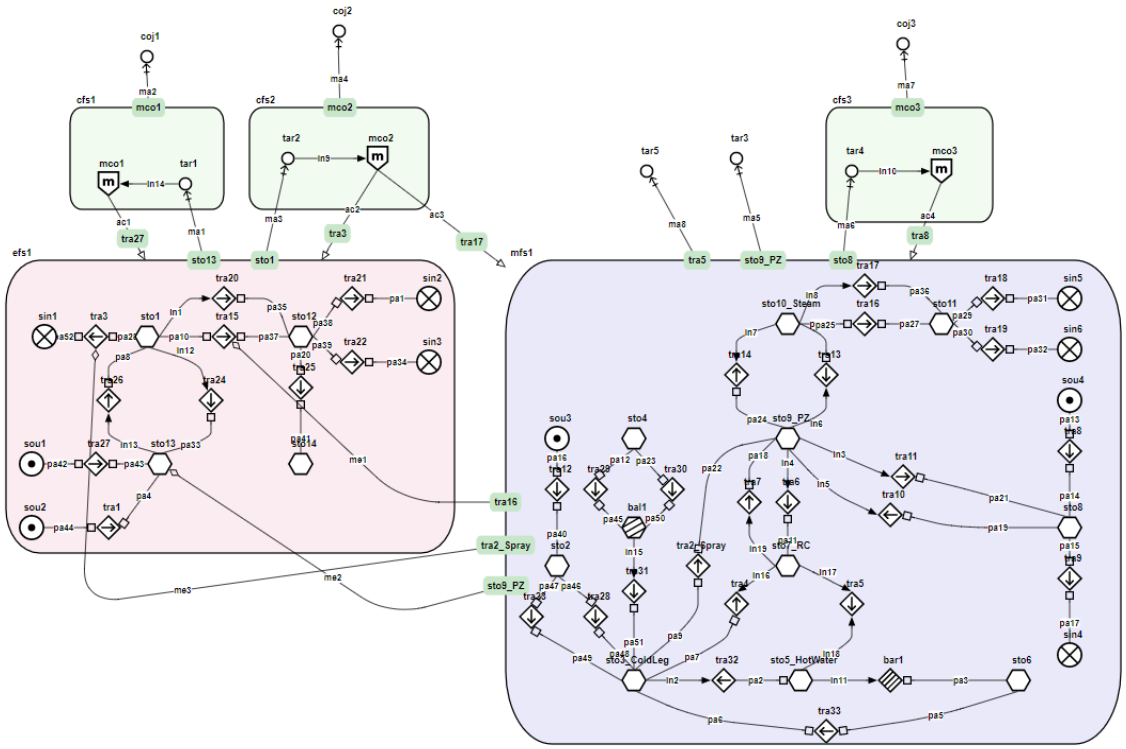

Fig.10 MFM model of RCS under normal operation

5.2 IPL analysis

As the approach described, the IPL analysis has to be evaluated after the safeguards are identified once the scenario and the initiating cause were selected.

The initiating cause event of the accident is the malfunction of the steam generators emergency feed water system (EFW, block valves left shut). Instead of looking at the initiating cause, in order to see the effect of the initiating cause effect on RCS, let's move one step forward to search for the direct effect on RCS caused by the initiating cause, the heat transport out of primary coolant is low, which means that the reactor coolant pressure increases. Then the arising temperature in the primary coolant caused the reactor to shut down and the PORV on top of the pressurizer was opened as design. However, PORV is stuck open, which means that the state of transport function tra 17 is high. Let's investigate the consequence. The consequence is shown in Fig 11.

It indicates that much of the primary coolant was drained away (sto11: high). Meanwhile, the water

and steam escape from pressurizer (sto10_steam: low& sto9_PZ: low). The pressure of pressurizer is low (sto 13: low). The water coolant is loss (tra5: low).

