



## Assessing Operational Situations.

Zhang, Xinxin

*Publication date:*  
2015

*Document Version*  
Publisher's PDF, also known as Version of record

[Link back to DTU Orbit](#)

*Citation (APA):*  
Zhang, X. (2015). *Assessing Operational Situations*. Technical University of Denmark, Department of Electrical Engineering.

---

### General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

# **Assessing Operational Situations**

Xinxin Zhang

Technical University of Denmark  
Kongens Lyngby, May 2015

## **Assessing Operational Situations**

### **Author(s):**

Xinxin Zhang

### **Supervisor(s):**

Asso. Prof. Ole Ravn, Technical University Of Denmark

Prof. Emeritus. Morten Lind, Technical University Of Denmark

### **PhD school:**

Department of Electrical Engineering, Technical University of Denmark

### **Technical University of Denmark**

Department of Electrical Engineering

Automation and Control (AUT)

Elektrovej, Building 326

DK-2800 Kgs. Lyngby

Denmark

[www.aut.dtu.dk](http://www.aut.dtu.dk)

Tel: (+45) 45 25 35 76

E-mail: [info@elektro.dtu.dk](mailto:info@elektro.dtu.dk)

---

Release date:	May 2015
Class:	1 (public)
Edition:	1
Comments:	This report is a part of the requirements to achieve the PhD degree at the Technical University of Denmark.
Rights:	©Xinxin Zhang, 2015

# Summary

---

In spite of the high level of automation commonly applied to today's engineering system, humans' skill and knowledge still plays a central role in the systems' daily operation, critical decision making, and accident management. The complexity of the engineered system poses great challenge for human operators to perceive and understand the operational situation. The research domain of situation awareness approaches the operational challenges from the human cognition perspective while the presented thesis aims at supporting situation assessment from the system perspective.

The thesis has reviewed different perspectives on situation awareness in the human factor studies and uses the knowledge reflectively for system representation and analysis. The human cognitive activities during complex plant operation and how they perceive a situation and what kind of knowledge has to be established in the human mental model for the operators to be aware of the situations has motivated the utilization of functional representation in system level of situation assessment. The thesis has summarized the MFM syntax and provides detail instructions of how to model by using the modeling technique.

A PWR primary system is used as a comprehensive modeling case to demonstrate the MFM modeling procedure. Then the thesis investigates the usability of functional modeling approaches to define and model a plant operational situation. MFM modeling is proposed because it is a formalization combining the means-end and part-whole dimensions of a system, so that the MFM models can therefore represent a complex system at several abstraction levels. MFM models also model cause-effect dependencies of functionalities and objectives of the system in different abstraction levels, so the model can be used for causal reasoning. This thesis extends the causal reasoning methods for MFM models and exploits the ability for MFM models to represent operational knowledge and operational modes. Both concepts are of great importance for situation assessment. By applying the extended MFM theory, situation assessment procedure is developed to assess the plant operational situation. The assessment procedure is demonstrated on the PWR model case.



# Resumé

---

Moderne industrielle systemer har en stadig stigende grad af automatisering. Menneskets færdigheder og viden spiller dog stadig en væsentlig rolle når operatørerne tager beslutninger i den daglige drift, især i kritiske situationer og ved håndtering af uheld. Systemernes kompleksitet gør det vanskeligt for operatøren at blive opmærksom på og diagnosticere unormale driftssituationer. Forskningen i menneske-maskine grænseflader undersøger dette "situation awareness" problem med fokus på viden om menneskelig kognition. Formålet med denne afhandling er at undersøge, hvorledes operatørens situationsopfattelse og håndtering af kritiske driftssituationer kan forbedres ved konstruktion af beslutningsstøttesystemer.

Afhandlingen giver en oversigt over menneske-maskine forskningen inden for "situation awareness". Heraf uddrages krav til de systemrepræsentationer og analyser, som et beslutningstøttesystem skal tilbyde for at operatøren skal kunne vurdere kritiske driftssituationer. Det begrundes, hvorfor repræsentationer af systemets formål, funktioner og kausale egenskaber med fordel kan anvendes i analyse og vurdering af kritiske situationer. Tre begrundelser fremføres: 1) operatørers kognitive aktivitet er målorienteret, 2) operatørerne skal anvende viden om systemets funktionelle formål ved analyse af driftssituationer og 3) operatørerne opfatter, forstår og fremskriver en situation ved anvendelse af kausale ræsonnementer.

Afhandlingen anvender formelle metoder til funktionel modellering til at definere og modellere driftssituationer. Det vælges at anvende Multilevel Flow Modeller (MFM), som kombinerer anvendelsen af part-helheds og mål-middel begreber i beskrivelsen af et komplekst system på flere abstraktions niveauer. MFM repræsenterer også kausale relationer og kan derfor også bruges til at ræsonnere over årsager og konsekvenser af hændelser i et system. Afhandlingen udvider eksisterende metoder til kausal ræsonnering i MFM og udvikler nye metoder til repræsentation af operationel viden og overordnede driftstilstande (modes). Begge udvidelser er af betydning for anvendelse af MFM modeller til vurdering af kritiske driftssituationer. Afhandlingen anvender den udvidede MFM teori til formulering af en procedure for situationsvurdering. Afhandlingen

omfatter tillige modellering af det primære kølesystem i en nuklear trykvandsreaktor (PWR). Modellen anvendes til at demonstrere den udviklede metode til situationsvurdering.

# Preface

---

This thesis was prepared at the Automation and Control Group, Department of Electrical Engineering, Technical University of Denmark as part of the requirements for acquiring the PhD degree in engineering.

The PhD project focused on fundamental research of the further development in the functional modeling methodology, Multilevel Flow Modeling (MFM) and MFM causal reasoning. MFM is invented by Morten Lind, who is co-supervising this PhD project, and has been developed for the past two decades. The system knowledge representation requirement in complex systems' design and operation has always been a motivation for the research in MFM modeling. This PhD project is also motivated by applying MFM and MFM reasoning in one area of the industrial application, which is situation assessment for operator decision support. This project is funded by OECD Halden Reactor Project (HRP), SOSPO project, and DTU. The major research is conducted in DTU while the modeling case used in the thesis is partially the research result from the external research stay in Institute of Energy Technology (IFE), Halden, which is the host institute of the HRP project. Although the modeling example is taken from the nuclear industry, the result of the research is also applicable for system that can be modeled by using MFM technique.

The thesis is written as a monograph which consists of 6 Chapters, including the scientific review, theoretical study, and methods demonstration.





# Acknowledgements

---

For all his guidance and inspiration I got during my master study and PhD project, I would love to express my sincere gratitude to my supervisor, Professor Emeritus Morten Lind. Morten has been extremely helpful and selfless when offering his professional knowledge and wisdom. He has been a great support to my study and research, and also a great friend that I am honored to have. I am also very thankful to my supervisor Associate Professor Ole Ravn for all his kind instructions and help during my PhD project.

I am especially thankful to Professor Emeritus Sten Bay Jørgensen, Dr. Niels Jensen, and Dr. Jing Wu for their inspirations and discussions. This thesis would not be finished without their generous support.

I am grateful to DTU Department of Electrical Engineering for providing me the PhD position and the work place. I am extremely grateful for all my colleagues in the Automation and Control Group and in the Department.

I would love to thank the OECD Halden Reactor Project, who provided a part of my PhD funding and also offered me the opportunity for my external research stay. I would love to thank my colleague Harald P-J Thunem in IFE Halden, who I worked with during the length of my project. I want to thank the SOSPO project that also funded my PhD study, and all my colleagues from SOSPO who provided me many inspirations from the power system domain.

Finally, I would love to thank my dearest parents Li Li and Yanfeng Zhang, who generously supported my staying and studying in Denmark from the beginning. I wouldn't be able to achieve this without them.



# Contents

---

<b>Summary</b>	<b>i</b>
<b>Resumé</b>	<b>iii</b>
<b>Preface</b>	<b>v</b>
<b>Acknowledgements</b>	<b>vii</b>
<b>Contents</b>	<b>xi</b>
<b>Glossary</b>	<b>xiii</b>
<b>1 Introduction</b>	<b>1</b>
1.1 Background . . . . .	1
1.2 Research Theme . . . . .	3
1.2.1 What is a situation? . . . . .	3
1.2.2 What to assess? . . . . .	6
1.2.3 How to approach complexity? . . . . .	7
1.3 Research Contribution . . . . .	7
1.4 Thesis structure . . . . .	9
<b>2 State Of the Art</b>	<b>11</b>
2.1 Situation assessment in operator support systems . . . . .	12
2.1.1 Human factors in operations . . . . .	13
2.1.2 Cognitive systems engineering . . . . .	14
2.1.3 Operator support systems . . . . .	16
2.1.4 Situation awareness . . . . .	17
2.1.5 Requirement for knowledge representation . . . . .	23
2.2 Functional modeling . . . . .	24

2.2.1	Functional concepts . . . . .	25
2.2.2	Functional modeling methodologies . . . . .	27
2.3	Current MFM theory . . . . .	31
2.3.1	MFM concepts . . . . .	31
2.3.2	MFM reasoning . . . . .	36
2.3.3	Tools and application . . . . .	36
2.4	Chapter summary . . . . .	40
<b>3</b>	<b>MFM Modeling Procedure and the PWR Model</b>	<b>41</b>
3.1	MFM modeling procedure . . . . .	41
3.1.1	MFM syntax . . . . .	41
3.1.2	Modeling Mass and Energy Flow with causal relations . . . . .	45
3.1.3	MFM model of simple heating system . . . . .	51
3.1.4	MFM modeling procedure . . . . .	55
3.2	Primary system of a pressurized water reactor . . . . .	56
3.2.1	System objectives . . . . .	57
3.2.2	RCS mass and energy flow . . . . .	58
3.2.3	Boron Injection and Rod Control . . . . .	60
3.2.4	Complete PWR primary system model . . . . .	61
3.3	Chapter summary . . . . .	64
<b>4</b>	<b>MFM Extension for Assessing Operational Situations</b>	<b>65</b>
4.1	Representing situations . . . . .	66
4.1.1	Intersubjectivity and subjectivity . . . . .	66
4.1.2	Function and action . . . . .	67
4.1.3	Perception, comprehension and projection . . . . .	68
4.1.4	Representation requirements . . . . .	69
4.2	MFM states and status . . . . .	69
4.2.1	Review of the functional concepts . . . . .	70
4.2.2	Means-end relation . . . . .	71
4.2.3	Abnormal states and status . . . . .	73
4.3	Causal reasoning . . . . .	75
4.3.1	Causal reasoning on part-whole dimension . . . . .	75
4.3.2	Causal reasoning on means-end dimension . . . . .	87
4.3.3	Reasoning propagation . . . . .	90
4.3.4	Rule Based System for MFM Consequence Reasoning . . . . .	91
4.4	Operational Mode . . . . .	95
4.4.1	The concept of mode . . . . .	95
4.4.2	Mode shifts and definition of operational situation . . . . .	97
4.5	Representing operational knowledge . . . . .	100
4.6	Chapter summary . . . . .	100

---

<b>5</b>	<b>Operational Situation Assessment</b>	<b>103</b>
5.1	Procedure for functional assessment . . . . .	103
5.2	Function structure relation . . . . .	107
5.3	Case Study with PWR primary system . . . . .	108
5.3.1	Cause and consequence reasoning for a LOCA situation .	109
5.3.2	Modeling different function-objective modes . . . . .	113
5.3.3	Applying the situation assessment procedure . . . . .	116
5.4	Chapter summary . . . . .	119
<b>6</b>	<b>Conclusions and Perspectives</b>	<b>121</b>
6.1	Contributions . . . . .	122
6.2	Perspectives . . . . .	124
	<b>Bibliography</b>	<b>127</b>



# Glossary

---

**Abstraction Hierarchy** Abstraction Hierarchy describes causal relations within an engineering system at different levels of granularity. The hierarchy includes five levels: Functional purpose, abstract function, generalized function, physical function and physical form.

**Causal Reasoning** Causal reasoning is the ability to identify causality: the relationship between a cause and its effect.

**Cognitive System Engineering** Cognitive systems engineering involves an interdisciplinary focus on the systems design with emphasis on the development of successful human-centered engineered systems.

**Ecological Interface Design (EID)** Ecological Interface Design is a framework for creating advanced user interfaces for complex engineered systems.

**Functional modeling (FM)** A type of qualitative modeling approaches that model a system's functionality and goals.

**Human Factor** Human factors (or ergonomics) is the scientific discipline concerned with the understanding of interactions among humans and other elements of a system. It applies theory, principles and methods to design in order to optimize human well-being and overall system performance.

**Multilevel Flow Modeling (MFM)** A functional modeling methodology representing industry plants by using means-end and part-whole decompositions.

**Operator Support System** Operator support systems are designed to provide useful information to operators for facilitating system operations.

**Pressurized water reactor (PWR)** A type of light water reactor used for nuclear power production. A PWR plant is constituted of a primary side and a secondary side. In the primary side, the coolant (water) is heated by the energy



generated by the fission of atoms in the reactor core under high pressure. In the secondary side, the thermal energy provided by the primary side is used to generate electricity.

**Rule-Based System** Rule-based systems are used in computer science as a way to store and manipulate knowledge to interpret information in a useful way. They are often used in artificial intelligence applications.

**Situation Awareness** Situation awareness describes operators' understanding of the system and environment when operating engineered systems. It is commonly accepted that situation awareness involves three stages: the perception of current elements in the system and environment, the comprehension of their meaning, and the projection of their status.

**Situation Assessment** Situation assessment is a category of methods and tools used for evaluating plant situation.

## CHAPTER 1

# Introduction

---

## 1.1 Background

In spite of the high level of automation which is commonly applied to today's engineering systems, the knowledge and skills of a human operator plays a central role in the systems' daily operation, critical decision making, and accident management. The complexity which is often posed as a challenge for managing modern systems lies not only in the system's operating environment, the physical system itself and human activities apart, but also permeates in the manners of how these three elements can interact with one another during operation. Figure.1.1 illustrates the elements of an engineering system.

It is noticeable that in Figure.1.1, the three elements in the context of an engineered system: humans, physical system, and the environment are interacting not only with one another, but also with themselves. First of all, in complex systems such as a power plant or chemical plant, the operation tasks are not fulfilled by one person but an organization. This creates interactions among humans. Secondly, the modern complex system is highly automated, so that there are complex interactions between the subsystems which realize the industrial process, the safety systems, and the automatic control systems. They work together to achieve the overall designed operational goal of the physical system. That is to say, subsystems that constituted the physical system interact with each other during operations. Finally, the environment also contains unknown internal interactions, meaning that different events can happen during the same time period. This combination of events may pose unpredictable effects on the other two elements in a system. The Fukushima Accident [1] is initiated by two natural disasters, a severe earthquake and a tsunami, and their combination

introduced additional complications in dealing with the environment.

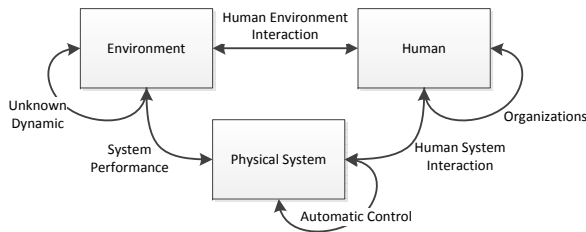


Figure 1.1: The elements of an operating engineered system in context

A complex engineered system such as an industrial plant or product in the context (including the environment, humans, and the physical system), is designed in such a way that it comprises efforts from different scientific domains. To design the system, one must understand 1) how different phenomena can be utilized to realize a specific purpose; 2) how the system should be built so the processes can be applied by the facilitation of the functions realized by physical components; and 3) how to built automatic control systems and design human operations, so that the engineered system can be used to achieve its overall design goal. Therefore, a significant amount of knowledge is poured into the system during design phases.

The complexity then introduces great challenges to the use of the system after it is constructed, even though the system is designed for “easy” operation. Therefore, operator support systems should be developed with the physical system, to provide useful information to the operators or automated systems for facilitating safe operation and control.

Petersen [2] summarized two types of operator aids for supporting the decision-making process: one to reduce or avoid higher-level cognitive activities of the operator by providing preplanned instructions, such as checklists, paper-based procedures, and conventional expert systems; the alternative approach is to support the operator’s higher-level cognitive activities, rooted in studies by researchers such as Rasmussen [3], Woods [4], and Vincente [5]. It has been argued that situation assessment plays a strategic role in decision making, providing the focus and thus serves to broaden the view of the operators and help them to frame the operational problems before solving them. This indicates that not only the knowledge specific for operation (how to carry out actions) is important in situation assessment, but to understand and represent all aspects of

design knowledge is also important so that a situation can be fully interpreted.

System representation (models) for situation assessment is a core task for enabling operator support system design. It is also very important to distinguish the knowledge representation and graphical representation. Model for situation assessment is a prerequisite to another scientific research area of designing human-machine interface to present information and analytical result to facilitate operation.

## 1.2 Research Theme

When talking about understanding and assessing the operational situations, all the elements in Fig 1.1 has to be taken into consideration. One of the challenges to frame an operational situation of such a system is to solve the problem of how to accommodate all the relevant elements into one unified and systematic representation. Only when the operational situation is perceived, understood and can be represented, we can start to develop tools for assessing the situations.

### 1.2.1 What is a situation?

Broadly speaking, a situation can be understood as a state, an event, or a process at a given moment. However, this loosely defined concept does not help researchers to develop assessment method for it, because to assess something, means to determine the significance of it in a specific context.

