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
©2023 ESREL2023 Organizers. *Published by* Research Publishing, Singapore.
doi: 10.3850/978-981-18-8071-1_P132-cd

Challenges in Functional Modelling for Safety and Risk Analysis

Jing Wu

Department of Electrical and Photonics Engineering, Technical University of Denmark, 2800, Lyngby, Denmark.
E-mail: jinwu@dtu.dk

Xinxin Zhang

Department of Electrical and Photonics Engineering, Technical University of Denmark, 2800, Lyngby, Denmark.
E-mail: xinz@dtu.dk

Mengchu Song

Department of Electrical and Photonics Engineering, Technical University of Denmark, 2800, Lyngby, Denmark.
E-mail: menso@dtu.dk

Morten Lind

Department of Electrical and Photonics Engineering, Technical University of Denmark, 2800, Lyngby, Denmark.
E-mail: mli@elektro.dtu.dk

Safety and risk analysis in a system's life cycle is a core activity to ensure a sound safety basis for the system. It is a type of problem-solving process. The functional value of a solution is indispensable for the understanding of its being a solution. It is also important for defining failures and their possible hazardous consequences. The functional modelling is motivated for development and has also been applied to safety and risk analysis in different industrial domains. However, the research on functional modelling for safety and risk analysis is not that widespread. The purpose of this paper is to draw attention to this area for researchers and point out the challenges in functional modelling for safety and risk analysis. First, it explains why functional modelling is needed for safety and risk analysis, including their challenges. Then, a literature review is conducted for each challenge, and our proposition is summarized. It is hoped that the paper can serve its purpose of making its contribution to opening up more potential research by using functional modelling for safety and risk analysis.

Keywords: Safety and risk analysis, functional modelling, artificial intelligence, problem-solving, social-technical systems, decision making support.

1. Introduction

System safety is the application of engineering and management principles, criteria, and techniques to achieve acceptable risk within the constraints of operational effectiveness and suitability, time, and cost throughout all phases of the system life-cycle. Duncker & Lees (1945) argued that the functional value of a solution is indispensable for the understanding of its being a solution. It is also important for defining failures and their possible hazardous consequences. The subordinated, more specialized characteristics and properties of a solution embody this principle and apply it to the particular circumstances of the situation. Therefore, functional modelling or analysis is motivated for development since the 1950s and has also been applied to safety and risk analysis in the different industrial domains. However, the research on functional modelling for safety and risk analysis is not that widespread. The purpose of this paper is to draw attention to this area for researchers and point out the challenges in functional modelling for safety and risk analysis. Firstly, the paper explains why functional modelling or analysis is needed for safety and risk analysis: the deficiencies of existing methods and the advantages of using functional modelling or analysis. Secondly, what are the challenges of using functional modelling or analysis, and how these challenges could be approached? It is hoped that the paper can serve its purpose of making its contribution to opening up more potential research by using functional modelling for safety and risk analysis.

2. Why Functional Modelling or Analysis for Safety and Risk Analysis

2.1. *The deficiencies of existing methods*

Safety and risk analysis methods can be divided into two categories: qualitative analysis and quantitative analysis. Risk assessment techniques can be found in IEC 31010: 2019. They are driven by analysis of different failure types: failures of events, functions, components, and parameters/operations.

Event-based methods include approaches such as Preliminary Process Hazard Analysis (PrHA), Fault Tree Analysis (FTA), Event Tree Analysis (ETA), What-if Analysis, and Checklist. However, full sets of events are hardly identified, and there are no structured approaches for analyzing the causes and consequences of the undesired events. They are mainly based on the experts' knowledge in a brainstorming way. If there are existing standards and practices that can be applied to generate situations or events, then these events can be used as inputs for brainstorming as well. Consequently, the analysis results are not systematic and often lack completeness. Bow-tie analysis is the combination of FTA and ETA, and the focus of bow-tie analysis is designing barriers to prevent the causes or mitigate the consequences. However, the barriers are identified for each identified undesired event, which means barriers are not identified completely. Layer of Protection Analysis (LOPA) is the analysis of a single cause-consequence pair as an accident scenario. It is also using an event tree approach. Therefore, in nature, it has the same limitation as bow-tie analysis. Event-based methods have another limitation is that due to it being event analysis, the risk level of different events is not the same. The safety and risk analysis based on event-based approaches may lead to non-distinguishable risk reduction in the end.

