CHEMICAL ENGINEERING TRANSACTIONS
VOL. 86, 2021
A publication of AIDIC
The Italian Association of Chemical Engineering
Online at www.cetjournal.it
Guest Editors: Sauro Pierucci, Jiří Jaromír Klemeš

ISBN 978-88-95608-84-6; **ISSN** 2283-9216
DOI: 10.3303/CET2186162

Identifying Safety Objectives and Functions for Emergency Shutdown in the Design Phase by Using Functional Modelling

Jing Wu*, Mengchu Song, Xinxin Zhang, Morten Lind

Department of Electrical Engineering, Technical University of Denmark, 2800, Kgs. Lyngby, Denmark
jinwu@elektro.dtu.dk

This paper proposes a functional modelling method, called Multilevel Flow Modelling (MFM) for identification of safety objectives and functions of emergency shutdown (ESD) system in the design phase for emergency shutdown safely. Firstly, the required information for designing safety objectives and functions for an emergency shutdown is analysed. The information includes process topology, the initial state of the process, the shutdown objectives, and other constraints, such as design and operational limits of unit operations and hazardous and environmental constraints. Secondly, a procedure is proposed based on the required information by using MFM. The procedure incorporates steps: 1) The MFM model of the process in normal operations are built by following modelling procedures, 2) Initiate states are defined and changing conditions are identified of the process when it shuts down unplanned by using the objective-function tree in the MFM modelling, 3) The goals of the shutdown operation are defined, 4) With the consideration of the shutdown operating goals and changing conditions, the first safety function during shutdown process are identified by using MFM causal reasoning, 5) By using MFM consequence reasoning based on the first identified safety function represented in the MFM model, the rest of the safety functions are identified, and the emergency shutdown procedures are generated. This procedure is demonstrated by designing safety functions in an emergency shut down of a seawater deaeration process in a seawater injection system. The results show that the produced emergency shut down procedure based on the proposed method is feasible and that it can be validated against the real operating procedure.

1. Introduction

In the area of process operations, at the plant level, the interest in the process verification and synthesis of operating procedures has been a research hotspot in decades (Grossmann & Westerberg, 2000). However, before the defined operating procedure is available, the safety objectives and functions are created intentionally with the consideration of safety in the overall process system (Mannan et al., 2015). Those safety objectives and functions can be identified based on the hazard identification process (American Institute of Chemical Engineers, 2010) by following a hazard analysis procedure.

In previous studies (Wu et al., 2020), a procedure was proposed for validating safety objectives and functions in normal operations. However, if the process shuts down as unplanned, so-called emergency shutdown (Nolan, 2011), the previous studies do not solve how the safety objectives and functions of ESD system, as a part of Safety Instrumented Systems (SIS), can be identified in the design phase of the process system (Basu, 2016). Consequently, the relevant ESD system (Sutton, 2014) can be designed afterwards to allow operators during operations to take the equipment out of service safely by following emergency shutdown procedures (Batres, 2013). Identification of safety objectives and functions of ESD system is important and critical, so that relevant accidents such as Chernobyl (International Atomic Energy Agency, 1992) can be prevented. It can make the conducted operating procedure sense both in improving operator's situation awareness and verification of safety design purposes. In this study, this challenge was addressed.

In the literature, the conventional hazard identification method (Crawley, 2020) such as HAZOP, is used to identify and verify safety objectives and functions of ESD system. However, HAZOP is not suitable for the visualization of the analysis process and results are likely inconsistent (Pasman & Rogers, 2016). Therefore,

Paper Received: 2 November 2020; Revised: 6 February 2021; Accepted: 12 April 2021
Please cite this article as: Wu J., Song M., Zhang X., Lind M., 2021, Identifying Safety Objectives and Functions for Emergency Shutdown in the Design Phase by Using Functional Modelling, Chemical Engineering Transactions, 86, 967-972 DOI:10.3303/CET2186162

in this aspect, the functional modelling method was recently proposed to cope with the limitations. The support of syntax and semantics of functional modelling method (Sierla et al., 2012) plays a key role in describing the propagation of possible hazards through the system for identifying safety objectives and functions of ESD system, and especially, across the boundaries of subsystems.
This paper focuses on the development of an approach to support identification of safety objectives and functions of ESD system in the design phase for emergency shutdown, with particular reference to the oil and gas industry. With respect to conventional approaches adopted in this field, a method using a functional modelling method, MFM, is hereby proposed. This is critical to overcoming limitations in standard and technical approaches, considering the information needed to design the ESD system's safety objectives and functions for an emergency shutdown, as discussed in Section 2. "The method is presented in Section 3 and in Section 4 the design of safety functions of the ESD system of a seawater deaeration process in a seawater injection system is demonstrated. Results and discussions are presented in Section 5. Section 6 reports conclusions and indications for future work.