Situation assessment is closely related to the research domain of situation awareness, where the concept of situation (either to be assessed and or be aware of by the operators) should be in common. Although, there is no agreed definition of situation awareness, a widely accepted definition comes from Endsley [6], stating that to be aware of a situation, one has to obtain three levels of knowledge: 1) “the perception of elements in the environment within a volume of time and space”, 2) “the comprehension of their meaning”, and 3) “the projection of their status in the near future”. This definition gives some level of overview of what a situation is, suggesting that a situation is not only related to the current events and states of the system, but also related to the future progression based on the current condition. However, this does not provide deep insight of the real contents which consist of a situation. For example, one may ask further questions such as what are those elements which the operators must perceive and comprehend and how to model them. Therefore, we try to search for the

definition of a situation from other research endeavors to understand the core elements which are included in the concept.

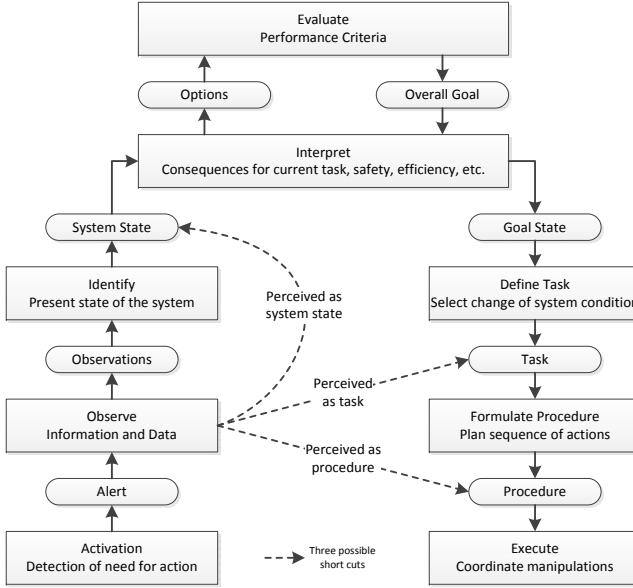


Figure 1.2: Rassmussen's decision making model [7]

Rassmussen's decision model [7] in Figure 1.2 provides a general framework to represent the procedure of information processes involved in making a control decision in relation to a complex system. It is noticeable that the initiation (activation) of such a decision making process stems from the detection of a need for action, terminates with the deployment of the selected procedure based on the step by step knowledge establishment to solve the problem. Shortcuts in Figure 1.2 suggest that if countable previous experience is available for the problem and further knowledge about plant operation can be derived based on a early stage activity in the decision model, the decision making procedure can be shortened. The decision model provides one way to frame the concept situation, for it offers great inputs of what knowledge is required for understanding an abnormal situation and how to response to it although it does not use the term situation in itself.

The knowledge that is required for situation assessment however, does not have the same sequential property and all the knowledge states in the decision model have to be organized in a different way so the emerged event can be viewed in context of all knowledge states presented in the decision model. Another key point that one can derive from the decision model is that, only when an

action is in need, then the decision making process is triggered. Thus there's a requirement for determining whether the situation is of the operator's concern or not. This offers some convenience in defining a situation because thus it is only needed to investigate the definition of the set of the situations which does require operators' attention in context of operational situation.

Dewey's study [8] from philosophy of science provides clues of what constitutes a situation from a learning perspective. He defined the concept of problematic situations, as the situations worth noticing, because those are the ones requiring further treatment. From this study, the problematic situation is a situation where instinctive or habitual responses of the human organism to the environment are inadequate for the continuation of ongoing activity in pursuit of the fulfillment of the human's needs and desires.

Although the definition of problematic situation is about knowledge inquiry, it offers several key points to understand the nature of a situation. First of all, as suggested by Burke [9], the term *situation* (in Dewey's study [8]), should not be misunderstood as referring simply to a material context or environment. Rather, it should be apprehended as a unified matrix of which the learner is an integral component. Secondly, the term "fulfillment of one's needs and desires" suggest that a situation is closely related to goal fulfillment, which is also suggested by the decision model in Figure 1.2. The third point that this definition gives is that when determining a problematic situation, one must referring to past experience (habitual responses) and given a projection of the future state (discontinuation of the fulfillment of needs and desires), which is also hinted to by Endsley's [6] formulation of situation awareness.

In Dewey's definition of a problematic situation, only humans and their environment are of consideration. However, in complex system, there are three players as emphasized in Section 1.1. To apply this definition, it is needed to determine the relation between humans and systems. Based on the design relations, the physical system is constructed to fulfill the design goal of humans, which means that the physical system serves as the means when considering goal fulfillment from an operation perspective. Lind [10] discusses the concept of goals and purposes in the context of modeling complex systems.

We can apply Dewey's theory to engineering system operation, combined with the inspiration provided by the decision model and other related definition. A problematic operational situation means a situation that, under normal operations the system's responses to the environment are inadequate for the continuation of ongoing operation to fulfill what the system is designed for, thus certain actions are required.

### 1.2.2 What to assess?

The purpose of assessing operational situations is to facilitate human operators to fulfill their operation tasks. Separating the problematic situations which require actions from normal situations is only the starting point for understanding the problem of situation assessment.

To detect a failure in goal fulfillment, only the knowledge about goal structure of the system is needed. However, the more important aspect of the assessment process, it to understand the cause effect of the failure in goal fulfillment and to reason about the remedial actions that the operator can perform so that the system can operate to fulfill the overall goal again.

According to the decision model, it should be emphasized that the new goal to perform the remedial actions (operation) is not necessarily the same on the goal prior to the failure, and how the new goal is achieved in some cases is by reformulating the system functions and function goal relations. Therefore, for situation assessment, the situation contains not only one operation mode but several. And the transition between different operation modes and the possibility of the modes transition are all parts of a situation and should be taken into consideration for assessment.

To summarize, a situation assessment should include the knowledge about:

1. current goal function relations,
2. a detection or prediction of goal failure and the cause effect of the current event,
3. the desirable operation modes that the system can be brought into by certain operations in the near future,
4. the possible operation plans.

After the required knowledge is identified, the next step is to find proper representation to make the knowledge explicit. For modern industrial plant and product, the challenge of knowledge representation is rooted in handling system complexity. The next section discusses how to approach the complexity when choosing modeling methodology for situation assessment.

### 1.2.3 How to approach complexity?

This section discusses the challenge of how to make the knowledge required for situation assessment explicit so that it can be used by both machines and humans to deal with the environment. The knowledge representation is challenging because the required knowledge is very diverse and it is difficult to formulate all the aspects in a unified way. The challenge also lies in representing the complexity of those systems that we are targeting, which include multiple elements and relations. The modeling approaches can be divided into two categories. One is qualitative modeling and the other is quantitative modeling. The goal function understanding and qualitative representation provide basis for the quantitative models while the quantitative model can represent the system dynamic in a more precise way than qualitative models. However, when the system is modeled by using quantitative methods, the narrative aspects is lasted in the abstraction. In operational situation assessment, using mathematical formulation to describe the overall goal and functions of the system is against the explanation purpose. Qualitative functional descriptions have to serve as an umbrella to cover the scope of a situation for representing its significance.

When dealing with complexities, abstraction is a natural solution for functional representations. However the abstraction level has to be determined so that the analysis result from the constructed representation is still meaningful to serve its purposes. To gain flexibility for using abstractions in modeling, the core concept is to decompose the system not only into parts, but also in a means-end manner. The means-end structure in a system describes how the system goal is fulfilled by abstract functions and how the functions can be realized. The abstraction levels changes along when decompose a system along the means-end dimension, so that it is easy to customize the abstraction levels to fit for the representation purposes.

## 1.3 Research Contribution

The discussion in Section 1.1 suggests that a proper modeling methodology need to be chosen as the framework for operational situation assessment in both knowledge representation and reasoning.

Petersen [2] investigated the fundamental questions associated with the use of one of the functional modeling approach, namely Multilevel Flow Modeling (MFM) for overall assessment of disturbance situations in complex process plant. Petersen argues that MFM provides an explicit representation of the in-



tentional structure of process plant in terms of goals and functions, and that it meets the requirements for situation assessment for supervisory control tasks by adopting the method for system level knowledge representation. Petersen also extended the modeling methodology by defining causal relations between different modeling concepts, so that the method is equipped with reasoning capability for determining the possible causes and consequences as well. A prototype which uses MFM for situation assessment was developed.

However, this pioneering study of using MFM for situation assessment does not fully explore situation as a concept in the context of plant operation. The present thesis will provide insights of how MFM models with the suggested extension of concepts and reasoning capability can define operational situations. Thus the modeling method can be used for situation assessment.

MFM as a modeling methodology has been extended several times after Peterson's first attempt to use the method for situation assessment. This thesis will review the state of art development of the MFM and make further extensions of the modeling methodology, so that the models of MFM are suitable for situation assessment.

The purpose of this thesis is to define operational situation representation (model) to reflect the need for the operator to achieve situation awareness and develop situation assessment procedure based on the developed model. The main research contribution for situation assessment includes:

1. framing an operational situation from the system perspective in reflection of how human operator perceive and understand the situation,
2. identify the requirements for model the operational situation, and applying functional modeling methodology, Multilevel Flow Modeling (MFM), as the modeling method for situation assessment,
3. extending MFM approach, designing and implementing consequence reasoning strategies for MFM, use MFM concepts to define and model operational modes which constitutes an operational situation.
4. designing assessment procedure by using MFM models and provides a use case.

## 1.4 Thesis structure

The major contents of the thesis are summarized in Fig.1.3. It includes two parts: 1) Methodology development and 2) Operational situation assessment application. First it will give a comprehensive explanation of how the chosen functional modeling approach can represent the key concepts of a complex engineering system for operational situation assessment. The theoretical contribution of the thesis will be explained so that the chosen modeling method is extended to fit all the requirements of representing process and operation knowledge of a complex system, and furthermore, the developed models are designed to fit for the purpose of situation assessment. Then by applying the theories the operational assessment method will be developed. A nuclear power plant, as a fairly complex and safety critical engineering system, is chosen as example domain to demonstrate the modeling and operational situation assessment procedure.

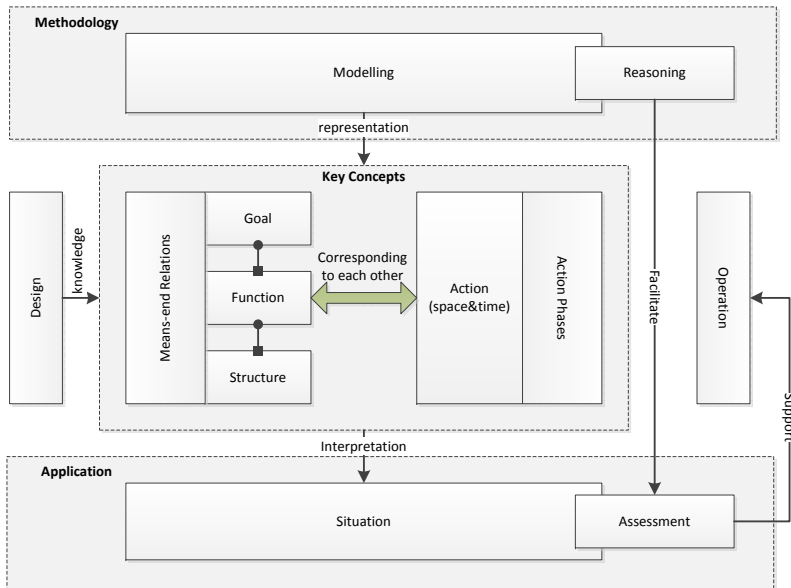


Figure 1.3: Thesis content overview

The thesis comprises 6 chapters, Chapter 1 introduces the overall problem and the research methodology. Chapter 2 provides a scientific review of the current modeling methodologies and the state of the art of operator support systems and situation assessment. Chapter 3 provides detailed explanation of the Modeling

of the primary system in a Pressurized Water Reactor (PWR) unit. Chapter 4 presents the theoretical contribution of this thesis to further extend the modeling methodology and reasoning strategy for situation assessment purposes. Chapter 5 demonstrates the operational situation assessment application by using functional models and reasoning. A case study is provided by using the modeling example from Chapter 3. Chapter 6 will conclude the thesis and present some future perspectives of this project.

## CHAPTER 2

# State Of the Art

---

The term situation awareness has its common usage [11] in daily life associate with driving, playing sports and even in activities such as crossing a busy street. This concept also has long history in military theory, which can be traced back to the ancient Chinese military general and philosopher Sun Tzu, who proposed several military strategies in his work “The Art of War”, such as “he who knows when he can fight and when he cannot will be victorious” and “if you know your enemies and know yourself, you will not be imperiled in a hundred battles”. The concept of “knowing” is essential when discussion situation awareness. When people interact with their environment, they want to know what is happening, what could happen and what kind of options they have in relation to what they want to achieve. Several literatures [11, 12] suggest that the scientific concept of situation awareness in engineering field is firstly identified in the field of military aviation. And this subject started to attract more attention in the technical and academic literature from the late 1980s after the society had witnessed several severe accidents such as Three Mile Island Accident and several aircraft crashes. Afterwards this concept of situation awareness, even though with non-agreeable and debatable definition of itself, becomes an important research domain in a variety of industries such as in aviation industry, chemical production industry, and power production industry. This increasing attention and focus on operators and operations is a result of the increasing system complexity and level of automation. The purpose of the research endeavors in this field is to eventually improve situation awareness of the human operators so that they can keep the system operating in a safe and efficient status. There are three aspects that are involved in the research theme, including: the fundamental understanding of situation awareness, the methodology for situation assessment, and the implementation of operator support system for situation awareness.

In all relevant literatures, the terms situation(al) awareness, situation(al) assessment and situation(al) measurement are used with ambiguous definitions and sometimes interchangeable. For the clearance, in this thesis, the term situation awareness and situation assessment are both used, though with different meaning. The latter refers to the status of the engineered system with human operator, physical system, and the environment enclosed as a whole, while the former refers to the human's understanding and reflection of the status (which has a strong focus on human factor). While both of the terms uses the concept of situation, however, the former emphasize on the intersubjective aspect of a situation, while the later emphasize the subjective aspect of the same concept.

In this chapter, relevant literature is reviewed in three major parts. Section 2.1 offers literature review of operator support systems developed based upon the concept of situation awareness and assessment. The review of the literature identifies the challenges of how the knowledge of operational situations should be represented in a systematic way, which leads to the second part of the literature review in Section 2.2, centered on Functional Modeling (FM) which is argued as a promising method to supplement the development of support systems for situation awareness and assessment because it has a strong scientific basis. Among the variety of FM methodologies, Multilevel Flow Modeling (MFM) is the choice of method for modeling in this thesis, for assessing operational situations. Thus a detailed review of MFM is also offered in Section 2.3. Section 2.4 concludes this section.

## 2.1 Situation assessment in operator support systems

As already mentioned above, situation awareness and assessment has rather non-agreeable definitions and are applied in various of industrial domains. Nofi [11] suggested that after a review in the field of situation awareness, it seems that many key researchers agreed that the definition of situation awareness is loosely defined, and the challenge partially lies on the fact that the understanding of situation awareness differs between applicable domains. However, these researchers also agreed that there are generic aspects in situation awareness which can be applied in general.

The review is arranged in such a way that it firstly introduces the application of situation assessment so that the reader can understand the key issues in the applications before the fundamental theory of situation awareness is reviewed. For the relevance of the case study in the present thesis, literature is reviewed especially in the application domain of nuclear power production among others.

However, the reader shall bear in mind that it is the generic approaches and frameworks that the thesis will examine in depth.

### **2.1.1 Human factors in operations**

A complex industrial plant such as power plants or a highly automated transportation system such as modern aircrafts and ships are often operated by operators in a control room. Usually, the operators in the control room consist of one or multiple operators and the number of the crew is different according to the tasks. The operators' role in such a plant or craft usually includes monitoring the system status and manipulating the control devices when necessary. The operators often perform supervisory roles of information acquisition and interpretation, planning, and decision making. Those tasks are usually complex and mentally challenging due to the complexity of the system and the environment.

In safety-critical and complex systems such as chemical plants, power plants, and transportation systems, human errors can be a serious cause of accidents. For example, in the aviation industry, statistics on the causes of accidents from 1959 through 1989 indicate that flight crew actions were casual in more than 70% of worldwide accidents involving aircraft damage beyond economical repair. [13] In the nuclear engineering, an analysis of the abstracts from 180 significant events reported from the nuclear power plants (NPPs) in the United States that 48% of the incidents were attributable to human-factor failures [14]. These severe accidents motivate researchers to focus on the human operators' performance. Lee and Soeng suggest [15] that there have been two approaches to prevent human error during nuclear main control room operations. The first approach is the provision of better training and education programs for operators. The second is to improve human machine interfaces (HMIs) with improved interfaces and operator support systems. These two aspects are drawn from human factor research.

Ergonomics, or human factors is the scientific discipline concerned with the understanding of interactions among humans and other elements of a system, and the profession that applies theory, principles, data and methods to design in order to optimize human well-being and overall system performance. Among different specializations within this research domain, cognitive ergonomics is concerned with mental processes, such as perception, memory, reasoning, and motor response, as they affect interactions among humans and other elements of a system. The relevant topics include mental workload, decision-making, skilled performance, human-computer interaction, human reliability, work stress and training as these may relate to human-system design and interaction.