Failure of components analysis methods includes Failure Mode and Effects Analysis/Failure Mode and Effects Critical Analysis (FMEA/FMECA). These methods select a system or component and split it into subsystems or subcomponents, postulate a failure mode of the subsystem or subcomponent, list the effects of the failure, safeguards or controls, and recommended remedial actions are following. The limitations of the component-based approaches are if the failure modes are not identified by experts, then there are ignored associated risks that may threaten the systems' safety. In addition, the methods prioritize important failure modes, therefore, the less important failure modes may not be analyzed in detail. However, the judgment of importance is dependent on experts. For a large complex system, such a study may take a long time to complete.

The representative method of failure of parameters/operation is Hazard and Operability Study (HAZOP). The system is divided into "nodes", and "guide words" combined with "parameters" (called "deviation") are applied to examine possible causes and consequences for each deviation in each "node", to consider safeguards and recommendations for action. The main limitation of HAZOP is that it lacks a structured way to analyze system-level hazards and operability problems.

In addition, not all the above-mentioned methods can be used for different stages of a system's life cycle.

The analysis of failures of functions will be discussed in the next subsection.

2.2. *The advantages of using functional modelling or analysis*

In a system's life cycle, the system goes through the concept stage, development stage, realization stage, utilization stage, enhancement stage, and decommissioning stage ((Lee, Cameron, and Hassall 2019). In each stage, safety and risk analysis is of particular importance and requires an understanding of the system from a functional perspective. In the concept stage, the function-centered design approach is dominant(B Chandrasekaran, Goel, and Iwasaki 1993). The functional requirements, including safety functions, are abstract. In the development stage, a detailed design is available, and methods of operation have been decided upon. The functional requirements are decomposed into different levels of detail, more specific, and quantified. In the realization stage, during an initial operation or startup of the system, the functions of the system as a whole may require new features compared with a simple summary of the functions of parts. In addition, such interactions among the parts may vary during the change of the system in the utilization and enhancement stages. In the decommissioning stage, the tasks of decommissioning are to deactivate the designed functions. As can be seen, the functions are always in focus at any stage of the system's life cycle. It is natural to use functional modelling or analysis to perform safety and risk analysis during the system's life cycle. Since 2000, machine safety has been regulated from the perspective of function and reliability.

In addition, safety barriers are parts of the overall system. They can be physical and engineered systems or human actions based on specific procedures or administrative controls. A safety barrier directly implements a safety function (Sklet 2006). Failures of safety functions can significantly increase the system's risk. Safety barriers are also going through their own life cycle. Fig. 1 shows the relation between safety barriers, safety and risk analysis and risk mitigation (safety function). Both tasks can be supported by functional modelling or analysis.

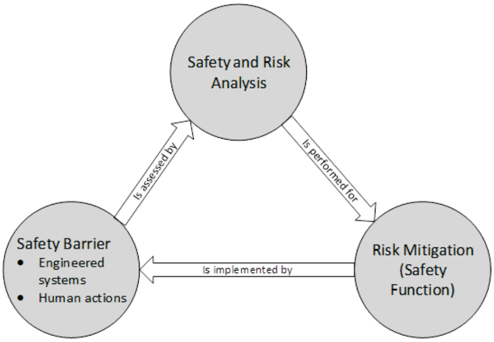

Fig. 1. The relation between safety barriers, safety and risk analysis and risk mitigation (safety function).

The advantages of using functional modelling or analysis for safety and risk analysis are:

(i) Functional modelling or analysis can be applied at all stages of the life cycle.

(ii) Functional modelling or analysis can be applied for complex systems.

(iii) Functional modelling or analysis can decompose systems in terms of systems' objectives and functions. The failure of functions can be mapped with the failures of systems' objectives, which means that their contribution to the risk level is clear.

However, there are challenges in functional modelling or analysis for safety and risk analysis.