2. Identifying safety objectives and functions in the design phase: open issues

This section refers to the main safety design requirements and references to open methods and issues to be addressed with the information necessary for the design of safety objectives and ESD system functions. Standard IEC 61511/ISA 84 requires that any industrial process should have a separated and well-designed SIS for controlling the risk associated with processing functions in a system as a whole to a tolerated safety integrity level. In addition, physical protection devices, such as relief valves, can further reduce the risk. ESD system is part of SIS for safety purpose and ESD system is active when operators activate it manually to protect the plant, environment, or people. Standard IEC 61511/ISA 84 is the only standard that outlines the practices in the design of SIS. In early design phase, identification of safety objectives and functions of ESD system is conventionally supported by hazard identification process, as suggested in the standard. However, conventional methods do not fully consider the required information for designing safety objectives and functions of ESD system (Batres, 2013).The following information is required by designers: a. the topology of the plant; b. the initial state of the plant; c. a description of the goals; d. a description of control element of the ESD system; e. constraints for unit operations; f. reaction constraints; g. production requirements (conditions); h. hazardous constraints; i. mechanical constraints; j. corrosion and erosion constraints.
In conclusion, to visually and consistently identify safety objectives and functions of an ESD system in the design phase for improving operator's situation awareness and verification of safety design purposes, it is necessary to use functional modelling, supported by artificial intelligence technology, and fully consider all the required information for designing safety objectives and functions of ESD system for emergency shutdown, as shown in the present work.

3. Methodology

The use of the MFM methodology to qualitatively simulate the process system, generate, and define initialization states and changing conditions when identifying safety objectives and functions of the ESD system can be performed following 5 steps (Figure 1).

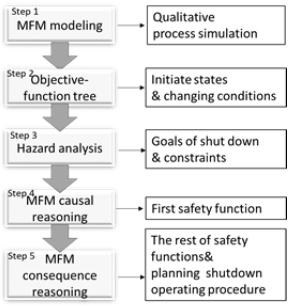

Figure 1: Flowchart of the methodology.

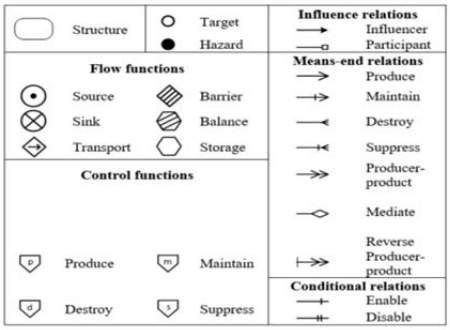

Figure 2: The basic MFM symbols.

The first step (Step 1 in Figure 1) is aimed at using MFM to simulate the process system by functional decomposition using symbols (Figure 2), by following modeling guideline, which analyzes system's objectives, functions (objective-function tree), material and energy streams (function-stream diagram), and structural topology at selected abstraction levels. Readers can find more information about semantics and

syntax of MFM in references (Lind, 2011). The simulation is performed by using an open web-based modeling tool: Kairos MFM Editor (egolf.azurewebsites.net/Home). Next, initial states and changing conditions (Step 2 in Figure 1) are identified of the process when it shuts down unplanned by using the produced objective-function tree during the MFM modelling process in Step 1. After the identification of the initial states and changing conditions, the analysis of hazards in relation to the process, environment, and people relevant to the shutdown process is analyzed so that the shutdown objectives and restrictions are identified (Step 3 in Figure 1). Step 4 (see Figure 1) uses the MFM causal reasoning capability to identify the first safety function with the consideration of operating goals and changing conditions identified in Step 2 and 3. The causal reasoning is initiated by selecting an operating objective or changing conditions (a particular function) corresponding with the shutdown process and set its deviation state such as high-high or low-low as the trigger. Then, from the trigger, the MFM reasoning module (Kairos workbench) can perform the diagnosis on the MFM model by using its casual reasoning engine. The first safety function is selected, which is located at the upmost upstream in the process boundary. Finally, Step 5 (See Figure 1) carries out the MFM consequence reasoning based on the first identified safety function in Step 4, the second safety function is identified. The consequence reasoning is initiated by selecting the function that triggers the shutdown and sets its low-low or high-high deviation state and the second safety function is detected in the MFM model for the first downstream at the process boundary. Then, an isolation area is formed. Inside the isolation area, the remaining safety functions are located based on the objective-function tree, identified in Step 1. Consequently, the planning of the shutdown operating procedure is determined.