The study of human factors mostly started from the human perspective, the systems that humans are interacted with are also important for human performance. It is pointed out by Reason [16] that it is imperative for aviation industry to accept that the failures of people involved in daily routines are symptoms of deficiencies at the deep foundations of the system. This can also be applied to other industries. The need for a systematic and comprehensive approach to cognitive issues in the design of systems involving human operators has emerged over the past 20 years especially as computer-based technologies have pushed the nature of operational work in a direction in which cognitive challenges gained more and more dominating position.

### 2.1.2 Cognitive systems engineering

Cognitive systems engineering [17, 18] involves an interdisciplinary focus on the systems design with emphasis on the development of successful sociotechnical systems. A sociotechnical system is one in which humans provide essential functionality related to deciding, planning, collaborating and managing. The concept describes most of the engineered systems nowadays and in line with the context of engineered system that is specified in Figure 1.1, Chapter 1. Drawing on contemporary insights from cognitive, social and organizational psychology, cognitive system engineers seek to design systems that are effective and robust. The central task of the domain is on amplifying the human capability to perform cognitive work by integrating technical functions with the human cognitive processes they need to support and on making that cognitive work more reliable. [17]

Elm et al.'s [19] review on cognitive system engineering suggests that at an abstract level of description, the approaches of cognitive system engineering are straightforward and very similar to the analysis and design strategies used in other engineering domains. It requires the observation of the field practices and representation of the knowledge. Thus the acquired knowledge of some form can facilitate the design of appropriate cognitive support systems. Those design solutions are then evaluated via computer modeling or human-in-the-loop simulation. While the approach may sound familiar to many engineers, the methodologies used for knowledge acquisition, knowledge representation and cognitive modeling may not. These methodologies have been developed specifically to deal with the complex and nonlinear nature of human cognition; its hidden interdependencies and those of its processes that are beyond the conscious awareness of the operational expert.

Rasmussen's [20] study in cognitive system engineering distinguishes between three levels of cognitive behavior of human operators, namely skill, rule and

knowledge-based behaviors. According to Rasmussen, human use different behavior to solve different type of cognitive tasks. The three levels are explained:

**Skill-Based Behavior** that depends on operator's direct sensory-motor interaction with his environment in a feed-forward manner. (Where no conscious attention is required.)

**Rule-Based Behavior** which is performed on the basis of rules. The rules in this context can be both internal established mental perceptual cues and external guidance (such as procedures)

**Knowledge-Based Behavior** of operators when utilizing explicit models of the system being supervised to interpret display information and reason about the system.

Among the three levels of cognitive activities, knowledge-based behavior is the most demanding type of task and is used only in unfamiliar situations where know-how and rules for operation are not readily available from previous cases.

The complete decision model (see Figure 1.2) illustrates the decision making procedure by adopting knowledge-based behaviors during which an operator has to go through different activities and establish all the required knowledge to be able to perform the required actions. Some examples of decision making short-cuts are also identified in the model. For example, the operator can map his/her observation with either internal or external rules to the tasks he/she shall perform directly, without formulating the goal explicitly, which indicates a rule-based behavior.

It is important to notice that there is no indication in the decision model that each knowledge state should be derived by human or provided by computerized systems. Combining with the understanding of different cognitive activities, the skill-based activities can only be improved by accumulating experiences through training, while the rule- and knowledge-based activities can be supported by external resources.

Petersen [2] reviewed the human cognitive activities during supervisory controls and discussed different cognitive levels (skill-rule-knowledge [20]) and the contextual model provided by Bainbridge [21]. Petersen summarizes that it is important to frame the situation according to the intentional structure of the system being supervised because the operator activities and actions are subordinate to the intentions ascribed to the system. During disturbances which cannot be handled by the automatic control systems, the operator must intervene and actively maintain or restore the goals ascribe to the system that they are operating.



According to the understanding of human centered system and the three types of operator behavior, operator support systems should be developed to facilitate the operation and they are especially important in the field that knowledge-based activities dominates operators tasks. In the next section the existing operator support system in safety critical system is briefly reviewed.

### 2.1.3 Operator support systems

As the processing and information presentation capabilities of modern computers increase, the trend is shifting toward the application of modern computer techniques to the design of advanced decision support system. Kim [22] suggests that the design of instrumentation and control (I&C) systems for various plant systems is rapidly moving toward full digitalization, with an increased proportion of automation.

Advanced plants, for example like modernized NPP control room, have been considerably simplified, and now use large display panels (LDPs) and LCD displays instead of analogue indicators, hand switches, and alarm tiles. In these control rooms, operators do not have to move around the room in order to view indicators or even control devices. Every necessary action is handled in their position. Moreover, many pursuits have been made to develop operator support systems that allow more convenient control room operation and maintenance. The operator support systems aim to provide useful information to operators for optimizing the workload of operators and to establish convenient operation environment. However, they could cause not only positive effects but also negative effects on the system safety. For example, if there is insufficient explanation and the functionality of the knowledge that used for developing the support system is hidden and become transparent to the operator, the adopting of using support system may cause problem during situations that the support system cannot provide meaningful aids to the operators.

Kim and Seong [23] identified that since operator support systems could directly affect the decisions of an operator, their effects should be evaluated carefully. The new systems could reduce the possibilities of specific types of human errors, but new types of human errors could occur or possibilities of some human errors could increase.

There are various kinds of support systems at work for the operators, aiding with surveillance, diagnostics, and the prevention of human error. Some of these, such as early fault detection systems [24], are capable of doing tasks which are difficult for operators. Others, such as operation validation systems, are intended to prevent human errors [25]. As the control rooms evolve, more

support systems will be adapted to digital displays and mobile devices.

However, according to the result of operator aids evaluations [26], a support system does not guarantee an increase in operator performance and inappropriate operator support systems or automation systems can have adverse effects. The report also concludes that some support systems could degrade an operator's situation awareness capability and may increase an operator's mental workload, for they provide more information for the operator the process.

The operator support system developed in modern control rooms such the MCR in an NPP is technology based and the performance of the support system is evaluated mostly through operators' performance when working with the support systems [15]. It is arguable that the implementation of the support system requires theoretical foundations to support the design. And most of the theories are coming from the study within human factor and cognitive system engineering. In next section, a narrower research area, namely situation awareness will be reviewed in depth.

#### 2.1.4 Situation awareness

Following the previous discussion, one may ask the question that what exactly is the requirement for the human operator to effectively avoid human errors. This is largely depending on which type of activity is required for the human operator. If only the rule based behaviors are required, then deployment of more automation and enhance the reliability of automation system is the preferable way to increase system operation reliability as a whole (including both human reliability and system reliability). However, for most of the complex systems, there is great uncertainty due to the dynamic environment of the systems, making the operator aware of the operational situation is an obvious requirement during that unfamiliar event occurrence. In this case, the introduction of more automation system does not ensure the minimizing human errors. To the contrast, Endsley reviewed much literature which documented the negative effects of increased automation on operator's situation awareness, leading to significant out-of-the-loop performance reduction [27].

Endsley's research [27] has pointed out that, based on Bainbridge's view on different levels of automation [28], such reduction in situation awareness for human operators to operate highly automated systems partly result from poor transparency and deficiencies in the design of the user interface. The operator's task is also shift fundamentally from the active observation to the passive response to system indicators. This shift accompanied by the typical approach of implementing automation systems put the operator in the role of monitor. This

research also was able to identify alternate automation paradigms, featuring intermediate levels of automation, which could minimize these losses of operator's awareness.

As mentioned previously, situation awareness is a widely applied concept for three major research studies mentioned by [29]:

1. How various design decisions associated with automation may negatively or positively affect situation awareness?
2. How to improve the system technologies, user interfaces, and display designs to support situation awareness?
3. How to develop training approaches for improving situation awareness?

To expand upon their three-stage procedure to achieve situation awareness, Endsley et. al. [30] describe the three hierarchical phases of situation awareness: perception, comprehension, and projection by using pilot and operating aircraft as an example (SA refers to situation awareness in the following quotes):

**Level 1 Perception of the elements in the environment:** “The first step in achieving SA involves perceiving the status, attributes, and dynamics of relevant elements in the environment. The pilot needs to accurately perceive information about his/her aircraft and its systems (airspeed, position, altitude, route, direction of flight, etc.), as well as weather, air traffic control clearances, emergency information, and other pertinent elements.”

**Level 2 Comprehension of the current situation:** “Comprehension of the situation is based on a synthesis of disjointed Level 1 elements. Level 2 SA goes beyond simply being aware of the elements that are present to include an understanding of the significance of those elements in light of the pilot's goals. Based upon knowledge of Level 1 elements, particularly when put together to form patterns with other elements, a holistic picture of the environment will be formed, including a comprehension of the significance of information and events.”

**Level 3 Projection of future status:** “It is the ability to project the future actions of the elements in the environment, at least in the near term, which forms the third and highest level of Situation Awareness. This is achieved through knowledge of the status and dynamics of the elements and a comprehension of the situation (both Level 1 and Level 2 SA).”

This explanations offers an example of what can be the elements in the operators' working environment (answering the question posted in Section 1.2.1 in a specific

domain). However, there is still a lack of formalization and cannot be applied to general systems.

Based on the levels automation proposed by Sheridan and Verplank [31], Endsley [27] analysis the 10 level of automation together with the control tasks (monitoring, generating, selecting and implementing) in the control room. This study suggests a sharing of tasks between human and automation systems. According to above definition, situation awareness is clearly a subjective concept, which requires a mental model of the operator. However, the knowledge about the system goal and function is designed and the operational situation also has an intersubjective aspect. Thus there is intersubjectivity lies in the concept of situation. The first level of situation awareness is to perceive, which require that enough (meaningful) information can be gathered by the operator. How the information is presented to the operator will highly affect the foundation of human situation awareness.

Harrald and Jefferson [32] states that the information component of situational awareness depends on both the particular domain and the users' dynamic information needs. To determine the information required it is necessary to focus on the basic goals of the decision maker and the major decisions that they need to make to achieve the goals. From the information required it is then possible to determine the individual data source that need to be collected. This emphasizes one of the difficulties with obtaining situational awareness; developing static and anticipated goals. Harrald and Jefferson summarized the general characteristics about data requirements based on the levels of situation awareness as follow:

1. Collect the data required to satisfy the decision makers goal. The data collected needs to directly support the decision maker in arriving at their objective. While there is often more data collected that is actually required it is important to group and present the data as information that can be directly used to achieve a desired result.
2. Data collected should have the attributes necessary to sufficiently describe a required piece of information.
3. Data must provide the ability to describe relationships between components.
4. Data must provide the ability to link the attributes for any given piece of information to time. It is important to maintain a time-line of what changes occurred in data values. This will allow the user to obtain Level 3 situation awareness by being able to predict future states.
5. Data must be of sufficient quality to meet the decision making and action needs.

Based on the theoretical research, applicable methodologies and applications are developed to support all the three stages of situation awareness: display design for supporting mostly in perception and also in comprehension, the system diagnosis tools support situation comprehension, and the situation awareness models for projection and prediction. The following sub sections will review each of these three research areas.

#### 2.1.4.1 Display design for information retrieval

Ecological Interface Design (EID) [33] is a framework for creating advanced user interfaces for complex engineered systems. Unpredictable events that occur in dynamic, open systems can lead to unfamiliar situations that are difficult for operators to identify comprehensively through user analysis techniques. The EID approach begins by generating a work domain model revealing the functional constraints of a system, this model is then used to structure the visual interface. The resulting design embeds the functional relationships between physical components into the display at different levels of functional abstraction. This provides an externalized system model, which should allow for a better understanding of the system state and support users dealing with unanticipated events. This approach supplement situation awareness which starts from the operator's task analysis rather than work domain analysis of the system and environment in which the operators work.

The key concept for work domain analysis in the EID approach is the Abstraction Hierarchy, which describes causal relationships within an engineering system at different levels of granularity, placing the high-level functional purpose at the top and physical functions carried out by components at the bottom [34]:

1. **Functional purpose** Production flow models, system objectives, constraints etc.
2. **Abstract function** Causal structure including mass, energy, and information flow topology, etc.
3. **Generalized function** Standard functions and processes including feedback loops, heat transfer, etc.
4. **Physical function** Electrical, mechanical, chemical processes of components and equipments
5. **Physical form** Physical appearance and anatomy; material and form; locations, etc.

AH defines the means-end hierarchy of the system. The same system can also be physically divided into sub-systems and further into individual components. This sort of decomposing a system is called part-whole decomposition. By combining part-whole and functional decompositions, a work domain model is generated in the form of an Abstraction Decomposition Space (ADS).

As introduced previously, operator behaviors when working with complex systems can be categorized into three different types: skills-based, rules-based, and knowledge-based [20]. These categories of behavior require information from progressively higher levels of the abstraction hierarchy. EID outlines three visual design principles to ensure that each mode is supported.

- To support skills-based behavior direct manipulation should be used and the representation should be isomorphic to the part-whole structure.
- To support rules-based behavior a consistent one-to-one mapping between constraints and the cues or signs provided by the interface should be provided.
- To support knowledge-based behavior the work domain should be represented in the form of an abstraction hierarchy to serve as an externalized system model.

Paulsen also designed for different displays in her PhD thesis [35], adopting the idea of Rassmussen's AH but emphasis on representing knowledge that is originated from plant design. The design framework developed by Paulsen use AH as basis but try to combine functional modeling approach such as Goal-Tree Success-Tree (GTST) into display design when considering functional knowledge about the plant. This framework offers an addition to the display's function in supporting situation awareness, not only to provide information about the current function and state graphically, but to consider the underlying process knowledge.

#### 2.1.4.2 System diagnosis for comprehension

As information is perceived by the operators, the second level of situation awareness is to make sense of the information. Endsley [36] has identified that diagnostic tasks is a challenge for operators especially during the comprehension level of situation awareness.

Petersen [2] suggests that cause-effect reasoning based on the current system state is a crucial part of understanding a disturbed situation which requires

control actions. He also adopted Rasmussen's AH as an initial framework for developing diagnosis methodologies in context of the system control goals.

In practice, diagnosis is a task performed with the aim of establishing a basis for formulating the goal of intervention and the particular action to take. Rasmussen [20] argued that diagnosis is a goal-directed activity inextricably connected with action, that cannot be separated from the contextual factors that determine actions. Both Rasmussen [17] and Vicente et al. [37] agreed that during fault diagnosis, a disturbance is often identified at an abstract level, while failed components are identified at a lower level of abstraction. This top-down approach of diagnosis reflects an appropriate way for diagnosis agents such as human operators to cope with system complexity.

However, as Petersen [2] later identified and also argued by Lind [38], AH is not a representation in itself, but rather a loosely defined framework for representation. According to Lind, the abstraction hierarchy has immediate intuitive appeal to engineers, but is conceptually difficult to apply for modeling. The means-end and part-whole concepts of AH is adopted by Lind for developing another Functional Modeling methodology to overcome the problems that shows in applying AH for modeling and reasoning.

#### 2.1.4.3 Situation assessment methods for prediction

Since situation awareness aims not only to perceive and comprehend but also to predict the status of a situation in the near future, which is the third level of the situation awareness, there are various situation assessment approaches to conduct the prediction. Also because the engineered system is a dynamic and collaborative process, the development of efficient assessing methods usually require data integration with the support of computer-based intelligent techniques.

Several tools have been adopted for assessing situations. Among those, studies have reported that machine learning techniques can provide an effective method of intelligent prediction by extracting rules from previous data to generate new assessment results. For instance, Lu et al. [39] developed a support vector machine-based assessment approach which has the ability to learn the rules from previous assessment results and generate the necessary warnings for a situation. They used a synthesized, artificially generated data set to illustrate the effectiveness of their proposed situation assessment approach. A neural network-based situation assessment module was developed by Brannon et al. [40] to provide a high level of SA for decision makers in force protection. Naderpour [41] pointed out that despite the usefulness of machine learning techniques for

situation assessment, their use in real environments is very limited because of the insufficiency in the training data.

Bayesian theory has also been widely considered in the situation assessment configuration in complex and safety-critical process under uncertainty. Miao [42] developed a computational model and a model-based situation awareness metric to quantify and measure operator situation awareness. The developed model is used to provide explicit representation of the operator's fundamental functions of information processing, situation assessment, and decision making in the system operation. Kim and Seong [43] developed an analytic model for the situation assessment of NPP operators also based on Bayesian inference. However, there is certain limitation for implementing these methods because the lack of a fundamental support to define a situation (or making assumptions).

Naderpour and Lu developed an expert system-based situation assessment method for a chemical plant [44] and extended it to incorporate the ability of neural networks to project the state of the environment in to the near future. However, because of the lack of appropriate data for abnormal situations, it could not be implemented in the real world. They also developed a situation awareness support system [41] based on goal-directed task analysis methodology for the development of a situation awareness support system to help operators in abnormal situations. However, similar problem remains for how to understand situation as a fundamental concept rather than analyze a situation based on the tasks of operator.

These models are useful for the operator support system to facilitating the prediction of plant situation development based on situation awareness, but do not emphasis on the semantic meanings of the data which is collected from the system.

### 2.1.5 Requirement for knowledge representation

Previous discussions in Section 2.1 provide an overview of development in support situation awareness and assessment. Figure 2.1 shows the research activities in the related area. Human operators create a reflection of the physical system's status through establishment of knowledge. This knowledge is graphically visualized by using displays. The operator understand the system function and goals and go through the three states of perception, comprehension and projection to reach situation awareness and decide how to operate in the specific situation. The representation of the engineered system for situation assessment, should reflect the cognitive procedure for facilitating the operators to generate the mental model.