3. Challenges in functional modelling or analysis for safety and risk analysis

Functional modelling or analysis is highly relevant for safety and risk analysis, especially for process engineering, since functional units here are well known. It should be very useful. However, why is research on functional modelling or analysis for safety and risk analysis not that widespread although this type of method is mentioned in literature reviews? (Aboutorab et al. 2021; Caiza and Sanz 2022; Cameron et al. 2017; Jørgensen, Lind, and Jensen 2019; Khan, Rathnayaka, and Ahmed 2015; Venkatasubramanian, Rengaswamy, and Kavuri 2003) for safety and risk analysis. There are several challenges when using functional modeling or analysis for safety and risk analysis.

Firstly, the functions of artifacts are inter-subjective (Searle, Willis, and others 1995). The dispositions or cause-effect relations between artifacts and their parts provide the possibility to realize certain functions, but the functions agreed upon in a domain (subjective) by the designers and users of the artifacts are therefore inter-subjective. Such consent provides a foundation for an ontology-based approach to functional modelling. However, there are discrepancies in such consent.

Secondly, the functions of individual artifacts (parts) are aggregated into a system (whole) to create new functions. Analysis of the functions of a system, therefore, requires principles for functional aggregation and decomposition (Pahl and Beitz 1988). In most cases, the realization of some functions is dependent on other functions or conditions. The relations between functions are important for causality analysis, i.e., if one component fails, how are other components or even the system level influenced as seen from a functional perspective? The principles for functional aggregation and decomposition in Pahl & Beitz (1988) are not sufficient. Because the term function is applied to the intended input/output relationship of a system whose purpose is to perform a task. An overall function, therefore, is often divided directly into subfunctions corresponding to subtasks. These task-specific functional aggregation and decomposition principles are not sufficient for analyzing safety functions.

Third, the safety functions in a broad sense, are any related functions that can prevent causes from hazardous situations occurring or mitigate consequences for hazardous situations. It requires an answer to another question: how a system can fail in a functional way (Imran Khan et al. 2014; Wang et al. 2021), and how do design safety functions accordingly? In order to apply functional modelling techniques to safety and risk analysis, the models must have the capability of acquiring knowledge about the hazards of the system and functionally representing them. This leads to another question, what are the hazards in terms of failures of the functions' realization? It is dependent on the views on functions (Balasubramanian Chandrasekaran 2005).

Fourth, there are different ways to represent functions. Natural language (Kitamura, Mizoguchi, and others 2003; Mohammad Modarres 1993) is one of them. The challenge is here that natural language may introduce ambiguity. The model that uses natural language may be extremely scaled up when modelling complex systems, even impossible. Artificial formal language (Minsky 1974) is another way. It is closely connected with theories of logic and semantics. If an artificial formal language with unclear meanings is used for human interface design, it may lead to misunderstanding. Consequently, it may cause wrong operations in action and accidents. Furthermore, model builders are required to follow a set of semantics rules to make a valid model. If models are not valid, it loses the accuracy of the representation. The model cannot be used for any applications.

In the next three subsections, literature reviews of works related to solving each challenge are presented, and our proposition is summarized.

3.1. *Functions are inter-subjective*

Within the area of knowledge acquisition methodologies, one research line is to refine the existing knowledge-level frameworks and emphasize their formalizations. The development and application of ontology technology open new ways of knowledge sharing and reuse (Gomez Perez and Benjamins 2009). The application of ontology technology to designing knowledge-based systems (Gulla 2008) has become a key topic in the field of artificial intelligence and is applied in process safety. For example, through ontological engineering, functional knowledge can be systematized and applied to engineering knowledge management (Kitamura and Mizoguchi 2004), and used in the design process. Domain ontologies for design are concerned with things to be designed and aim at the representation of the design targets themselves and/or temporal changes of their physical attributes. Kitamura et al. (2003) defined a function of a device as a teleological interpretation of its behavior under the intended goal. The behavior is disregarding the designer's intention and is therefore objective. The process of functional decomposition is the process where the consensus of functions is reached by designers and users of the artefact. However, some researchers (Vermaas 2009) think technical functions should be seen as subjective relations between artifacts and their technical context including the mental states of agents. Functions are intersubjective because they are social facts (Searle, Willis, and others 1995). The consensus provides a foundation for an ontology-based approach to functional modelling.