4. Application to the water injection systems

4.1 Description of the seawater deaeration process

The seawater deaeration process in a seawater injection system in offshore platforms is used as a case study. Here, the booster pump and injection pump are also included in the process flow diagram (Figure 3). The deaeration tower removes dissolved oxygen from the sea water and consists of a 3-stage packed bed mass transfer column, operating under vacuum. Vacuum in the deaerator tower V-101 is provided from the vacuum pump package, A-102, which consists of two vacuum pumps (2 x 100%), P-106 and P-107, two seal water separators, T-106 and T-107, and four ejectors X-101/102/103/104. Oxygen scavenger is added when required to lower the remaining dissolved oxygen level even further. Deaerated water is collected at the bottom of the tower and flows to the suction of the water injection booster pumps (2 x 100%). The water injection booster pumps feed the injection pumps, which raise the water pressure sufficiently for injection into the reservoir.

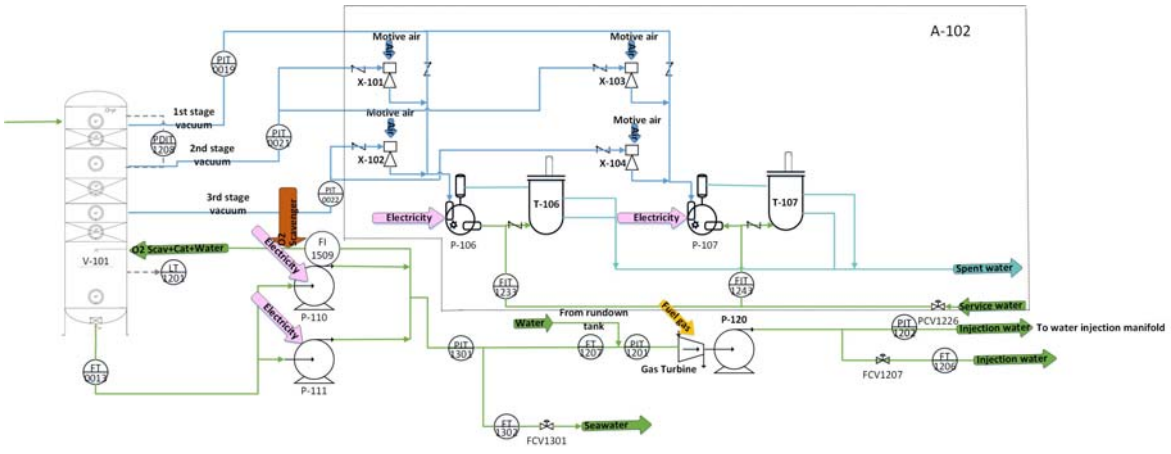

Figure 3: Process flow diagram of the seawater deaeration process with booster and injection pump.

4.2 Description of the MFM model

At the early design phase, only Process Flow Diagrams (PFD) are available, and they represent plant subsystems and their interconnections by material and energy streams. The plants are material and energy processing systems, i.e., the primary goals and objectives of plant operation can be expressed by the streams and their properties. The subsystems connecting the streams can accordingly be the means provided by the plant designer for the realization of the stream interactions required for achieving the plant purpose. The functions of these subsystems can accordingly be expressed by their intended effect on the streams.

Therefore, by following the MFM procedure, the first deliverable is a function-stream diagram, which outlines the major steps of the process flow. The second is an objective-function tree that highlights relations between process objectives and functions needed for their fulfillment. The function-stream diagram and the objective-function tree of the seawater deaeration process are shown in Figures 4 and 5.