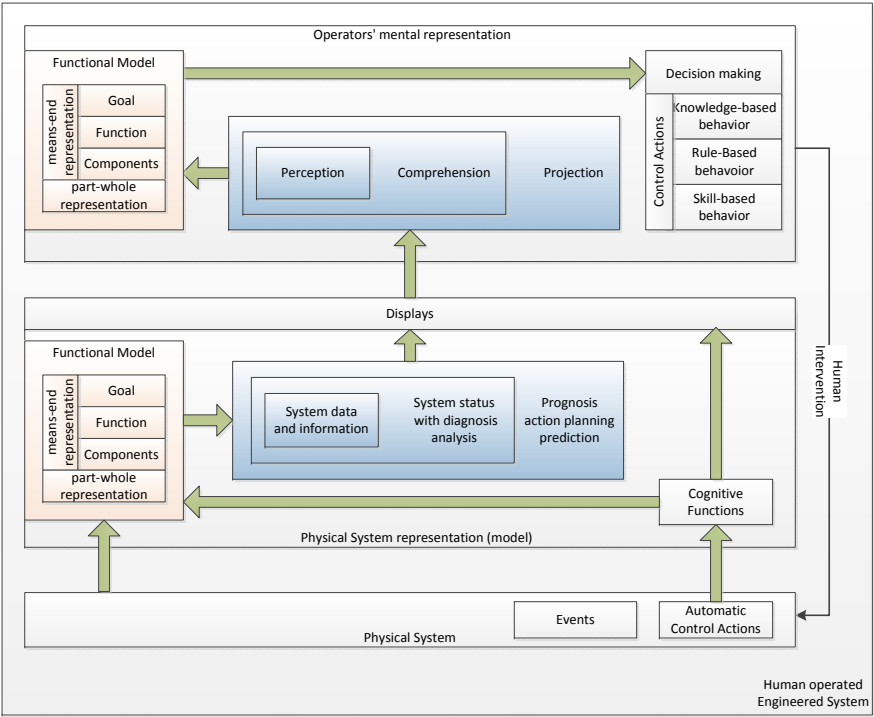


Figure 2.1: Modeling context for situation assessment.

One of the challenges has been identified by Endsley is that the automation system give negative effect on operator's situation awareness. Therefore, the automatic control actions, should be represented to the operator in context of the same intentional structure as the human operation. These control intentions, should be represented together with the process goal-function relations.

Therefore, the modeling approach is selected within the category of functional modeling, which represent system in a functional abstraction level, which can facilitate the human operator to build their mental model for understanding the situation.

## 2.2 Functional modeling

Functional Modeling comprises concepts, methods and tools which for representing the purposes and functional organization of complex dynamic systems.

Lind [45,46] and Chittaro [47] among other researchers has been promoting that models representing functional knowledge are useful for improving the performance of system diagnosis, which is part of the operators tasks for understanding the situation.

Lind [45] suggested two basic motivations to use a FM method. The first is that the concepts of FM provide a systematic framework for formalizing intersubjective knowledge which is shared among participants in design and operation of complex systems, i.e. engineers and operators. The second is motivation is that FM is a systematic approach to apply different perspectives and degrees of abstraction in the description of a system and to represent shifts in contexts of purpose. These abilities are crucial for handling semantic complexity.

It is also argued by Rasmussen [3] in relation to operator support systems for complex process plants that there is a motivation for utilizing functional models based on the fact that this type of knowledge is closely related to the way operators conceive the process being supervised.

In this section, literature related to the functional concepts and functional modeling methodologies is reviewed.

### 2.2.1 Functional concepts

Functional and means-end concept are often used intuitively in all engineering domain. But to apply the concepts for modeling, formalization is required. AH [3] provide a general framework to represent complex system at different abstraction levels by using functional concepts. For each of the abstraction level, functional concepts can be decomposed in the part-whole dimension. This is the key contribution to the pioneering research development to use functional concepts for modeling complex work domains.

However, the concepts of functions and purposes which are used in AH has their ambiguity and the means-end relation proposed in AH also lack explicit explanation. Lind [38] analyzed the problem with applying AH for modeling activities and emphasize that it is not possible to derive knowledge about the functional organization of a complex system from an analysis of its physical constitution alone. Functions are inextricably connected with goals and acquiring knowledge of system functions presupposes knowledge of a particular goal context.

### 2.2.1.1 Functions

Lind [46] identified four aspects of the concept of a function in an engineering domain.

#### **Functions are social facts**

Functions are ascribed to items or systems depending on the interest of a user. They are subjective in an ontological sense but objective in an epistemic sense because having a function is a fact which cannot be disputed. This is to say that one has a function of a certain kind is true according to the knowledge shared by a community of designers and users. These types of facts are intersubjective and are called social facts by Searle [48] and distinguished from (physical) brute facts which are objective. This social aspect of functions reflects their dependence on purposes or goals.

#### **Functions are relative to goals**

Function is not an intrinsic property of a physical structure but is related to a particular intention or goal by its user. The same physical object can be ascribed with different functions in different goal contexts. This suggests that functions are concepts that relative to the users' intention. It is not meaningful to discuss functions without their goal context.

#### **Functions represent the static aspect of system compare with roles**

Functions should be distinguished from the concept of roles, where function implies the dynamic aspects of the physical system (changes), while roles implies the static aspects of the functions. During the course of function realization, function implies the change that introduce by a certain action through its preparation to its execution and eventualization, while roles are the abstract features which will persist during all action phases.

#### **Functions are realized by structure with certain disposition**

When functions is ascribed to physical structures, they must have the capability of realizing it. That is to say functions and roles of entities are dependent on the physical structures' dispositions. (The disposition of an item includes all possible ways it could interact with the environment, its functions and roles is a subset of its dispositions.)

### 2.2.1.2 Means-end structure

With this understanding of the concept of a function, Lind [49] abstract the means-end representation independently of the means-end structure in AH. In a means-end relation the different aspects of the means-end relation connect the

means for action (the structure and the dispositions) with the potentials and opportunities available for action here and now (the roles and the functions) and objectives to be achieved in the future. One important aspect of the means-end concept specified by Lind is that the ordering of the elements (goal, function, and structure) in the means-end relation should not be seen as forming a hierarchy. A hierarchy would imply that the elements were ordered according to a principle of subordination, but this is not always the case. As indicated, the ordering has temporal aspects but is fundamentally related to the distinction between the potential and the actualization of an action.

Lind [46] also mentions that in modeling complex system, usually several means-end related activities need to be modeled. Therefore, the interrelations between different means-end relations (from physical structure to goal) need to be considered. Lind suggests that the goals in means-end relations can be defined differently, so that one means-end relation can link to one of the elements in another means-end relation through its goal. There are four different kinds of goals according to Lind.

- to achieve the state produced by the action/function;
- to execute the function or serve a role;
- to enable another function or role;
- to produce a structural means for another function ...

Figure 2.2 shows the means-end relation and means-end structure.

## 2.2.2 Functional modeling methodologies

### 2.2.2.1 Goal-Tree-Success-Tree

Goal Tree-Success Tree (GTST) method proposed by Modarres [50] is a deep knowledge approach that was devised to represent complex dynamic domain knowledge. This approach can model the underlying principles of a given process domain in a hierarchical way. GT identifies the hierarchy of the qualities of the system and decomposing the system objectives in the means-end dimension, representing the functions which support the system goals. Both main and support functions, are considered in GT. The main functions are functions directly involved in achieving the goal, whereas, the support functions are needed to support and realize the main functions. For example, the goal function of safely

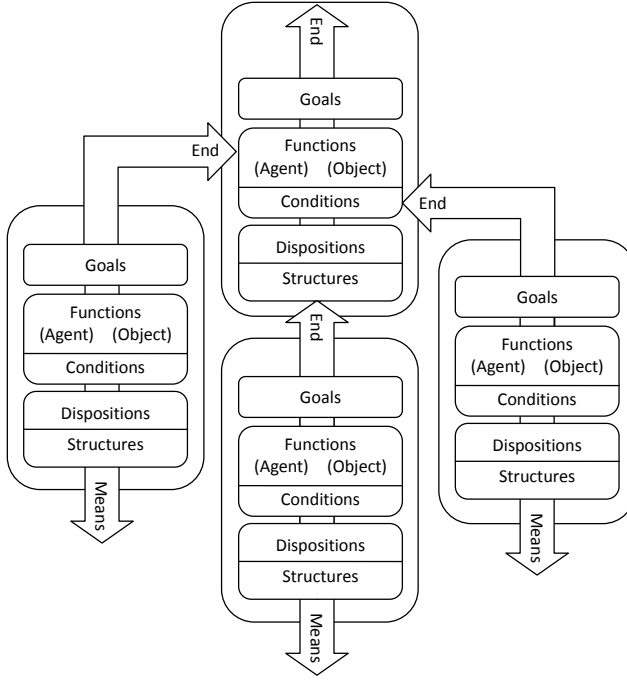


Figure 2.2: Means-end structure. [46]

generating electric power in a nuclear power plant is attained by a combination of many functions as heat generation, heat transportation, emergency heat transportation, heat to mechanical energy transformation, mechanical to electrical energy transformation. Each of these functions then require the support of other functions. [51] ST represents the hierarchy of the objects of the system and decomposes the system along the part-whole dimension, building from the whole system to the parts necessary to attain the last levels of the GT. This hierarchy is built identifying the elements that are part of the parent objects. As for the GT, two types of objects are distinguished: main and support objects. The first ones are directly needed to achieve the main functions, whereas the second ones are needed for the operation of the main objects. [50] For example, generating power plants, electric power transmission and distribution networks are the support objects to provide ac power to a pump.

Hu and Modarres [52] proposed to use GTST combine with the Dynamic Master Logic Diagram (DMLD) for representing full-scale time-dependent behavior and uncertain behavior of complex physical systems. The DMLD is an extension of the Master Logic Diagram (MLD) to model the dynamic behavior of

a physical system. It identifies the interactions between parts, functions and parts and functions, in the form of a dependency matrix and it adds the dynamic aspect by introducing time-dependent fuzzy logic. Ferrario and Zio [53] adapted the GTST-DMLD framework for developing safety assessment method. A similar framework including the GTST-MPLD (Master Plant Logic Diagram) framework proposed by Modarres.

However, GTST model does not equip with systematic graphical representation that can be used and the model is largely depends on system descriptions. There is a lack of semantic foundation and formalization of the methods. GTST model alone does not support formalized analysis method for reasoning and inference.

### 2.2.2.2 Function block diagram

A Functional Block Diagram (FBD) [54] in systems engineering and software engineering is a block diagram, which describes the functions and interrelationships of a system. The FBD has four components:

- Functions of a system pictured by blocks,
- input and output elements of a block pictured with lines and,
- the relationships between the functions,
- the functional sequences and paths for matter and or signals.

FBD can be combined with flow charts to be developed in a specific type of diagrams called Functional Flow Block Diagram (FFBD). The FFBD approach is originated from 1950s, [54] as a multi-tier, time-sequenced, step-by-step flow diagram of a system's functional flow. FFBDs show the same tasks identified through functional (part-whole) decompositions as FBD and display the function blocks with logical, sequential relationship to connect them. Each functional block in FFBDs must be linked with logic symbols to represent the relations between functions.

FBD is different from the other functional modeling approaches in a sense that it does not emphasize the functional concepts of the system (such as goals and functions). FBD does not offer abstraction representations as Functional models usually do, although it is commonly considered as one of the functional modeling approach. In FBD, functions are viewed as simple input-output blocks and can only represent the connectivity between subfunctions rather than deal with the means-end decomposition and abstraction.

### 2.2.2.3 Multilevel flow modeling

Multilevel Flow Modeling (MFM) is a methodology for modeling of industrial processes on several interconnected levels of means and part-whole abstractions. The basic idea of MFM is to represent an industrial plant as a system which provides the means required to serve purposes in its environment. MFM has a primary focus on representation of plant goals and functions and provides a methodological way of using those concepts to represent complex industrial plant. [55]

The development of the conceptual foundations of MFM modeling language, the tools and applications have been ongoing for more than two decades. The basic ideas of MFM were conceived by Lind [56] and developed over the years by his and other research groups. The research is originated from Rasmussen's AH, and attempts to solve problems related to representing complex systems in human machine interfaces for supervisory control by adopting the idea of means-end structure and abstraction. But later on MFM has been further developed into a broader research field dealing with modeling for design and operation of engineered systems, and try to tackle the fundamental representation problems. [38]

### 2.2.2.4 Other modeling methodology

Function Flow Diagram (FFD) is a very similar functional modeling method with FBD/FFBD. FFD is a network representation of the system which portrays the system in terms of its component functions and the logical interdependencies or flows between the functions. FFD is also not an ideal approach for modeling complex system for the purpose of situation assessment because it suffers the same problem with FBD.

Marcos [57] proposes to use a functional modeling approach called D-higraph to represent a complex system by capturing both the functional and the structural aspects of the process plants. D-higraphs are an extension of an existing formalism called Higraphs, which can be understood as a combination and extension of conventional Directed Graphs and Euler/Venn diagrams. Mata et al. [58] proposed methods for applying D-higraphs to diagnose abnormal situations. Although the logical structure of D-higraphs can enable reasoning and inferences, however, the method does not give a lot of input on modeling the semantic complexity of the engineered system.

MFM modeling is chosen to be the fundamental modeling methodology for the

project, because of the following points:

- it is the method that has the ability to approach the complexity issue for representing complex system for cognition purposes;
- MFM models causality between different functions and goals which provide the user a systematic way to conduct causal reasoning by using developed models;
- MFM also developed a set of control functions, which describe the control intentions together with the process model. [59] This Modeling approach covers the conceptual requirements for knowledge representation in this study.

A more detailed review on MFM research is provided in Section 2.3.

## 2.3 Current MFM theory

As mention previously, MFM is a modeling methodology for representing complex systems at different abstraction level of specifications. It has been used for modeling engineering system in several safety critical domains such as nuclear power plant [60] [61] and chemical engineering system [62] [61]. The conceptual foundations, the development of MFM modeling language, tools, and applications have been undergoing for more than two decades. The most recent introduction for MFM can be found in [55] [63].

The further development of MFM theory is an undergoing project which also includes the present PhD project. A most recent version of MFM is introduced in this section. Most of the review content is based on the [55]. However, certain changes are made because of the updates from the research since 2011, and the changes will be specified in the following text.

### 2.3.1 MFM concepts



#### 2.3.1.1 Objective and threats

MFM distinguishes between system goals in two different categories based on the nature of the concepts. One is to achieve a certain state, while the other



is to avoid an undesirable state. These two can be expressed by using only one concept of goal with different logical expressions. However, the differentiation between the two concepts is the key to understand safety issues of complex system. Goals in MFM is not expressed only by the target states only, but has to be expressed by using target together with a means-end relation (will be introduced later). Table 2.1 shows the MFM symbols for MFM goal target.

Table 2.1: Definition of MFM targets.

Terminology	Symbol	Definition
objective	obj1 	An objective represents a desirable state which should be produced or maintained.
threat	thr1 	A threat represents an undesirable state which should be destroyed or suppressed.

2.3.1.2 Flow functions

In contrast to other functional modeling methodologies, MFM adopts a specific functional ontology. In MFM functions are defined in relation to the processing of flows of mass and energy. MFM is based on a set of six generic flow functions representing different primitive operations performed on either mass or energy flow. The list of MFM flow functions are shown in Table 2.2 and 2.3.

Flow functions in MFM are not isolated. They has to be included in a function structure. In MFM, a function structure represents a set of functions connected by causal relations. A function structure can contain mass and energy flow functions and control functions. Three subtypes of are therefore distinguished: mass flow structures, energy flow structures and control flow structures.





2.3.1.3 Causal relations

Causal relation in MFM specifies the causality between MFM flow functions. The terminology of MFM causal relations is specified in Table 2.4.

2.3.1.4 Means-end relations

There are two types of means-end relations. The first type of means-end relation should be link to MFM target to form description of objectives in the model.



Table 2.2: Definition of MFM flow functions. (1)

Terminology	Symbol	Definition
Source		A source represents the function of a system serving as an infinite reservoir of mass or energy. No physically realizable has in principle unlimited capability to deliver mass or energy. However, the source function is used to provide an adequate abstraction of the physical phenomena considered.
Sink		A sink represents the function of a system serving as an infinite drain of mass or energy. As for the source function, this function can be used in many cases as an adequate abstraction.
Storage		A storage represents a system which serves as an accumulator of mass or energy. A storage function can have any number of connections and any number of enabling conditions. An example could be the function of a tank when used as a device for accumulation of a fluid, in this example we are dealing with a mass storage. Another example could be the storage of energy in a boiler by heating the water.
Balance		A balance represents the function of a system which provides a balance between the total rates of incoming and outgoing flows. Each balance function can have any number of connections and any number of conditions

These relations includes *produce*, *maintain*, *destroy*, and *suppress* and the end of these relations is a MFM target. The second type of means-end relation including producer-product (pp) relation and mediate relation is used to describe the relation between function and a goal function. The second type of means-end relation indicates a direct shift of perspective of function structure. These relations are used when the function structure realize a functional end (activity) rather than a target state. These relations include *producer-product* and *mediate* and the end of these relations is a MFM function. The list of Means-end relations is shown in Table 2.5.

It should be noticed that the means-end relation together with the target state, for example “to produce an object” is the “end” in the means-end relation, and the function structure is the means to achieve the end.