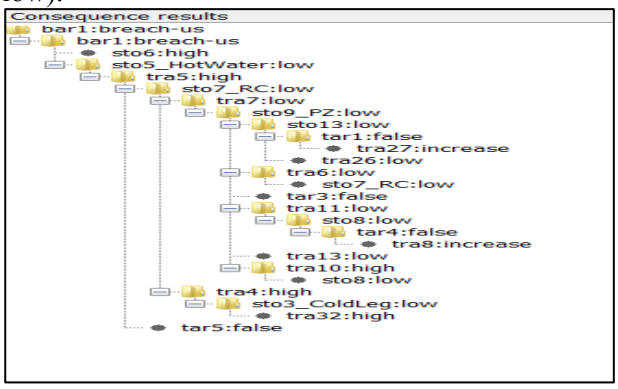

Fig. 11 Plausible consequences and counteractions of PROV stuck open

Responding to it, it is to increase make up (tra 8: increase). Because the pressure of pressurizer is low (sto13: low), the counteraction is to actuate transport function tra 27 to increase, which means that high-pressure injection pumps automatically pushed replacement water into the reactor to increase the pressure. Those two counteractions are the independent protection layer to prevent the severe accident leading to the reactor core meltdown consequently.

6 Discussion

In the case study, the existing independent protection layers were identified. However, recommended barriers to avoid the "PROV struck open" and "manual valve close condition" can also be analyzed.

PROV struck open (tra 17 is high) can be avoided by extra layer of protection, that is, measure the differential pressure across the PROV, in case of low differential pressure for a period, close the block valve.

Manual valve close condition can be avoided by implementing another barrier, that is, all the manual valves in feed water line to steam generator with closed feedback connected to control system with an alarm.

The case study presented identified the barriers for the LOCA scenario of PROV stuck open. However, the MFM model presented in Fig.10 can also be used to find out consequence and possible counteractions if there is a leak (bar 1 is breach-us) from the hot water to the steam generator.

7 Conclusions

The paper investigates application of functional modeling for independent protection layer analysis of risk assessment in complex industrial plant with special reference to nuclear power production. It is concluded that the production objectives and protection objectives decomposition of the process is very important to facilitate the acquisition of the relevant process knowledge from the engineering documents. The means-end decomposition of objectives is an important step in the development of an MFM model. It is also demonstrated that MFM can be used to reason about process, control and barrier. However, how the threats (ends) and safety functions (means) are linked in the MFM model requires more work. A case study using functional modeling for independent protection layer analysis is demonstrated in a PWR LOCA accident scenario.

The paper investigates applications of functional modeling for independent protection layer analysis of risk assessment with special reference to nuclear power production. However, the challenges and the results presented are common for other industries involving risk, such as hydrocarbon production and chemical processes.

Acknowledgement

The work presented has been supported by Danish Hydrocarbon Research and Technology Centre (DHRTC) and ELDOR Technology as part of the Water Management Project.

References

[1] American Institute of Chemical Engineers, Layers of protection analysis—simplified process risk assessment, Center for Chemical Process Safety, New York, 2001.