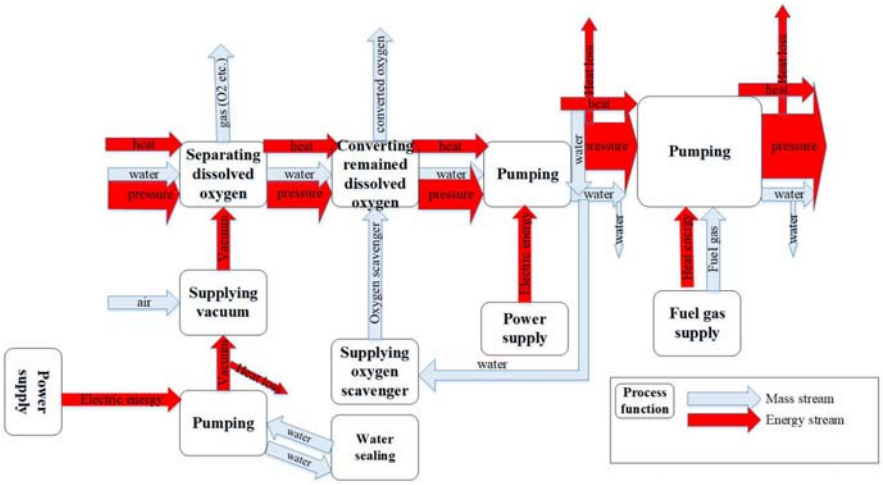

Figure 4: Function-stream diagram of the seawater deaeration process with booster and injection pump.

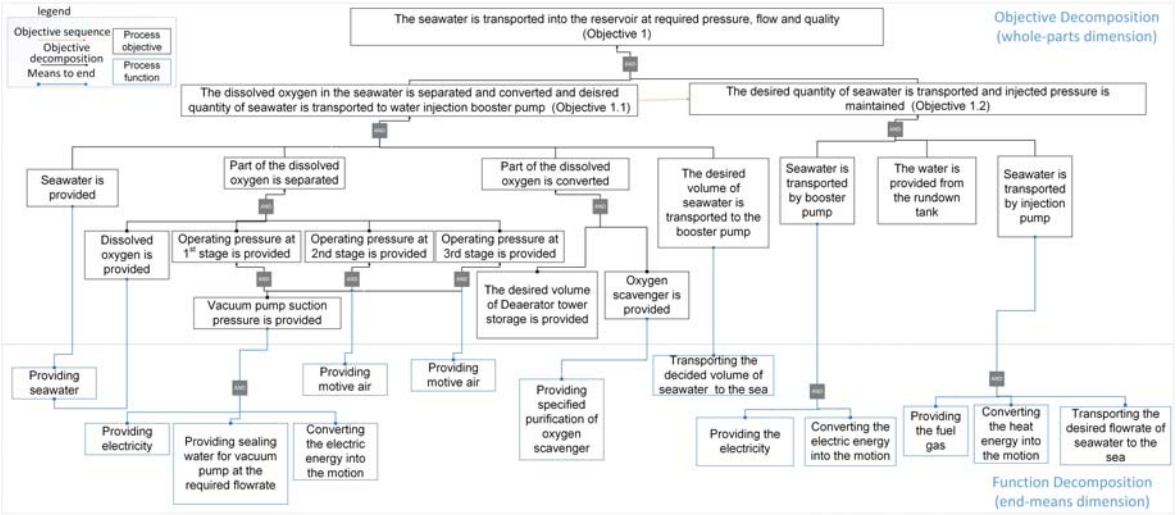

Figure 5: Objective-function tree of the seawater deaeration process with booster and injection pump.

The resulting functional representations of the process units are, then, interconnected and linked to process objectives, according to information provided in the function-stream-diagram and objective-function-tree. Further information about the procedure is found in the work of Lind (2017). The normal operation control of the process is not the focus of the study; therefore, the information (control) streams, control objectives, and functions are not included. The resulting functional model is shown in Figure 6.

4.3 Initial states and changing conditions for an emergency shutdown

Initial states and changing conditions (Step 2 in Figure 1) are identified for the seawater deaeration process when it shuts down unplanned by using the produced objective-function tree (Figure 5) during the MFM modelling process in Step 1. The initial states and changing conditions could be the failures of relevant objectives and functions analyzed in the objective-function tree based on the monitoring process parameters. Therefore, for the deaeration system itself, the initial states and changing conditions can be the following: low-low level of the deaerator tower storage; low-low flowrate of sealing water for vacuum pump. Here, the low-low level of the deaerator tower storage is selected as the initial state and changing condition for identifying safety objectives and functions for the leading emergency shutdown.