Table 2.3: Definition of MFM flow functions. (2)

Terminology	Symbol	Definition
Transport		A transport represents the function of a system transferring mass or energy between two systems or locations. A transport function has one upstream and one downstream connection to an influence relation. The downstream connection point is indicated by the arrow head representing the direction of flow. Note that the flow direction is not identical to the directions defined by the influence relations.
Barrier		A barrier represents the function of a system that prevents the transfer of mass or energy between two systems or locations. Typical examples of systems which implement barrier functions are the cladding on nuclear fuel rods, heat isolating material and a trap in water systems



### 2.3.1.5 Conditional relations

The fulfillment of an objective and emerge of a threat could disable or enable a flow function. A condition relation which is a special means-end relation (interactivity-relation), describes the relation between a flow function which may be enabled by an objective or disabled by the threat. The definition of conditional relations are shown in Table 2.6. Although that these two relations is defined together in [55] with the MFM control relation actuation (which will be introduced in the next section), these two should be distinguished from the actuation relation. This is because the condition can only be realized by objective fulfillment in a means-end structure. The control functions can “actuate” on the condition of a function rather than has a direct relation to serve as condition for a function realization.

### 2.3.1.6 Control function and control relations

Von Wright’s action types and the extensions with descriptions proposed by Lind [64] provide a formal foundation for the definition of elementary control functions. The introduction to how the control functions are introduced in the MFM ontology is provided in [59]. The control function and control relations are listed in Table 2.7.

Table 2.4: Definition of MFM causal relations.

Terminology	Symbol	Definition
Influencer		A flow function F (source, sink, storage or balance) is connected with a transport T upstream or downstream with an influencer relation if it has the role of influencing the amount of substance transported by T.
Participant		A flow function F (source, sink, storage or balance) is connected with a transport T upstream or downstream with a participant relation if the system realizing F has the role of passively providing or receiving substance for the transport T.

### 2.3.1.7 Roles and structures

The existing MFM concepts also includes the lower level in the mean-end structure. The concept of roles and structures is used to link the functional representation to the physical system. However, MFM ontology on both roles and structures is not solidly defined, thus there is no agreeable MFM concepts is implemented in the current modeling tool.

Previous researchers who adopted MFM methodology often use a direct approach to associate physical structures with MFM functions. [] However this is not an elegant solution to solve the problem because the relation between physical structure and system function has to be supported by fundamental means-end theory.

Lind [65] introduced a preliminary analysis for extending MFM functions to enable the representation of roles. MFM roles are defined in relation between physical structure and the function, which is clearly suggested in the means-end structure. Wu [66] identified the need for the roles that need to be introduced in MFM models for chemical engineering applications. She also proposed four roles namely: object, agent, patient, instrument to model system functions so that the developed model can be used in HAZOP analysis with the complete set of guide words. However, to include roles in MFM models is still a challenge.

With the absence of a definite role ontology in the current MFM methodology, this thesis try to abridge the structure-function relation through state evaluation rather than trying to define the structure-function relation.

### 2.3.2 MFM reasoning

Because MFM models a complex systems' objectives and functions with different type of relations, the developed model can be used to analyze the dependency relations between different functions and objectives. Reasoning with MFM models is based on cause-effect relations which are generic i.e. independent of the particular modeling object. MFM is therefore very effective for building knowledge bases for model based expert systems. The need to develop rules for reasoning about causes and effect which is a characteristic of rule based systems is eliminated entirely and the effort is reduced to building the MFM.

The cause-effect relations are associated with goal-function and function-function patterns in MFM models. These patterns are defined by influence relations interconnecting the flow functions within the flow structures and the means-end relations making connections between flow structures. For each of the influence relations and the means-end relations there is a corresponding set of cause-effect relations relating a state of a function or goal with the state of another function or goal in the model. These generic cause-effect relations can be implemented as a rule base system for MFM reasoning.

Petersen [2] has developed a set of rules using an earlier version of MFM ontology where the causal relations are defined differently from the present thesis. To support comprehensive reasoning of MFM, the causal relation has been further developed in recent years. Lind introduces the new causal reasoning foundation in [67]. In this thesis, the MFM causal reasoning will be re-examined in context of norm and fault occurrence to extend on the MFM reasoning algorithm implemented before 2012.

### 2.3.3 Tools and application

MFM methodology has well defined graphical symbols, and MFM models can be built by using computerized tools. Petersen [2] has implemented a MFM model builder prototype in a G2 system for using the same platform to develop expert system for reasoning about the root causes of disturbances by using MFM models.

Lind and his research group later developed a Microsoft Visio template for MFM model building process. And another software which is called MFMWorkbench is developed by using Java Expert system Shell (Jess) to reason about root causes after the MFM models have been developed in Microsoft Visio.

Recently, Thunem et al. [68, 69] has developed a Java-based program MFM-Editor which offers a friendlier user environment for MFM model building. And MFM-Editor is later updated as MFM Suite which is developed in relation with this PhD project [70]. The author of this thesis has been developing the reasoning package which can be plug-in the MFM Suite as analysis tool box for Reasoning about causes and consequences. A screen shot is provided in Figure 2.3.

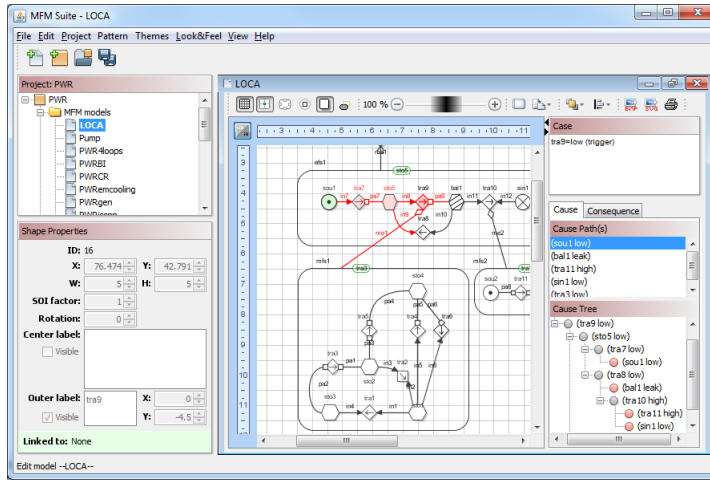


Figure 2.3: Screen shot of MFM Suite.

Table 2.5: Definition of MFM means-end relations.







Terminology	Symbol	Definition
produce		A produce relation connects an objective with a function structure if one or several functions in the structure contribute to produce the objective.
maintain		A maintain relation connects an objective with a function structure if one or several functions in the structure contribute to maintain the objective.
suppress		A suppress relation connects a threat with a function structure if one or several functions in the structure contribute to suppress the objective.
destroy		A destroy relation connects an threat with a function structure if one or several functions in the structure contribute to destroy the objective
pp		A transport represents the function of a system transferring mass or energy between two systems or locations. A transport function has one upstream and one downstream connection to an influence relation. The downstream connection point is indicated by the arrow head representing the direction of flow. Note that the flow direction is not identical to the directions defined by the influence relations.
mediate		A barrier represents the function of a system that prevents the transfer of mass or energy between two systems or locations. Typical examples of systems which implement barrier functions are the cladding on nuclear fuel rods, heat isolating material and a trap in water systems

Table 2.6: Definition of MFM conditional relations.








Terminology	Symbol	Definition
enable		An enable relation connects a function with an objective. It is used when the function is enabled when the objective is satisfied. All functions can be enabled.
disable		A disable relation connects a function with a threat. It is used when the function is disabled when the threat is emerged. All functions can be disabled.

Table 2.7: Definition of MFM control functions and actuation relation.

Terminology	Symbol	Definition
Steer		To steer is the function of a system which is producing a new state in the controlled system.
trip		To trip is the function of a system which is destroying an actual state of the controlled system.
regulate		To regulate is the function of a system which is maintaining an actual state of the controlled system.
suppress		To suppress is the function of a system which is suppressing a potential new state of the controlled system.
actuation		An actuation relation connects a control function with a function structure containing a flow function which is the direct object of control.



## 2.4 Chapter summary

This chapter reviewed the problem or situations assessment posed in the operation in complex industrial plants. It is important to note that although the situation awareness is a subjective concept which require the precise mental model of a situation in the minds of operators, the knowledge source of for operators to generate such a mental model is objective and lies in the system that they are interacting with.

Therefore, it is important to abstract the knowledge of the system situation in a representation which is most suitable to human perception. The choice of modeling methodology is crucial to enable the development of support system for situation assessment and situation awareness.

Human understanding of the situation and their generated intentional behaviors are based upon the functionalities and the design intentions of the system itself. Functional modeling approach is a great tool to model system goal function aspects and can handle the system complexity at the same time because it adopted the means-end structure. Thus the FM approach should be adopted as modeling method for situation assessment to facilitate human cognitive activities. MFM as a mature functional modeling methodology is equipped with the capability of covering all aspects for the purpose of supporting situation assessment in complex systems. However the modeling concepts and reasoning strategies of MFM need to be extended to fulfill the operator support tasks.

MFM has been adopted for various modeling applications, the literature about MFM modeling procedure and syntax is rare and scattered. The next chapter will introduce the detailed MFM modeling syntax and procedure, and use sufficient examples to demonstrate the modeling techniques.

## CHAPTER 3

# MFM Modeling Procedure and the PWR Model

---

Readers can get some insights of how to built MFM models for the process by previous literatures [2, 55, 71]. Huessen and Lind [59, 72] explains how to model the control function on top of the process model. However, there's no comprehensive instructions for modeling by using the latest developed MFM modeling ontology and syntax. The purpose of this section is to introduce the present version of the modeling technique.

The Chapter will start with a detailed explanation of the MFM syntax and using partial models to explain how to use MFM functions to represent different physical structures in Section 3.1. A small example of how to model a thermal power plant at a very abstract level will be explained. And a procedure for MFM modeling is summarized. Section 3.2 will be dedicated to explain a model of a PWR primary system in a fairly detailed representation. Section 3.3 concludes this chapter.

## 3.1 MFM modeling procedure

### 3.1.1 MFM syntax

As already introduced in Section 2.3, MFM represents a complex system by using both means-end and part-whole decompositions. Along the means-end dimensions, MFM represents a system in terms of objectives and flow functions

at different levels of abstractions. And each of the flow-structures in an MFM model includes a set of different flow functions which decompose a function structure in the part-whole dimension. Control functions and control objectives are independent of the process model but are linked to the process model by control relations. Sometimes, adding control functions to the process model may impose changes to the flow functions. Examples will be provided shortly.

As opposed to the functional modeling methodologies such as GTST [22], MFM has a well-defined ontology rooted in action theory and regarding mass and energy flow balance which based upon using first principle phenomenological information to represent internal process and system relations.

#### 3.1.1.1 Flow functions

In an MFM model, flow functions do not exist outside their flow structures. The flow structure indicates whether the function included is a mass flow function or a energy flow function. Inside of each flow structures, flow functions are never isolated but has to be connected with other flow functions. While source and sink functions represent the boundaries of a flow structure, meaning that the flow in this function structure enters from the source and disappear from the sink. The mass or energy flows beyond the source and sink function is not of concern in a particular flow structure. The storage functions represent the storage capability inside a flow structure, while the balance functions represent the system's capability of balancing the total inflow rate and out flow rate. All the source, sink, storage, and balance functions are separated in physical space within a flow structure, thus all the functions has to be connected through transport functions (or barrier functions) to form a flow structure. Because the transport or barrier function are the only functions represent the mass or energy flow should or should not go from one stationary function to another. The arrows inside a transport function indicates the flow direction. Therefore, for each of the flow functions, one must distinguish between the in-port (upstream) connection and the out-port (downstream) connection.

The function connection rules are illustrated in Table 3.1 below.

#### 3.1.1.2 MFM relations

The four type of relations in MFM should also be used by following the MFM syntax introduced in the following sections.

Table 3.1: The connection syntax of between flow functions.  
(sto/bal is abbreviation for storage or balance)

Flow Functions	(Num. of)In-port	(Num. of)Out-port
source	(0)n/a	(1)transport
sink	(1)transport	(0)n/a
transport	(1)source/sto/bal	(1)sink/sto/bal
barrier	(1)sto/bal	(1)sto/bal
sto/bal	(1-n)transport	(1-n)transport

### Causal relations

Causal relations should be used in two different occasions. Firstly, they should be used between different flow functions to indicate the causality between them. Because the nature of flow function connections, the transport or barrier function will always be causal to both its in-port connection and out-port connection. Therefore, the causal relations that used between flow functions only indicate that whether there is a active influence by flow functions of source, sink, storage, or balance to the connected flow functions of transport or barrier. If a transport or barrier function is influenced from the in-port connection or out-port connection, an arrow (influencer relation) should be marked at the connection port, otherwise, a box (participant relation) should be marked at the connection port. The second usage of the causal relation is to indicate whether there is a influence relation from a control objective to its control function.

Table 3.2: The syntax of causal relations.

Causal relations	start	end
influencer	source/sink/storage/balance	transport/barrier
participant	source/sink/storage/balance	transport/barrier

### Means-end relations

MFM distinguishes between two types of means-end relations.

One type is the means-end relations that used between a target (objective or threat) and a flow function, which indicates that the target is the end that is realized by using the function as a means through the specific means-end relation. These relations includes produce, maintain, suppress, and destroy. The purpose of distinguishing between the four relations is to make sufficient expression of the models semantic meanings to enable reasoning and explaining

a situation. Therefore, the four relations has to be used according to the MFM syntax. Produce and maintain have to be used between a flow function with a positive target (an objective), while suppress and destroy have to be used between a flow function with a negative target (a threat).

The second type of means-end relations are used between flow functions in different flow structures that represent different abstraction levels.

Table 3.3: The syntax of means-end relations.

<b>Means-end relations</b>	<b>start</b>	<b>end</b>
produce/maintain	flow function	objective
suppress/destroy	flow function	threat
pp/mediate	flow function	flow function

In MFM terminology, all the functions that are linked to the start of the means-end relations is called main function. Semantically, one flow structure in a whole is the means to realize a target objective or a purposeful function. However, MFM means-end relation links the function which is directly responsible for the change of status of targets or states of the purposeful function in another flow structure is tagged as main function in the means flow structure. The syntax serves the purpose to organize causal reasoning which will be explained in detail in Chapter 4.

### Conditional relations

A conditional relation is used to link a target to a flow function, which indicates that the target state is the pre-condition for enabling or disabling a flow function at another abstraction level.

Table 3.4: The syntax of conditional relations.

<b>conditional relations</b>	<b>start</b>	<b>end</b>
enable	objective	flow function
disable	threat	flow function

### Control relations

Control relations are the actuation relations from a control function to a flow function. The actuation relations can have three different meanings including adjusting, enabling and disabling.

Table 3.5: The syntax of control relations.

control relations	start	end
actuation	control function	flow function

3.1.2 Modeling Mass and Energy Flow with causal relations

Source functions

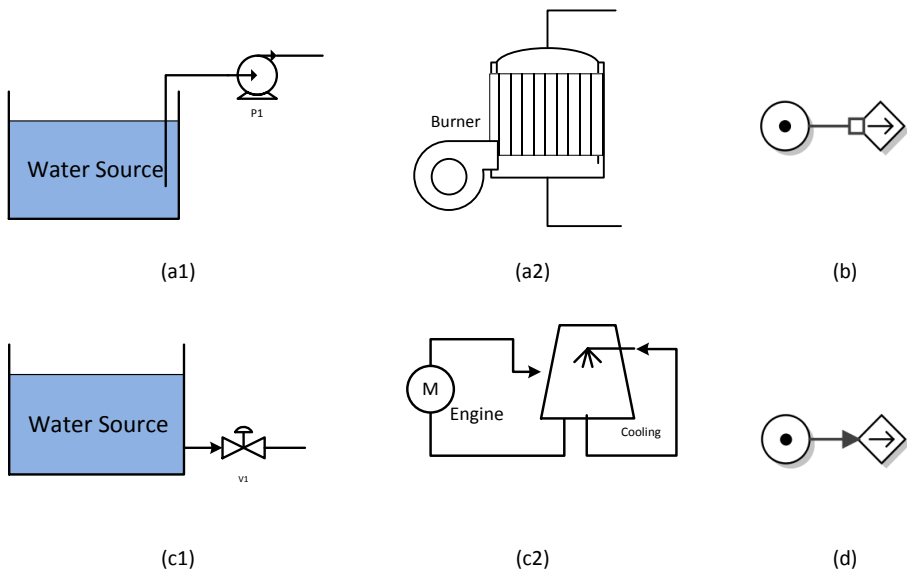


Figure 3.1: Model source functions

As stated in the function definition in Section 2.3, there is no physical structure can provide infinite mass or energy, thus in practical modeling, the source function represent the inflow boundaries. To enable reasoning about the abnormality of a source function later in Chapter 4, any quantity of mass or energy can be represented as source depending on the modeling perspective. Consider the physical components in Figure 3.1(a1), a water tank connected with an outlet pipeline. The function of the physical structure can be considered as a mass source connected with a transport function, as shown in Figure 3.1(b). The influencer relation indicates that the states of the source function has a influence to the transport function. Compare Figure 3.1(a1) with Figure 3.1(c1), an obvious difference is that the water flow rate which is transported out of a

source function is regulated by the pump rather than influenced by the states of the available water source. In this case, the physical structure in Figure 3.1(c1) has to be modeled as in Figure 3.1(d) according to MFM syntax.