The discussion on the nature of functions is also relevant to how to validate functions (Wu et al. 2015). Since the functions are inter-subjective, they should be validated against two aspects of a means-end relation: the casual aspect and the teleological aspect (Lind 2014). The causal aspect relates to the designer's experience that the means used can produce or prevent the end or design goal. The teleological aspect implies that the means have been selected to achieve the goals. When dealing with functional models' truth therefore cannot be established or tested alone by physical experiments (Nielsen et al. 2020). To test the validity of objectives and purposes we need to test these against the consensus of a group of experts (e.g., designers and operators). Based on this conclusion, a procedure for the validation of a functional model (Wu et al. 2014) was proposed. Since the validation implies the validation of the means-end relation, it leads to another discussion of how means-end structures are derived, as a way of aggregation and decomposition of functions. This will be discussed in the next subsection.

3.2. *Knowledge acquisition of hazards and safety functions*

As discussed earlier, safety functions are the means to avoid hazards (the end). The safety functions can be manifested only if the hazards are known and specific. It is therefore necessary to acquire hazard-related knowledge of the means and ends as an input for the functional modelling in applications for safety and risk analysis. This means that this knowledge should not only include what the hazards are but also include how the hazards occur, i.e., failures of safety functions. The safety functions are here meant in a broad sense since any related functions can prevent causes from hazardous situations occurring or mitigate consequences for hazardous situations. A safety function is a technical or procedural action, and not an object or a physical system. It is an action to be achieved in order to avoid or prevent an event or to control or limit the occurrence of the event. This action will be realized thanks to a safety barrier.

So, what are the hazards in terms of failures of the functions' realization? The hazards could be process hazards or the (derived) hazards connected with the failure of safety functions. Modarres & Cheon (1999) asserted that in the function-centered approach to risk analysis, an event can be viewed as the consequence or as the cause of (i) using a wrong function, (ii) using a correct but degraded function, or (iii) complete loss of function. Functional Hazard Assessment (FHA) is being increasingly recommended (e.g., by the Aerospace Recommended Practice - ARP 4754 [SAE94]) as a means of performing hazard identification. It is a process hazard analysis (PHA) form transformed into the aerospace industry. In a similar way, it considers hypothetical failure modes, e.g., 'Loss of function', 'Function provided when not required', 'Incorrect operation of function (high, low …)'. Wilkinson & Kelly (1998) pointed out that failure modes for lower-level sub-systems may not be well understood and hard to apply FHA. Goal tree-success tree (GTST) for each part, 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 causes of hazards are associated with components since the mapping relations between structures and functions are explicit. Again, it is related to the failure modes of components. Jalashgar (1998) offers a terminology to define and categorize different types of system aspects for supporting knowledge acquisition. The research can identify and model systems in terms of different groups of capabilities and combines the advantages of both MFM and GTST methods. Applications are hard in all of the above-mentioned perspectives. The main reason is that hazards in terms of failures of the function's realization are dependent on the aggregation and decomposition of functions discussed previously: parts-whole views and means-end views. In our view, any factors that prevent the realization of the parts-whole relations or means-end relations are the contributions to the hazards and should be considered. Otherwise, hazard identification will not be systematic and suffer from inconsistency and incompleteness.

3.3. *Knowledge representation of hazards and safety functions*

Knowledge representation in general is a field of study in AI concerned with using language to represent a collection of propositions believed by some agent. Based on the knowledge representation, reasoning logic can be used to produce a representation of new ones. So, knowledge representation has two functions: representing existing knowledge and afterward using such knowledge for reasoning (Brachman and Levesque 2004). As mentioned previously, there are two kinds of languages for knowledge representation: natural language and artificial formal language.

Some researchers develop methods for using natural language to represent knowledge in functional models. SADT (Structured Analysis & Design Techniques) uses a graphical presentation that shows the intent in the square box with four arrows in and out, input-output horizontally, and constraints-methods vertically.