4.4 The goals and constraints of the emergency shutdown

Step 3 (in Figure 1) examines the goals and constraints of the emergency shutdown based on the hazard analysis. As can be seen in the objective-function tree, if the objective of the desired volume of seawater tower storage is not met (low-low level), then the objective 1.1 is not achieved. It means that the dissolved oxygen would not be converted, and the quality of the seawater would not reach the requirement. The hazard for the process would be the corrosivity of the seawater, associated with the presence of oxygen, which can corrode the piping and equipment. Also, the desired seawater cannot be transported to the booster pumps. This can damage the pumps. Therefore, the goal of the emergency shutdown does not allow any water to leave the deaerator that has not been deaerated. The constraint of the emergency shutdown is to protect the injection booster pumps.

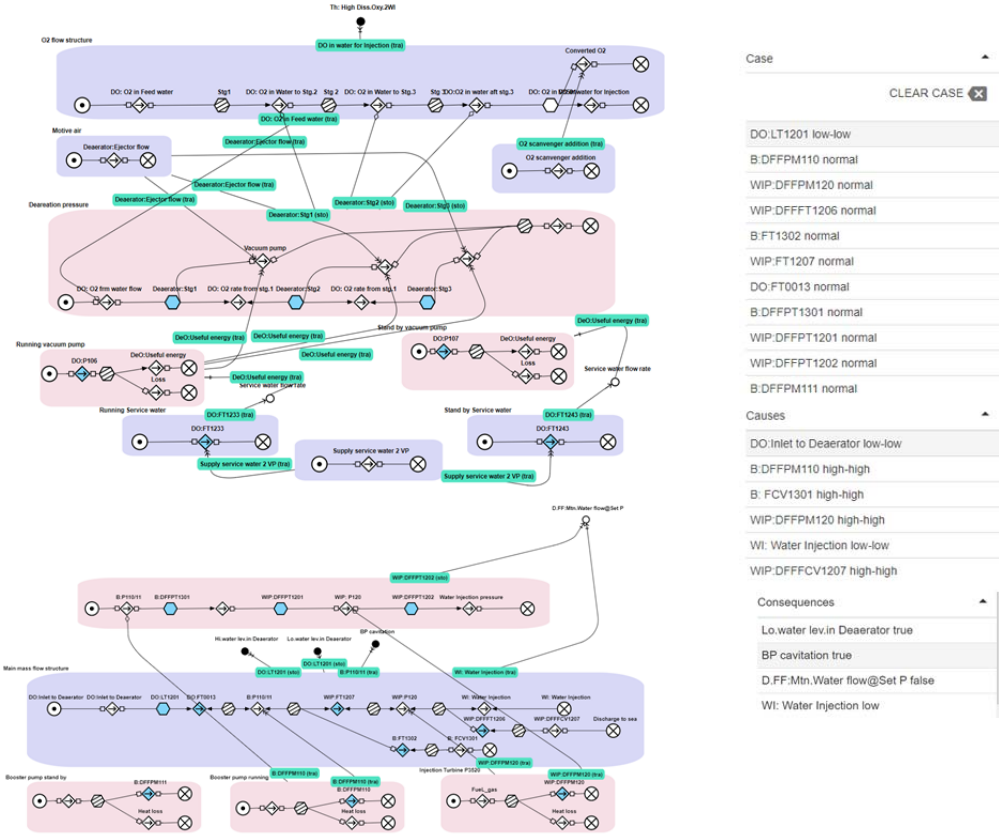

Figure 6: MFM model of the deaeration process and causes and consequences of the low-low level of the deaerator tower storage.

4.5 Identifying the first safety function

Based on causal reasoning with the low-low trigger of the storage function labeled DO: LT1201 (the low-low level of deaerator tower storage), the causes are listed in the upper right corner in Figure 6. Among the causes, the first function, located at the upmost upstream in the process boundary, deviates from the normal state is the inlet stream (low-low state) to the deaerator. Therefore, the first safety function should be a shutdown function to shut the water supply to the deaerator.