The physical components in Figure 3.1(a2) shows a burner which is used to boil water in the boiler. Consider the energy balance, that the burner has a function of energy source to produce heat. The energy source clearly influence how much heat is transported out of the source. Therefore, the physical structure in Figure 3.1(a2) can also be represented by using MFM flow function in Figure 3.1(b) within an energy flow structure. Figure 3.1(c2) shows a engine cooling loop. The energy flow in this context is the heat transported from the heated engine to the cooling tower. This small system can also be represented by using a energy source and transport function. Compare Figure 3.1(c2) with Figure 3.1(a2), the difference is that in Figure 3.1(c2), the coolant flow control the energy flow rate while the energy source (heated engine) does not. Therefore, Figure 3.1(c2) can be represented as Figure 3.1(d) by using MFM flow functions in a energy flow structure.

We define a source with a participant role is a potential source, where a source with an influencer role is a current source.

### Sink functions

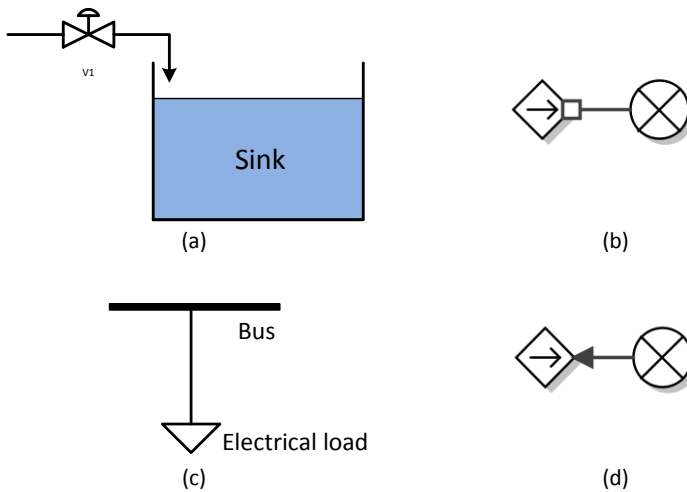


Figure 3.2: Model sink functions.

Similarly to the source, there are two type of sinks. According to the semantic meaning of a sink function, normally we do not consider the volume of a sink. This means that in most systems, a sink function do not influence its upstream transport function. Figure 3.2(a) shows a sink example which can be modeled in MFM by using Figure 3.2(b) in a mass flow structure.

However in some energy flow structure, energy sinks do influence the transports which are connected to the them. Consider the electrical load which is connected to a distribution network in Figure 3.2(c), the state of the load directly influence how much energy is transported into it. The load cannot be modeled as storage function because the energy flows is not stored. Electrical loads certainly have the function of an energy sink thus they can be represent in MFM as energy sinks but with a influencer role to its upstream transport. Figure 3.2(c) can be represented by using the MFM functions in Figure 3.2(d) in an energy flow structure.

### Storage functions

Any component who has a volume of capacity to store mass or energy (or both) can serve the function of storage, thus it can be represented by a storage function in MFM. Figure 3.3(a) illustrates four different layouts for the in-port and out-port connections of a water tank. The difference rests on fact that whether the level inside the water tank influence the in and out flow rate in the system. All the layouts can be represents with transport-storage-transport connections, with the storage serving different causal roles to its upstream and downstream transport functions. The MFM representation of the mass flow function of Figure 3.3(a) is shown in Figure 3.3(b).

One can also consider that the water tank as an energy storage for the water it contains can carry energy (for example in form of heat). Thus the function of the water tank can also be represented by using the same MFM function in Figure 3.3(b) but in an energy flow structure. During MFM modeling, physical components can realize several different functions in both mass and energy flow. Those functions that are realized by the same physical components viewed from different perspective often have means end relations as well. In the case of the water tank example, the mass storage function mediate the energy storage function of the water tank. This relations can be represented by the MFM model in Figure 3.3(c).

Note that a storage function can have multiple transport functions connected to either the in-port or the out-port of the storage functions as the physical component of a storage tank can have multiple inlets.



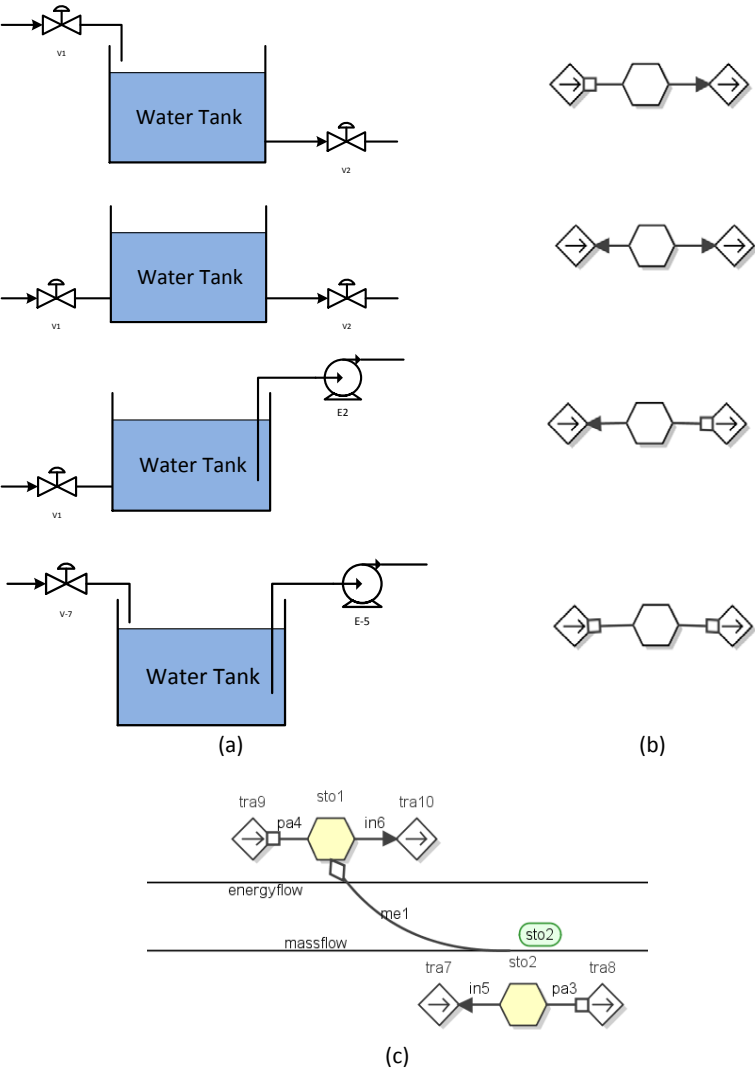


Figure 3.3: Model storage functions.

Balance functions

Balance is a function to maintain the equalization of the input and output flow rate. A balance can have multiple upstream and downstream transport functions connected to it. The balance function is achieved by either matching the input flow rate to the output flow rate, or matching the output flow rate to the input

flow rate. Therefore, at least one influencer role has to be attached to a balance function, meaning at least one transport function has to be influenced by the balance function. Otherwise, the balance function has no means to balance the flow, which suggests that the balance function does not exist.

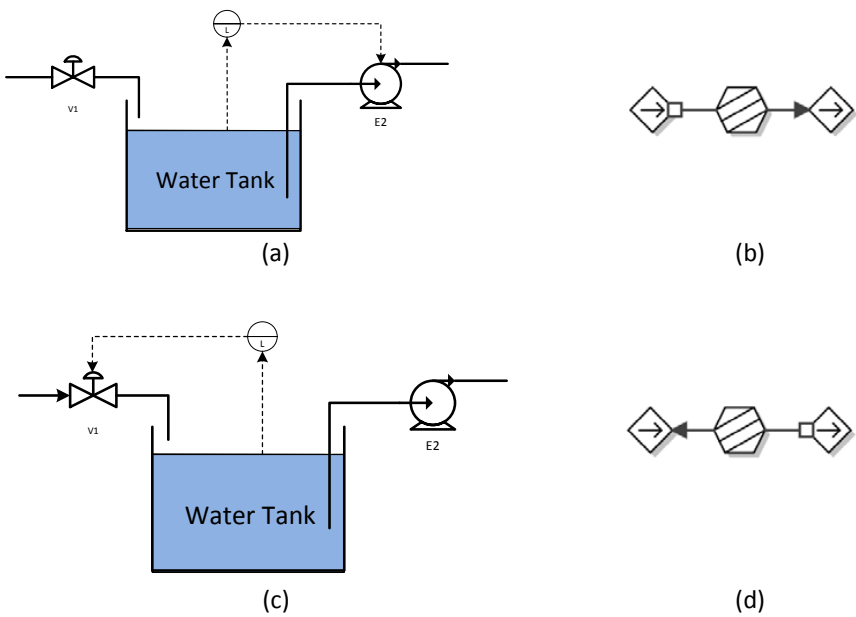


Figure 3.4: Model balance function.(1)

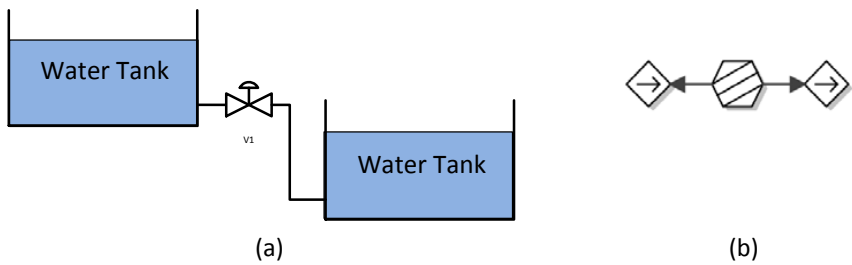


Figure 3.5: Model balance function.(2)

Considering the physical system shown in Figure 3.4(a) where a water tank is connected with one inlet and one outlet. It is quite similar to the layout of the example in Figure 3.3, except that there is a controller to maintain the level of liquid in the tank constant by manipulating the outlet pump. To model

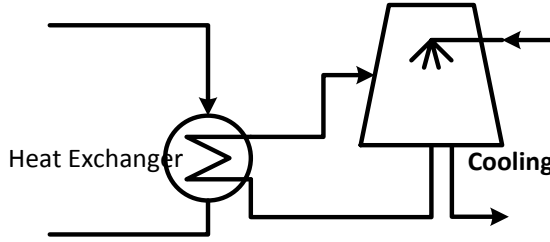


Figure 3.6: Model balance function.(3)

the mass flow of this physical system, we should consider the tank has a flow balance function because the purpose of which is to maintain constant level and the means of achieving this is to use the automatic control to match the outlet flow with the inlet flow. In MFM modeling this system can be modeled as in Figure 3.4(b) in a mass flow structure.

Consider a similar system in Figure 3.4(c), instead of having the controller manipulate the outlet pump as in Figure 3.4(a), assuming the controller can control the inlet flow to match the outlet. The MFM mass flow model is shown in Figure 3.4(d).

If two water tanks are connected in series by using a section of pipeline. The first water tank is physically located higher than the lower tank to insure a constant flow direction. In Figure 3.5(a), the pipe has a balancing function which matches the water outlet rate in the first tank with the water inlet rate in the second tank. This Physical layout can be modeled in as shown in Figure 3.5(b).

Another energy balance example is shown in Figure 3.6. The physical system is a heat exchanger in a cooling loop. The heat exchanger has the function of balancing the heat transport between two loops.

## Control Functions

Consider the physical system in Figure 3.4(a), if there is a need to model the controller's function separately and not including it as part of the process, the physical system can also be modeled as in Figure 3.7, with explicit control functions represented in the MFM model. The control objective is to maintain level (volume) inside the water tank, the means for the controller to control the

level is to actuate on the outlet pump.

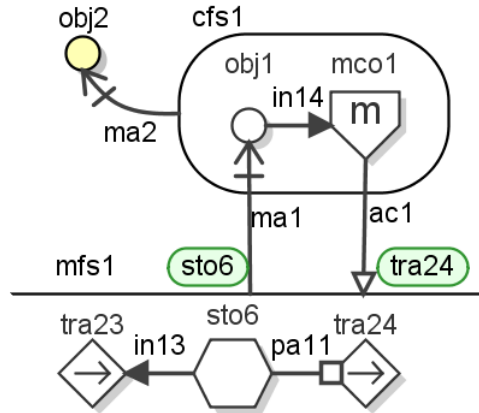


Figure 3.7: Modeling control functions.

### 3.1.3 MFM model of simple heating system

In this section, an small modeling example will be demonstrated. The subject of modeling is shown in Figure 3.8.

In Figure 3.8, different level of system goal is summarized and the goal is translated in terms of MFM objectives. Among the objectives, maintaining temperature is the main concern of the system functionality.

In the MFM methodology, the first consideration is how the main objective is achieved. The temperature is clearly related to the energy flow functions which are realized by the physical structure. Figure 3.9 shows the general consideration by adopting the means-end decomposition of the system. The temperature is maintained, by the heat energy flow from the burner to the radiator, and then dissipated to the environment. This is modeled in the energy flow structure *efs1*. MFM function *soul1* in Figure 3.9 represent the function of the combustion process as an energy source. According to the previous discussion of the MFM syntax, this energy source is a current source for it controls how much energy is injected into the system. The source function is linked by a transport function to a storage in the system in form of heat (*sto1*). Afterwards, the energy is further transported to the radiator that serves the function of an energy sink (*sin1*).

- G1: Maintain Comfort
- O1: Maintain room temperature at 20 degree
- G2: Ensure that fuel can burn
- O2: Maintain flow ratio within conditions for combustion
- G3: Ensure that pump can rotate
- O3: Maintain oil flow within condition for lubrication
- G4: Ensure that water can move
- O4: Maintain water level above limit

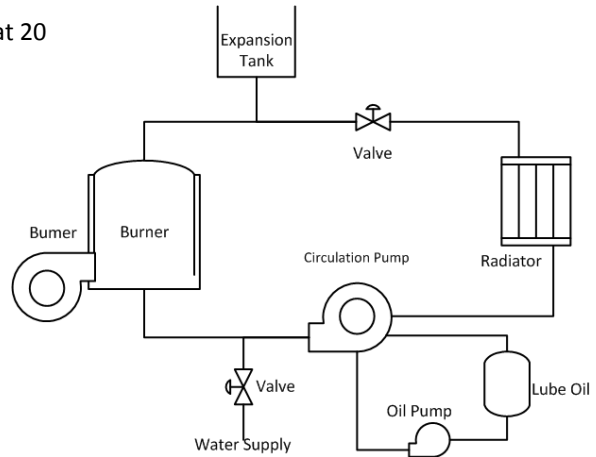


Figure 3.8: The physical layout of a simple heating system.

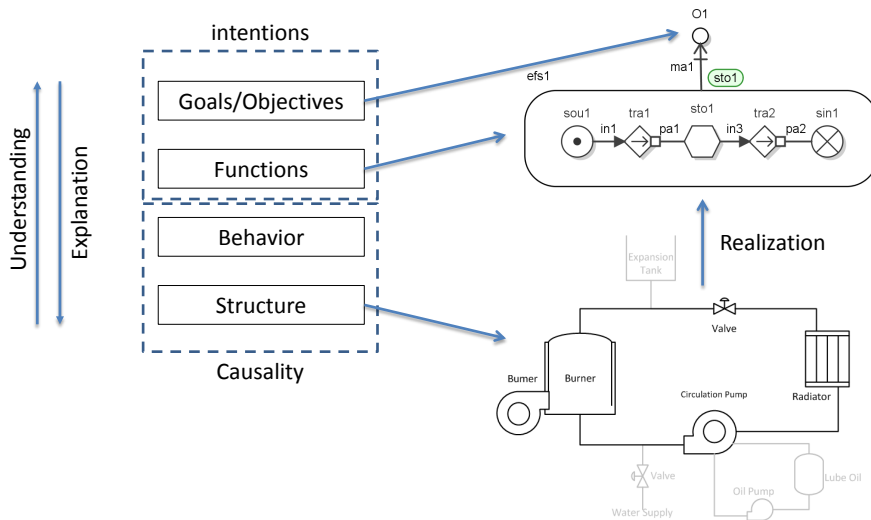


Figure 3.9: Modeling the energy flow structure of a simple heating system.

When the basic energy flow is modeled in the heating system, we can decompose the system function along the means-end dimension, asking questions of how the energy is transported from the burner to the radiator. The answer that the heat

is transported by circulating the water. Further question of how the water is circulated can also be asked, and the answer is by using the pump. If the pump in the system is viewed as a physical component that does not need to consider its inner function, the function modeling procedure ends with the components. However, the pump can be viewed as a system as well, and functions of the pump can also be decomposed into more detailed functional representation. The water is transported by means that of the pump converting electrical energy to kinetic energy. Therefore, the mass flow of water transportation can be modeled as the end of the pumps inner energy flow structure. The modeling procedure is illustrated in Figure 3.10. *mfs1* represents the water flow structure and *efs2* represents the energy flow structure for the pump. In *efs2*, *tra5* represents the energy transport which turns into kinetic energy to move the water, *tra6* represents the energy which turns into heat loss during the operation.

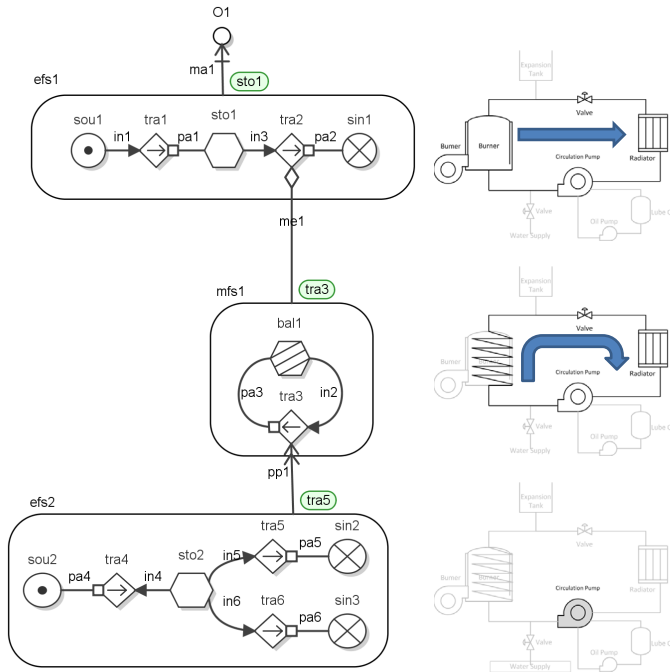


Figure 3.10: MFM model of the simple heating system with three flow structures.