The inputs, outputs, constraints, and methods are described by natural language. A detailed description of SADT can be found in Rasmussen & Whetton (1997). Similar to SADT, there are other input-output functional modeling methods, such as functional flow diagrams (FFD), and Functional Basis for Engineering Design (FBED). Function Analysis Diagram (FAD) is a form-dependent functional modeling method. Each block represents a part and not a function. Those blocks are connected to annotated arrows, which denote the function performed by each component, its functional relationship with other components, and the type of function performed (Aurisicchio, Bracewell, and Hooey 2016). The Inherent Behavior of Functional Models (IBFM) method (McIntire et al. 2016) is a functional modelling approach. It is presented in a directed graph, which is composed of nodes and bonds. The nodes are functions and bonds are flows of material, energy, and signal. Each function has modes and conditions, each flow has effort variables and rate variables. Each mode has flow types and behaviors and so does a condition. And the behaviors should be applicable and/or testable. The model can simulate faulty scenarios including multiple faults simultaneously in a short period. The modes and conditions are generated manually, which may not be complete. The functions seem to be domain specific. GTST is a model described using natural language. The model can be extremely scaled up when modeling complex systems. 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 in GTST and control functions is not clear. Natural language represents the knowledge that may introduce ambiguity, and the models may be of little re-usability (G. Hawkins and Woollons 1998).

Other researchers work on methods using artificial formal language to represent knowledge in functional models. To support the interface design of automatic control systems, a set of functional primitives (Liu, Nakata, and Furuta 2004) was proposed to present functions of control systems: “control”, “generate”, “transform”, “set”, “select”, “calculate”, “limit” and “delay”, by graphical means. However, this work simply represents control functions by describing the 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 does not help the operators to understand the causes of control failures, because the causality is not in control signals per.se. but in their meaning. Based on action theories, a set of process functions: “source”, “transport”, “balance”, “storage”, “barrier” and “sink”, and control functions: “maintain”, “produce”, “destroy”, and “suppress” was proposed in MFM. 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. The knowledge representation in MFM models is relatively easy to understand (Wu et al. 2020). The future work using MFM for safety and risk application is summarized in Li et al. (2022). There is also a challenge in using artificial formal language for safety and risk analysis. If the language is purely logical representation, it does not have ambiguity in representation, but it may not be very natural, and inference may not be so efficient.

Knowledge representation is related to how to understand safety modelling in a conceptual structured way. As we pointed out above natural language may introduce ambiguities, and the safety and risk analysis based on such models will not identify all scenarios of failures.

4. Conclusions

Safety and risk analysis in a system’s life cycle is core to ensuring a sound safety basis for the system. To meet functional requirements, functional modeling or analysis should be utilized for supporting all the relevant tasks in safety and risk analysis. The challenges of functional modeling are analyzed, and related literature reviews are summarized for coping with such challenges. The propositions by the authors are concluded after analyzing each challenge.

It is stressed that hazards come from multi-dimensional factors in technical-social systems, functional modeling can distinguish the desired and undesired situations which make the safety and risk analysis goal-oriented and meaningful. Functions including safety functions should be seen as actions for achieving their purposes, and they are intersubjective, which influences identifying what are the causes of failures, and how to validate functional models. To build a functional model for the application of safety and risk analysis, the means-end and parts-whole principles are all required for the decomposition and aggregation of functions including safety functions. Knowledge acquisition is the pre-requisite process for acquiring all the safety-related knowledge for building functional models. The consistency of such knowledge should be ensured. However, such knowledge may be explicitly or implicitly located in different resources in different forms. Such consistency could be a challenge. Establishing a procedure for knowledge acquisition for building functional models could be a solution. Knowledge representation represents existing knowledge and afterward uses such knowledge for reasoning. It is related to how to understand safety modeling in a conceptual structured way. We believe that artificial formal language can conquer the deficiencies of ambiguities in natural language so that such functional models can identify all the possibilities of failures in the context. In this way, it ensures that all the safety bases are sufficient enough for coping with all the possibilities of failures in the context. The safety and risk analysis results are complete.