4.6 Identifying the rest of safety functions

The MFM consequence reasoning, based on the first identified safety function, the rest of the safety functions are identified here. The consequences are shown in Figure 6. The low water level in the deaerator causes the booster pump to cavitate. Therefore, the second safety function is to stop and isolate the booster pumps. Until now, the deaerator is isolated therefore, according to the objective-function tree (Figure 5), the functions for achieving objective 1.1 should be deactivated: the vacuum pump should be isolated and sealing water for the vacuum pump should be stopped. Then, the objective of the providing vacuum would fail, any residual vacuum in the deaeration tower should be relieved and the seawater in the tower sump should be drained.

5. Results and discussions

Based on the identified safety objectives and functions for the emergency shutdown, the emergency shut down procedure is as follows:

- Shut the water supply to the deaerator;
- Stop and isolate the booster pumps;
- Isolate the vacuum pump;
- Stop the sealing water for the vacuum pump;
- Relieve any residual vacuum in the deaeration tower;
- Drain the tower sump.

The identified safety objectives and functions can be used as an input for the design of the ESD system, so the safety sensors, control logics, and control elements can be designed. The produced emergency shut down procedure can be extended and detailed with the actions upon the specified control elements after the ESD system is designed.

6. Conclusions

The aim of the present work was to develop a methodology for identification of safety objectives and functions for emergency shutdown in the design phase. With respect to the conventional approaches adopted for this field, the present work illustrates how operator's situation awareness can be improved and safety design purposes can be verified by using functional modelling supported by artificial intelligence technology with full consideration of all the required information for designing safety objectives and functions of ESD system for emergency shutdown. The novelty introduced by the method is related to the planning of the emergency shutdown procedure, which allows the process verification and synthesis of operating procedures. Thus, important information may be derived to support the operators' counteractions during the shutdown process. The example is demonstrated on an oil and gas process. However, the method is suitable for extension in any process system.

Acknowledgments

The authors would like to thank The Danish Hydrocarbon Research and Technology Centre (DHRTC).

References

American Institute of Chemical Engineers, 2010, A Practical Approach to Hazard Identification for Operations and Maintenance Workers, John Wiley and Sons, New York, USA.

Basu, S., 2016, Plant Hazard Analysis and Safety Instrumentation Systems, Academic Press, Cambridge, USA.

Batres, R., 2013, Simulation-based planning of shutdown operations, In Procedia Computer Science, 22, 1294–1302.

Crawley, F., 2020, A Guide to Hazard Identification Methods, Elsevier, Amsterdam, Netherlands.

Grossmann, I. E., & Westerberg, A. W., 2000, Research challenges in Process Systems Engineering, AIChE Journal, 46(9), 1700–1703.

International Nuclear Safety Advisory Group, 1992, The Chernobyl accident : updating of INSAG-1 ; a report by the International Nuclear Safety Advisory Group, International Atomic Energy Agency, Vienna, Austria.

Lind, M., 2011, An introduction to multilevel flow modelling, Nuclear Safety and Simulation, 2(1), 22-32.

Lind, M., 2017, Knowledge Acquisition and Strategies for Multilevel Flow Modelling, International Symposium on Future Instrumentation and Control for Nuclear Power Plants, Gyeongju, Korea.

Mannan, M. S., Sachdeva, S., Chen, H., Reyes-Valdes, O., Liu, Y., & Laboureur, D. M., 2015, Trends and challenges in process safety, AIChE Journal, 61(11), 3558–3569.

Nolan, D. P., 2011, 11 - Emergency Shutdown, In Handbook of Fire and Explosion Protection Engineering Principles, 119–126, William Andrew, New York, USA.

Pasman, H., & Rogers, W., 2016, How can we improve HAZOP, our old work horse, and do more with its results? An overview of recent developments, Chemical Engineering Transactions, 48, 829-834.

Sierla, S., Tumer, I., Papakonstantinou, N., Koskinen, K., & Jensen, D., 2012, Early integration of safety to the mechatronic system design process by the functional failure identification and propagation framework, Mechatronics, 22(2), 137–151.

Sutton, I., 2014, Plant Design and Operations, Gulf Professional Publishing, Texas, USA.

Wu, J., Song, M., Zhang, X., & Lind, M., 2020, A Procedure for Modelling and Verification of Safety Objectives and Functions, the 30th European Safety and Reliability Conference and the 15th Probabilistic Safety Assessment and Management Conference, Venice, Italy.