### 3.1.3.1 Level of abstractions

As already experienced, an MFM model can be decomposed along the line of means-end relations. Each function in MFM can be considered to be realized by physical subsystem or components directly. However, it can also be decomposed in the functional representation. This offers great flexibility for MFM to model a complex system in a very abstract way but keep the decomposition capability for exploring the system functionality in detail. The previously developed model in Figure 3.10 can be further decomposed as shown in Figure 3.11

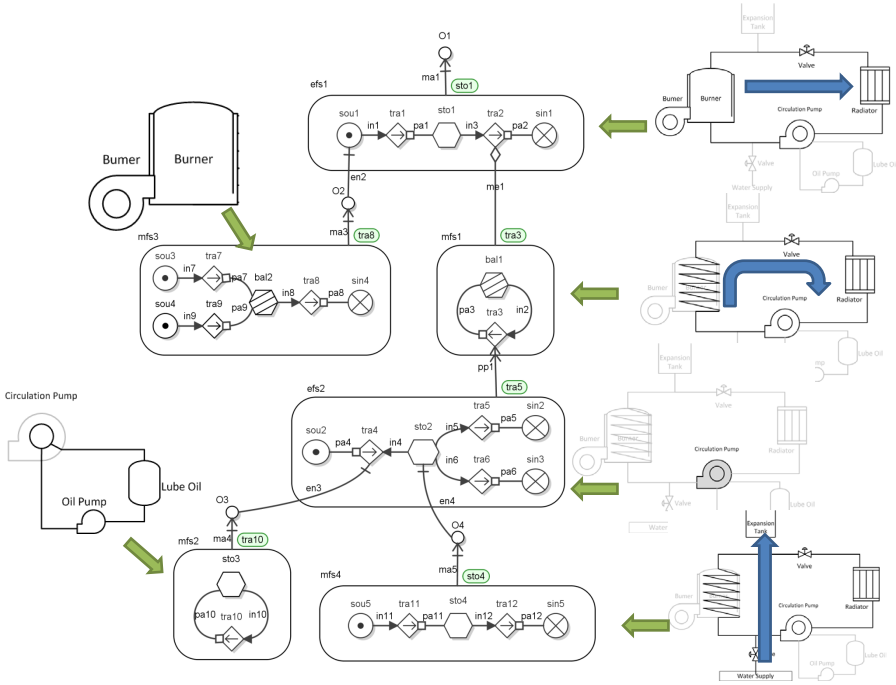


Figure 3.11: Detailed MFM model of the simple heating system.

The function flow structure of the water injection system, pump lubrication system, and the combustion process is added to the model in Figure 3.11. Both the water injection and the pump lubrication serve as conditions for the pump to work properly, and the combustion process serves as condition for the energy source function to be available in the system.

A MFM model can also be decomposed along the part-whole dimension. For example, in the modeling procedure of this simple heating system, the water

circulation (*mfs1*) is modeled without any storage function because when the circulation is considered, the mass flow is perfectly balanced by *bal1* and there is no adding or taking water from the system. However, when the water injection is considered (*mfs4*), the volume of the system has to be considered as a storage function (*sto4*) to represent the functionality of the system. The model aggregation or decomposition can also be seen in the more complex modeling example in the following section.

### 3.1.4 MFM modeling procedure

Lind and Zhang [46] summarized two different modeling approaches to model a system by using MFM. For a modeling activity that involves previous modeling experience, the model can be developed by a decomposition strategy, which is to decompose the physical system into subsystems by determine different mass and energy flows. Then Model each of the subsystems respectively and make connections between subsystem models afterwards by using causal relations or means-end relations. This method may increase the efficiency of the modeling procedure. When the modeling activity is unfamiliar to the modeler, the basic approach has to be adopted. Basic MFM modeling combines both the top down and the bottom up modeling approach. The modeling steps are indicated as below.

- Step 1.** Understand and determine the system objectives and the main mass and energy flows. Analyze the means-end relation between different flow structures and their objectives.
- Step 2.** Identify sources and sinks for each flow structure. Identify storage functions and balance functions between sources and sinks according to the choice of abstraction level. Connect these functions by using transport functions following the MFM syntax. Determine the causal relations between adjacent functions.
- Step 3.** Review the means-end relations between flow structures and identify the main function and the target function for each means-end relation. If the main function or target function cannot be identified precisely due to over-abstraction (lack of detailed function representation in the model), decompose the existing functions and then try to identify the main function or target function again.
- Step 4.** Review the developed model and add extra means-end relations for existing functions if needed.



Note that this modeling procedure is not necessarily to be strictly followed once a modeler is sufficiently familiar with the MFM modeling technique. However it can serve as a general guideline for beginners when first starting to use the methodology.

## 3.2 Primary system of a pressurized water reactor

Pressurized water reactors (PWRs) constitute the large majority of all Western nuclear power plants and are one of three types of light water reactor (LWR), the other types being boiling water reactors (BWRs) and supercritical water reactors (SCWRs). In a PWR, the primary coolant (water) is pumped under high pressure to the reactor core where it is heated by the energy generated by the fission of atoms. The heated water then flows to a steam generator where it transfers its thermal energy to a secondary system where steam is generated and flows to turbines which, in turn, spin an electric generator. In contrast to a boiling water reactor, pressure in the primary coolant loop prevents the water from boiling within the reactor. All LWRs use ordinary water as both coolant and neutron moderator.

PWR can be divided into two major sub-systems, the primary system which transport nuclear energy to generate heat and the secondary system which transfer heat into electric power. In PWR, the mass flow of primary system and of the secondary system is strictly separated to prevent the release of radiation. However, the energy flow of the primary system and secondary system is connected. For demonstration purposes, only the primary system is modeled in this thesis. View from the perspective of the primary system, the secondary system has a sole function which is to serve as an energy sink. In MFM the separation of subsystems according to the perspective and functionalities is easy to achieve, for source and sink function in MFM defines the modeled system boundary.

Figure 3.12 shows a diagram of the PWR primary system that is to be modeled. The system includes three Reactor Cooling Loops (RCL). Each RCL contains a Steam Generator (SG), a Reactor Coolant Pump (RCP) and a cold-leg collector (CC) connected to the main circulation pipeline. The pressurizer surge line is connected to the second RCL. The system also includes the Chemical and Volume Control System (CVCS), and the safety injection system. In this system the low pressure safety injection pumps are combined with residual heat removal pumps, and the high pressure injection pump is combined with the inlet charging pump from the CVCS. The control rods, which are not illustrated in the diagram, are also to be modeled in this case. In this section, a step by step

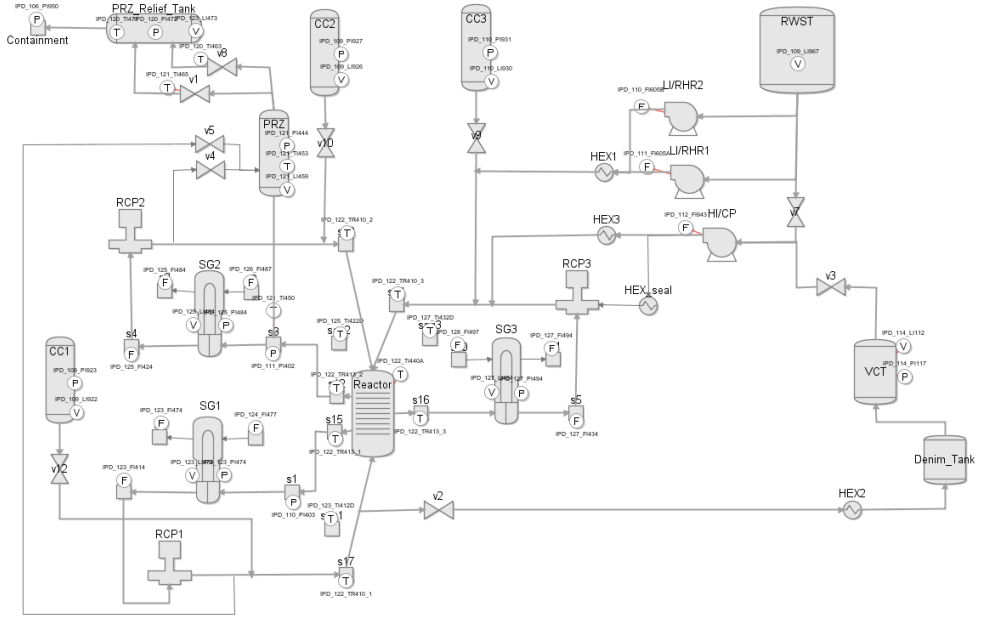


Figure 3.12: Diagram of the Ringhals PWR primary system.

explanation is provided to model the PWR primary system by using the MFM technique.

### 3.2.1 System objectives

Following the steps describe in Section 3.1.4, the objectives and mass/energy flows need to be determined first. The main operational objective for the PWR primary system is to generate and transport energy (in the form of heat). This objective is achieved by transporting the heat produced in the reactor to the SGs. The energy will be further transported from the primary side coolant loop to the secondary steam line inside the SGs. The energy is transported by means of the water circulation in the RCLs. The objectives can be summarized as follow.

1. maintain heat production,
2. maintain delivery of produced heat for power production,

3. maintain water level in RCS,
4. maintain water circulation in RCS,
5. maintain the average temperature and pressure (energy level) in the system.

### 3.2.2 RCS mass and energy flow

Two major flow structures (one energy flow and one mass flow) can be easily identified. The coolant (mass) flow has three circulation in the physical structure and all the coolant belongs to the same body of object. while the heat transfer (energy flow) in the system is directional.

For the energy flow, the reactor is considered to be the energy source, and two energy sinks can be identified from the process. The first energy sink is the SGs in which the primary system energy flows to the secondary system. Afterwards, the secondary system uses the heat generated in the reactor to produce steam, which in turn moves the turbine to generate electric power and deliver the power further into the grid. The energy sink function is realized not only by the physical components of a single SG, but is realized by SG plus the whole secondary system. This has to be emphasis because in MFM, physical components and MFM flow functions do not have a one to one mapping but a many to many mapping. The second energy sink is provided by the emergency cooling system. During the safety injection period, the heat that is generated from the reactor will be consumed by additional coolant.

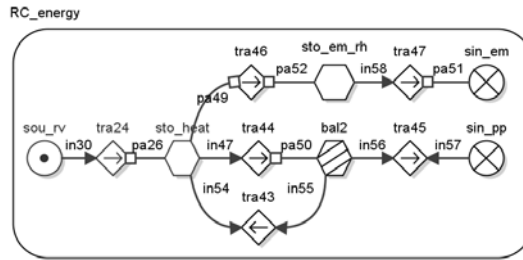


Figure 3.13: MFM model of the energy flow structure of the PWR primary system.

The model of the energy flow is shown in Figure 3.13. Noted that the function names of the partial models shown in the figures are not definite, they may vary from the final complete model shown in Figure 3.18.

During the normal energy production,  $tra_{44}$  delivers the generated heat from the primary to the secondary side. The remaining heat will circulate back to the general energy storage  $sto_{heat}$  through the cold legs. During emergency situations, when  $sin_{pp}$  is not available, the energy is removed through  $sin_{em}$ , by using the emergency cooling facilities.

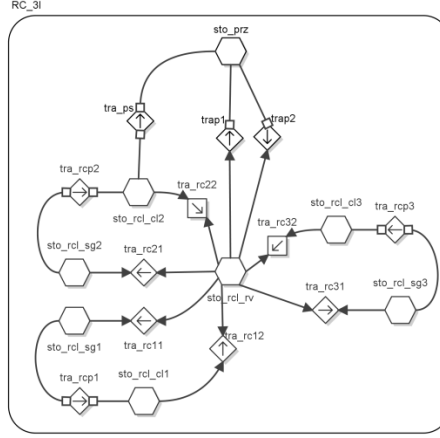


Figure 3.14: Mass flow structure of the RCL system with pressurizer.

The mass flow structure can be considered as a closed system during operation and modeled only using different storage functions to represent the water storage capacity of the reactor vessel, SGs, CCs, and the pressurizer. Figure 3.14 shows an MFM model of the RCLs with the pressurizer. The transport function  $tra_{ps}$  represents the pressurizer spray line.

However, considering the operational aspects, the Reactor Coolant System (RCS) is failing when any single cooling loop fails to meet the operational requirements, and from a functional perspective it is reasonable to represent (through abstraction) the three reactor cooling loops as one coolant circulation loop. This offers a simpler model with full function representation of the RCLs. So in the general model, the water circulation can be represented in MFM as in Figure 3.15.

The make-up system is not modeled in this study, so the CVCS can be considered as the water storage with an open loop from a source to a sink (omitting the recycling of the boron and water) that is connected directly to influence the level in the RCS.

In Figure 3.15  $sto_{vct}$  represents the function of the VCT tank for storing water.

Additionally, another water source can be considered, which is the function of

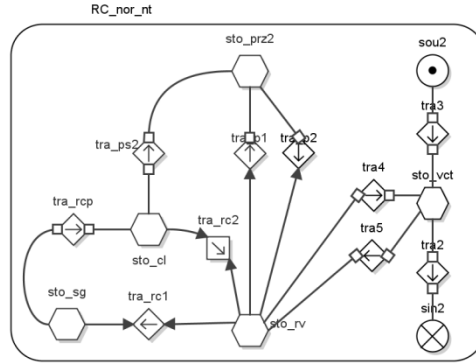


Figure 3.15: Abstract mass flow structure of the RCL system with pressurizer and VCT.

the Reactor Water Storage Tank (RWST). There is also another sink function which is realized by the component of the Pressurizer Relief Tank (PRT). Two partial models are shown in Figure 3.16.

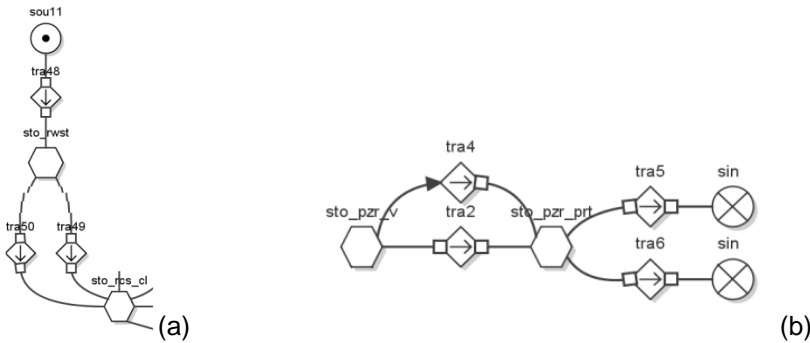


Figure 3.16: Additional mass flow functions in the mass flow structure.

### 3.2.3 Boron Injection and Rod Control

Through two methods, that an operator or the control system can influence the reactivity in the system, which are used to control the energy production in the system: one is the control rods insertion, and the other is boron injection through CVCS. These two can be modeled as two additional mass flows, which serves as alternative conditions in energy transportation.

Boron injections and control rods insertions are modeled with separate mass flows. Both of them can be modeled by using the model shown in Figure 3.17. Here we consider the storage function as the total amount of boron or inserted rods, which influences the reactivity in the reactor. Transport *tra34* and *tra35* represent the process of injection and removal, respectively.



Figure 3.17: MFM model of boron injection/removal or control rods insertion/removal.

### 3.2.4 Complete PWR primary system model

After the above discussions, one can combine all the partial models already derived and make proper modification (adding additional storages, balances, and transports) to produce a complete MFM model of the process from Figure 3.12. The proper means-end relations need to be drawn between different flow structures. A complete MFM model of the PWR primary side is shown in Figure 3.18. Notice that four additional energy flow structures are added to the model. The energy flows *efs2*, *efs3* and *efs4* represent the energy flow within the RCPs, the high head safety injection pump (also used as CVCS charging pump), and the low head safety injection pumps (also used as Residual Heat Removal Pumps), respectively.

The main function in each of these three energy flows provides means to transport water in different parts of the coolant mass flow in *mfs1*. For the modeling demonstration purpose, an additional function of the charging pump is also modeled in Figure 3.18, which is to provide the pressure for RCP seals. In the figure, *bar1* represents a functional barrier which is conditioned by the pump energy flow. However, during normal operation, the water flow through the pump seals is too small to make an impact on the system function, and thus can be neglected during the modeling.

The fourth energy flow structure that has not been mentioned in the previous discussion is *efs5*, which represents the pressure control function of the pressurizer. The pressurizer is an important component of the PWR system and requires detailed energy balance representation. The energy flow structure *efs5* is overlapping with *efs1* for the reason that the pressurizer has the func-

tion of controlling the pressure of the whole primary system. Therefore, *efs5* can also be viewed as a detailed representation of *sto8* in *efs1*. Because it is chosen to model the pressurizer vapor phase (*sto20*) and liquid phase (*sto22*) separately in *efs5*, for the purpose of representing the functional thermal dynamic aspects, the function of the pressurizer in the mass flow *mfs1* is also decomposed into vapor storage and liquid storage. Between the mass flow and energy flow of the pressurizer dynamic, the energy gathered in the two different phases drives the form changes through one phase to another, while the energy is transported alongside with the form changes. The MFM means-end relation producer-product is used to describe the influence from energy storages *sto20* and *sto22* to the mass transports *tra6* and *tra5*, while the MFM mediate relations are used to describe the influence from the mass transports *tra6* and *tra5* to the energy transports *tra52* and *tra51*.