[2] M. Lind, “An Introduction to Multilevel Flow Modeling,” Nuclear Safety and Simulation, Vol.2, No.1, pp. 22–32, 2011.
[3] M. Lind, and X. Zhang, “Applying Functional Modeling for Accident Management of Nuclear Power Plant,” Nuclear Safety and Simulation Vol.5, No. 3, pp.186–196, 2014.
[4] M. Lind, “Modeling Safety Barriers and Defense in Depth with Mulitlevel Flow Modeling,” Proceedings of First International Symposium on Socially and Technically Symbiotic Systems, Okayama, Japan, Aug. 29~31, 2012.
[5] O. Svenson, “The Accident Evolution and Barrier Function (AEB) Model Applied to Incident Analysis in the Processing Industries,” Risk Analysis, Vol. 11, No. 3, pp. 499–507, 1991.
[6] J. Reason, Managing the Risks of Organizational Accidents, Ashgate, 1997.
[7] American Institute of Chemical Engineers, Guidelines for Safe Automation of Chemical Processes, Center for Chemical Process Safety, New York, 1993.
[8] W. Haddon Jr, "On the escape of tigers: an ecologic note," American Journal of Public Health and the Nations Health, Vol.60, No.12, pp. 2229-2234, 1970.
[9] W. G. Johnson, MORT safety assurance systems, Marcel Dekker Inc, 1980.
[10] J.R. Taylor, C.G. Petersen, J. Kampmann, L. Schepper, E.K. Kragh, R.S. Selig, P. Becher, and K.E. Petersen , Kvantitative og kvalitative kriterier for risikoaccept (Quantitative and qualitative criteria for risk acceptance, in Danish), Miljøprojekt nr. 112, ISBN 87-503-7938-0, Danish Environmental Protection Agency, Copenhagen, 1989.
[11] N.J. Duijm, and M. Frank, "Safety-barrier diagrams as a tool for modelling safety of hydrogen applications," International Journal of Hydrogen Energy, Vol. 34, No.14, pp. 5862-5868, 2009.
[12] N. J. Duijm, "Safety-barrier diagrams as a safety management tool," Reliability Engineering & System Safety, Vol. 94, No.2, pp. 332-341, 2009.
[13] E. Hollnagel. Barriers and Accident Prevention. Ashgate Publishing Limited, Hampshire UK, 2004.
[14] American Institute of Chemical Engineers, Inherently Safer Chemical Processes: A Life Cycle Approach: Second Edition, Center for Chemical Process Safety, New York, 1993.
[15] Nuclear Safety Analysis Center, Analysis of Three Mile Island - Unit 2 Accident, NSAC-80-1. NSAC-1 Revised March 1980.
[16] A. E. Summers, “Introduction to Layers of Protection Analysis,” Journal of Hazardous Materials, Vol. 104, No.1-3, pp. 163–168, 2003.
[17] A.M. Dowell, and T. R. Williams. “Layer of Protection Analysis: Generating Scenarios Automatically from HAZOP Data,” Process Safety Progress, Vol. 24, No.1, pp.38–44, 2005.
[18] V. D. Dianous, and C. Fiévez, "ARAMIS project: A more explicit demonstration of risk control through the use of bow–tie diagrams and the evaluation of safety barrier performance," Journal of Hazardous Materials, Vol. 130, No.3, pp. 220-233, 2006.
[19] A. S. Markowski, and A. Kotynia, "“Bow-tie” model in layer of protection analysis," Process Safety and Environmental Protection, Vol. 89, No.4 pp.205-213, 2011.
[20] Guidelines for Initiating Events and Independent Protection Layers in Layer of Protection Analysis, Wiley, 2015.
[21] R. J. Stack, "Evaluating non-independent protection layers," Process Safety Progress, Vol. 28, No.4, pp.317-324, 2009.
[22] A. M. Dowell, “Is It Really an Independent Protection Layer?” Process Safety Progress, Vol. 30, No.2, pp. 126–131, 2011.
[23] M. Lind, Knowledge Acquisition and Strategies for Multilevel Flow Modelling. Proceedings of the ISOFIC2017, Geyongju, Korea, November 26-30, 2017.
[24] X. Zhang, L. Morten, "Multilevel Flow Modelling: A Tutorial", Halden Report HWR-1192, Institute for Energy Technology, August 2017.
[25] X.Hu, Z.Wu, M. Lind, J.Wu , X.Zhang , J.Frutiger, & G.Sin. “Using MFM methodology to generate and define major accident scenarios for quantitative risk assessment studies,” In A. Espuña, M. Graells, & L. Puigjaner (Eds.), Proceedings of the 27th European Symposium on Computer Aided Process Engineering (ESCAPE 27) (1 ed., Vol. 40). Elsevier Science, Barcelona, Spain, Oct. 1~5, 2017.
[26] X. Zhang, Assessing Operational Situations, Ph.D Dissertation, Department of Electrical Engineering, Technical University of Denmark, 2015.
[27] X. Zhang, M. Lind, “Reasoning about Cause-effect through Control Functions in MFM,” Proceedings of the ISOFIC2017, Gyeongju, Korea, Nov. 26~30, 2017.
[28] J.Wu, M.Lind, X.Zhang, S. B.Jørgensen & G. Sin, “Validation of a functional model for integration of safety into process system design. In 25th European Symposium on Computer Aided Process Engineering (pp. 293-298),” Elsevier Science, 2015.
[29] R.Mitchell. Three Mile Island: A report to the commissioners and to the public. No. NUREG/CR-1250 (Vol. 1). Nuclear Regulatory Commission, Washington, DC (USA), 1979.
[30] D. J. Hanson, et al. Accident management information needs. No. NUREG/CR-5513-Vol. 2; EGG--2592-Vol. 2. Nuclear Regulatory Commission, Washington, DC (USA). Div. of Systems Research; EG and G Idaho, Inc., Idaho Falls, ID (USA), 1990.