Acknowledgment

This work was supported by Danish Offshore Research Centre (DTU Offshore).

References

Aboutorab, H., O.K. Hussain, M. Saberi, F.K. Hussain, and E. Chang. (2021). A Survey on the Suitability of Risk Identification Techniques in the Current Networked Environment. *Journal of Network and Computer Applications* 178: 102984. https://www.sciencedirect.com/science/article/pii/S1084804521000114.

Aurisicchio, M., R. Bracewell, and B.L. Hooey. (2016). Rationale Mapping and Functional Modelling Enhanced Root Cause Analysis. *Safety Science* 85: 241–257. https://www.sciencedirect.com/science/article/pii/S0925753515003513.

Brachman, R.J., and H.J. Levesque. (2004). *Knowledge Representation and Reasoning. Knowledge Representation and Reasoning.* Elsevier Inc.

Caiza, G., and R. Sanz. (2022). Digital Twin for the Industry 4.0: Overview, Challenges, and Opportunities. *SSRN Electronic Journal* (February 18).

Cameron, I., S. Mannan, E. Németh, S. Park, H. Pasman, W. Rogers, and B. Seligmann. (2017). Process Hazard Analysis, Hazard Identification and Scenario Definition: Are the Conventional Tools Sufficient, or Should and Can We Do Much Better? *Process Safety and Environmental Protection* 110: 53–70. https://www.sciencedirect.com/science/article/pii/S0957582017300307.

Chandrasekaran, B, A.K. Goel, and Y. Iwasaki. (1993). Functional Representation as Design Rationale. *Computer* 26, no. 1: 48–56.

Chandrasekaran, Balasubramanian. (2005). Representing Function: Relating Functional Representation and Functional Modeling Research Streams. *Ai Edam* 19, no. 2: 65–74.

Duncker, K., and L.S. Lees. (1945). On Problem-Solving. *Psychological Monographs* 58, no. 5: i–113.

G. Hawkins, P., and D.J. Woollons. (1998). Failure Modes and Effects Analysis of Complex Engineering Systems Using Functional Models. *Artificial Intelligence in Engineering* 12, no. 4: 375–397. https://www.sciencedirect.com/science/article/pii/S0954181097100115.

Gomez Perez, A., and V.R. Benjamins. (2009). Overview of Knowledge Sharing and Reuse Components: Ontologies and Problem-Solving Methods.

Gulla, J.A. (2008). Experiences with Industrial Ontology Engineering. In *International Conference on Enterprise Information Systems*, 61–72.

Imran Khan, D., S. Virtanen, P. Bonnal, and A.K. Verma. (2014). Functional Failure Modes Cause-Consequence Logic Suited for Mobile Robots Used at Scientific Facilities. *Reliability Engineering & System Safety* 129: 10–18. https://www.sciencedirect.com/science/article/pii/S095183201400060X.

Jalashgar, A. (1998). Function-Oriented System Analysis. Putting the GTST, MFM and HMG Methods into Perspective. Ed. M Modarres. *Proceedings*: 51–57.

Jørgensen, S.B., M. Lind, and N. Jensen. (2019). Functional Modeling View on Product and Process Engineering in Design and Operations. *Industrial & Engineering Chemistry Research* 58, no. 26: 11129–11148.

Khan, F., S. Rathnayaka, and S. Ahmed. (2015). Methods and Models in Process Safety and Risk

Management: Past, Present and Future. *Process Safety and Environmental Protection* 98: 116–147. https://www.sciencedirect.com/science/article/pii/S0957582015001275.

Kitamura, Y., and R. Mizoguchi. (2004). Ontology-Based Systematization of Functional Knowledge. *Journal of Engineering Design* 15, no. 4: 327–351.

Kitamura, Y., R. Mizoguchi, and others. (2003). Organizing Knowledge about Functional Decomposition. In *DS 31: Proceedings of ICED 03, the 14th International Conference on Engineering Design, Stockholm*, 55–56.

Lee, J., I. Cameron, and M. Hassall. (2019). Improving Process Safety: What Roles for Digitalization and Industry 4.0? *Process Safety and Environmental Protection* 132: 325–339. https://www.sciencedirect.com/science/article/pii/S0957582019317057.

Li, R., J. Wu, O. Ravn, and X. Zhang. (2022). Analyzing Hazards in Process Systems Using Multilevel Flow Modelling: Challenges and Opportunities. In *32nd European Safety and Reliability Conference*, 1441–1448.

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

Liu, Q., K. Nakata, and K. Furuta. (2004). Making Control Systems Visible. *Cognition, Technology & Work* 6, no. 2: 87–106. https://doi.org/10.1007/s10111-003-0148-5.

McIntire, M.G., E. Keshavarzi, I.Y. Tumer, and C. Hoyle. (2016). Functional Models with Inherent Behavior: Towards a Framework for Safety Analysis Early in the Design of Complex Systems. In *ASME International Mechanical Engineering Congress and Exposition*, 50657: V011T15A035.

Minsky, M. (1974). A Framework for Representing Knowledge.

Modarres, Mohammad. (1993). Functional Modeling of Complex Systems Using a GTST-MPLD Framework. In *Proceedings of the International Workshop on Functional Modeling of Complex Technical Systems*, 12–14.

Modarres, Mohammad, and S.W. Cheon. (1999). Function-Centered Modeling of Engineering Systems Using the Goal Tree-Success Tree Technique and Functional Primitives. *Reliability Engineering and System Safety* 64, no. 2: 181–200.

Nielsen, E.K., A. Gofuku, X. Zhang, O. Ravn, and M. Lind. (2020). Causality Validation of Multilevel Flow Modelling. *Computers & Chemical Engineering* 140 (September): 106944. https://linkinghub.elsevier.com/retrieve/pii/S0098135419303953.

Pahl, G., and W. Beitz. (1988). *Engineering Design-a Systematic Approach* . The Design Council.

Rasmussen, B., and C. Whetton. (1997). Hazard Identification Based on Plant Functional Modelling. *Reliability Engineering & System Safety* 55, no. 2: 77–84. https://www.sciencedirect.com/science/article/pii/S0951832096000324.

Searle, J.R., y S. Willis, and others. (1995). *The Construction of Social Reality*. Simon and Schuster.

Sklet, S. (2006). Safety Barriers: Definition, Classification, and Performance. *Journal of Loss Prevention in the Process Industries* 19, no. 5: 494–506.

Venkatasubramanian, V., R. Rengaswamy, and S.N. Kavuri. (2003). A Review of Process Fault Detection and Diagnosis Part II: Qualitative Models and Search Strategies. *Computers and Chemical Engineering* 27, no. 3: 313–326.

Vermaas, P.E. (2009). On Unification: Taking Technical Functions as Objective (and Biological Functions as Subjective). *Functions in Biological and Artificial Worlds: Comparative Philosophical Perspectives, Vienna Series in Theoretical Biology*: 69–87.

Wang, Y., T. Henriksen, M. Deo, and R.A. Mentzer. (2021). Factors Contributing to US Chemical Plant Process Safety Incidents from 2010 to 2020. *Journal of Loss Prevention in the Process Industries* 71.

Wilkinson, P.J., and T.P. Kelly. (1998). Functional Hazard Analysis for Highly Integrated Aerospace Systems. *Iee Certification of Ground/Air Systems Seminar (Ref. No.1998/255)*: 4/1-6.

Wu, J., M. Lind, X. Zhang, S.B. Jørgensen, and G. Sin. (2015). Validation of a Functional Model for Integration of Safety into Process System Design. In *Computer Aided Chemical Engineering*, 37:293–298. Elsevier.

Wu, J., M. Song, X. Zhang, and M. Lind. (2020). A Procedure for Modelling and Verification of Safety Objectives and Functions. In *30th European Safety and Reliability Conference and 15th Probabilistic Safety Assessment and Management Conference*, 1647–1654.

Wu, J., L. Zhang, S.B. Jørgensen, N. Jensen, X. Zhang, and M. Lind. (2014). Procedure for Validation of a Functional Model of a Central Heating System. In *World Conference of Safety of Oil and Gas Industry, Okayama, Japan*, 1-10.