Remembering the objective summary in the beginning of Section 3.2.1, in Figure 3.18, *obj2* and *obj5* represent objective 1) and 2), *obj4* and *obj3* represent objective 3) and 4), *obj6* represent objective 5).

Some decomposition is done for the model, for example the additional storage (*sto13*) and balance (*bal3*) functions are added to fully describe the function of the CCs in the system. However, the model presented in this section is still a highly abstract functional representation of the process, but it serves well for the purposes of further demonstrating how to add operational knowledge into the existing model. The ability to choose the level of abstractions to fit the modeling purpose is one of MFM's features for dealing with complexity. The causal relations between functions are not explained in this paper. These relations describe the influence between function states based on the mass and energy conservation rules. The reasoning rules will be explained in detail in Chapter 4 and an updated version is also included in the appendix as summary tables. These can provide a hint for modeling these relations.

The causal relations between different functions within a flow structure allow the model to be used for causal reasoning (reason about causes and/or consequences for abnormal function states).

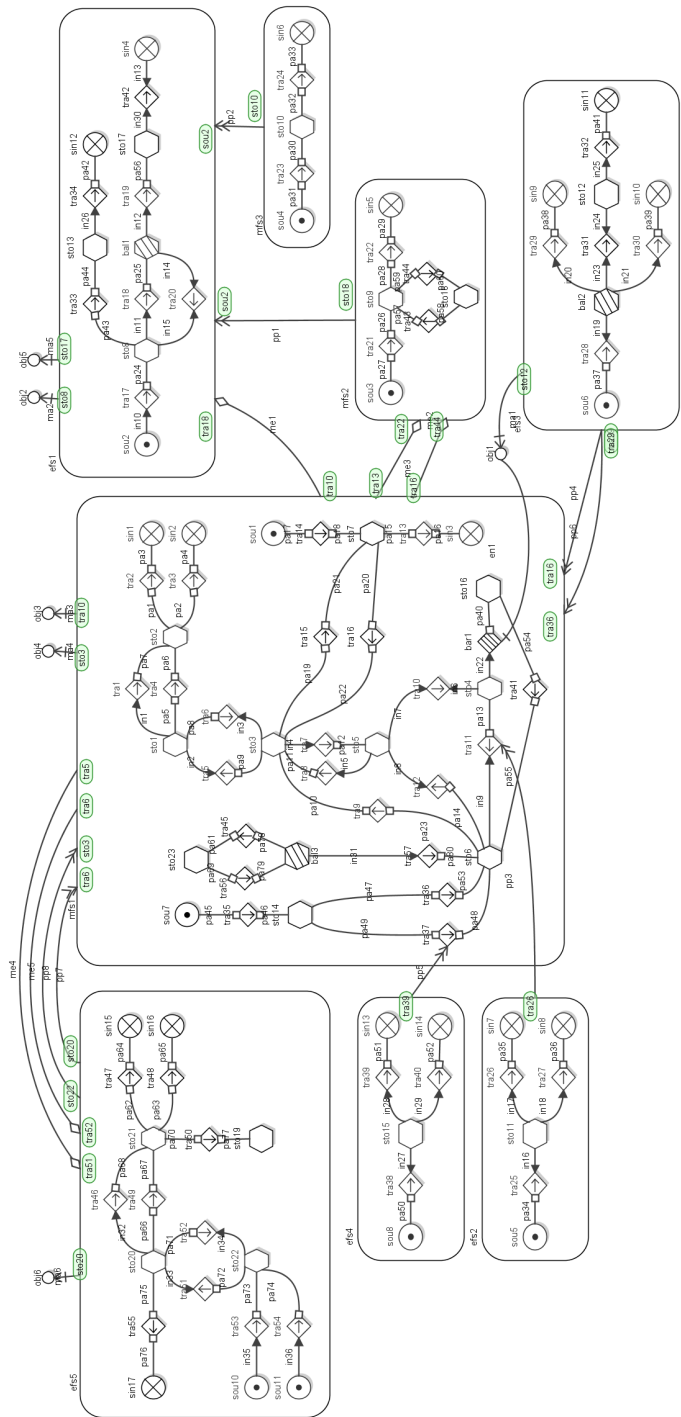


Figure 3.18: A complete MFM model of the PWR primary system.



### 3.3 Chapter summary

In this Chapter, the MFM syntax and MFM modeling technique is thoroughly explained. It is a big supplement to the existing literature about MFM modeling where the models are not usually explained but being used for other purposes.

It should be noticed that MFM is a modeling methodology has formalized semantic syntax and graphical representations. And it has great flexibility to represent the same system with different level of abstractions according to the user's need. Macros [57] has pointed out in his PhD thesis that MFM tend to get more complex when the physical system get more complex is a false conclusion.

The MFM functions model with causal relations is sufficient to capture the dependencies between different functions thus MFM models can be used to analyze the functional event propagation. This will be introduced in the next chapter.

## CHAPTER 4

# MFM Extension for Assessing Operational Situations

---

The distinguishing between intersubjective situation and subjective situation is of great importance because the aim of this thesis is to model the intersubjective perspective of the situation in reflection of the human perception. This is directly the opposite way to approach situation assessment with the research on situation awareness, where the mental model is core for situation representation. However, the two research strategies are not contradict with each other but just have different emphasis. It is assumed that to achieve situation awareness, the mental model of an operator has to be an accurate reflection to the real world. Thus the strategy of providing situation assessment support in this PhD project, is to represent the real world situation as closely to how humans reflect on it.

This chapter deals with theoretical problems in defining a situation from the intersubjective perspective and adopts MFM as the methodology to represent operational situation. The existing tools lies in the MFM research is not sufficient for this representation. Thus this chapter offers extensions of the MFM tool box to make the modeling approach available for situation assessment.

The requirement for situation representation is discussed in Section 4.1 while Section 4.2 to 4.5 will introduce the development of the MFM theory to fulfill the requirements. Section 4.6 summarize this chapter.

## 4.1 Representing situations

### 4.1.1 Intersubjectivity and subjectivity

Dewey [8] defines a problematic situation as a situation where instinctive or habitual responses of the human organism to the environment are inadequate for the continuation of ongoing activity in pursuit of the fulfillment of one's needs and desires. Burke [9] suggest that the term *situation* (in Dewey's study), should not be understood as only referring to a material context or environment, but rather should be apprehended as a unified integration of the human and the his/her material world.

At first glance, this definition hinted that a situation is subjective and it is a reflection of the objective world from a personal perspective. Viewing a situation from an subjective perspective, the term *fulfillment of one's needs and desires* suggests that a situation is closely related to the human's goal fulfillment. This indicates that the objective existence of the environment must be viewed in the context of the human desire (goals). If the goal is different, the situation, however the objective substances are the same, is a different situation.

In Dewey's formulation of problematic situation, only humans and their environment are of consideration. However, in complex systems, there are three elements as it is emphasized in Section 1.1. In addition to human and environment, there's also the artifact (engineered system) that has to be considered. The problem of applying the definition is to determine who is the material context and whose goal is in consideration during the operation of the engineered systems.

Lind [10] suggests that goals and purposes are concept only subject to humans not the natural objects. However, he also suggests that there is a distinguishing between natural objects and artifacts. Based on the design relations, the physical system is constructed to fulfill the design expectation of the humans (designers), which means that the physical systems is designed as an artifact to serve as a means to achieve certain goals when talking about goal fulfillment from an operational perspective.

Thus there is an aspect of the goal of the system operation in an operational situation which is independent of the human operator. And to insure the effective and successful in operation, the fulfillment of the systems' design goals dominates the operators' operational goal. This means to the human operator, the system goal is a required knowledge for them to operate the system. This knowledge about the system's designed operational goal is not a subjective

concept, but is a social fact like the concept of function mentioned previously. Which is to say that the goal is intersubjective and it has to be agreed between the designers and the operators.

This suggests that if the system can be represented in context of the system's designed operational goal, they can become the use of operators to match a situation with their own operational goal.

If Dewey's theory of situation is applied to the system operations, a problematic operational situation means a situation that, under normal operations the system's responses to the environment are inadequate for the continuation of ongoing process to fulfill what the system is designed for. Thus a situation exist not only in an operator's mind, but can be associated with the goal and function of the system. Therefore, it is possible to represent the intersubjective aspect of a situation explicitly and the representation can be evaluated.

#### 4.1.2 Function and action

The definition of a problematic operational situation only solve the problem of distinguish the objective and interobjective part of a situation, but did not provide framework of modeling a situation. A situation also lies in the material world. In the engineered systems, for an operator, the immediate material world is not only the environment, but also the physical constitution of the engineered system. The designed operational goal fulfillment is depends on the means to realize the goals.

To model a situation, only model the system's goal structure is obviously not sufficient for it to be used by the operator. The system goal structure must be developed such that the operator can understand how the system goal is achieved. Eventually, the system goal is all achieved by the lowest level in the means-end relation, which is the physical components and physical process. But because the complexity of the systems that is dealt with in the engineering field, there's a need to solve the problem of complexity.

The means-end structure is extremely useful for the purpose of approaching the systems complexity, as the operator can understand the means-end dimension when reason about system goal achievement. The concept of function is introduced as intermediate level in a means-end relation to support the goal structure, so that the system can be represent at a sufficient abstraction level for human to comprehend.

Another important aspect about function lies in how a function is defined. The

concept of function is closely relate to action. Lind [10] suggests that in a means-end relation, the physical system serve as the means for action, while function describes potentials and opportunities available for action here and now. For the operator, to operate is to act; while for the system, to function is to act. The functional level description of a system can therefore unify the human operation and the system function at the same abstraction level. According to this observation, it is argued that for operational situation assessment, functional representation of the physical system is desirable.

### 4.1.3 Perception, comprehension and projection

Dewey's definition of situation indicates that when determining a problematic situation, one must refer to the past experience to make inferences (habitual responses is no longer sufficient) and make a projection of the future state of goal fulfillment (discontinuation of the fulfillment of needs and desires). Endsley's situation awareness model [6] also suggests that, to achieve situation awareness during operation of a dynamic system, the situation itself cannot be viewed statically. On top of the perception of a situation, Endsley emphasizes two further states of awareness, namely comprehension and projection.

To understand the dynamic aspect of a situation, the concept of event has to be examined. Intuitively, the difference between an event and a situation is that an event happens while a situation persists. Events are normally responsible for the change of situations. To be aware of the situation, one has to understand how different events can affect the system status. However, a change of a situation does not rely on a certain event but only depends on how events will impact the goals and objectives. Event is an external input to a system which causes the change of system behavior, which depending on the means-end relations, change the states of the system function and the status of the goal fulfillment.

Therefore, to support situation assessment, it is not sufficient to describe the general composition of a system's functions and goals. The means-end relations has to be represented explicitly to evaluate the event dynamics and system goal. In a complex system, normally, events do not only propagate through the means-end dimension, but also through the same level of abstraction. Something happened in part of the system which can affect the whole system performance. Therefore, the dependency relations along the part-whole dimension also has to be represented for the purpose of understanding a situation.

#### 4.1.4 Representation requirements

It is argued in the above section that to represent an operational situation for the operator, the system goal structure has to be developed so the operator can understand how the goal is achieved. And to cope with the complexity of the engineered systems, representations adopt means-end decomposition is extremely useful. Functional level of representation is a good solution because the concept of function unified the process behavior, and the human behavior. Also based on the dynamic feature of situation assessment and event propagation, functions and goals relations has to be modeled explicitly so that the model can be used to inference that how event can affect the goal and objectives of the system.

The adopted modeling methodology MFM has all the required features for representing operational situations in a engineered system like a power plant. However, before it can be used to assess the situations, the reasoning schema of the MFM has to be extended.

MFM models has been used mainly as a fault diagnosis tool in previous applications. But the dependency relations (both causal relations and means-end relations) in MFM suggest that it can also be used to make prediction of the system status. However, the consequence reasoning of MFM has not been implemented previously and the root-cause reasoning is only implemented using a previous version of MFM concepts (which is less sophisticated in representing dependency relations). There is also a lack of formalization of function states for MFM concepts. In Section 4.2 the author will first develop the complete set of function states is developed and in Section 4.3, a causal reasoning algorithm based on the latest version of MFM concepts is introduced.

## 4.2 MFM states and status

Lind [67] has introduced the basic principles for MFM models to be used for causal reasoning. However, the definitions of function states is absent. Previous MFM literatures adopted the function states set that Petersen [2] developed with basic understanding of MFM flow functions. However, to use the MFM models for causal reasoning and make the reasoning result meaningful, functional understanding of the state and status is also required. Thus in this section, the MFM function states and their status will be redefined.

### 4.2.1 Review of the functional concepts

Functional concepts have been the subject of investigations for a long time and are still within both philosophy of science, cognitive psychology, biology and artificial intelligence. In engineering systems, functionality is often discussed as a teleological term where the purpose of a function plays an important role for explaining the function itself. Wimsatt [73] introduced a general schema for teleological function statements, which is given by the Equation 4.1.

$$F[B(i), S, E, P, T] = C \quad (4.1)$$

It can be read as “According to theory  $T$ , the function  $F$  of item  $i$ , in producing behavior  $B$ , in system  $S$  in environment  $E$  relative to purpose  $P$  is to bring about consequence  $C$ ”.

The elements in Wimsatt’s equation are all highly relevant for the operational functions in engineering systems and are necessary for the further discussion of how to define and evaluate function state and status, though some of the elements can be changed to terms that are more specific for the operational function in engineered systems.

In engineering systems, talking about “the function of  $x$  is  $A$ ” usually means “ $x$  is designed/used to do  $A$ ”, where  $A$  is an action to do and  $x$  is the subject/agent who perform the action. Implicitly, the statement also normally refers to another object  $y$  that is done  $A$  by  $x$ . For example, a pump’s function is to transport, and in a certain system, water maybe implied as the object which is being transported. However the function of the water is being transported is rarely discussed even though it is usually equally importance to the pumping function. Therefore the behavior in the equation is changed into an action (a subset of behavior)  $A(x, y)$  with an agent  $x$  and an object  $y$ .

The theory in Equation 4.1 refers to the knowledge at how a function is recognized as a function in a given perspective. A physical entity may do a lot of things (that is to say, has many dispositions), for example, a pump may transport water, produce heat, create noises, but in a given water circulation system, the pump’s function is to transport water. This means that the assumptions are being made when a function is defined that one have the knowledge of the system and the kinds of causal laws assumed to be applicable to the description and explanation of the operation of the system. More specifically, it means that the ways of disposition selection is known. The theory is described as the dispositions of the items selected under the context in Equation 4.2, where *cntx*

is the given context,  $D_x$  and  $D_y$  are the disposition chosen function for agent  $x$  and an object  $y$ .

$$T = D_x(cntx)D_y(cntx) \quad (4.2)$$

The purpose of a function in an engineering system refers often more directly to the achievement of a specific state (either local or within system), which is more commonly described as a function goal  $G$ . The Function equation is changed into Equation 4.3.

$$F[A(x, y), S, E, G, D_x(cntx)D_y(cntx)] = C \quad (4.3)$$

Equation 4.3 can be read as “By chosen disposition  $D_x$  of item  $x$  and  $D_y$  of item  $y$  under the context of  $cntx$ , the function  $F$  of item  $x$ , in executing action  $A$  to item  $y$ , in system  $S$  in environment  $E$  relative to achieving  $G$  is to bring about consequence  $C$ ”. It is important to note that the goal ( $G$ ) and the consequence ( $C$ ) is not the same concept, where the goal represents the intention of the action and the consequence is the achievement of the goal. Function describes the process that the consequence brought about by the action is the fulfillment of the goal.

### 4.2.2 Means-end relation

Despite the importance of the general concept of function and its elements introduced above, they do not provide sufficient basis for developing a formalized methodology to model the functional aspects of the system and for providing guidance for defining function states. There is a lack of the temporal resolution (dynamic aspect) and relations between each functional element. Means-end relations has to be brought up to create a more detail explanation of how elements of functional concepts are linked. Firstly, we need to examine the function from outside of its entities and goal. When a goal rather than a purpose is introduced in the functional elements, there is a more direct relation between function and its goal, which can be described as a means (function) to an end (goal). The function itself is realized by means of the physical structure that is assumed to have the necessary dispositions to fulfil the roles, which are required to carry out the function related action. In Figure 4.1, the grey boxes describe means-end relationship between entity function and its goal. The transformation describes the expected change from the current state to the goal state. The functional



roles (i.e. of agent  $x$  and object  $y$ ) fulfillment are the prerequisites for the possibility of the transformation.

The different aspects of the means-end relation connect the means for action (the structure and the dispositions) with the potentials and opportunities available for action here and now (the roles and the functions refer to the current time instance and location in the system) and goals to be achieved in the future. The means-end structure in Figure 2.2 in Chapter 2 explains the functional concepts offer a preliminary sense of how to assess the function, but only in an off-line context. However, by talking about evaluation of operational functions, real actions have to be considered. During operation, a function appears in the form of its action, and only the action can bring about the consequences to be evaluated at the execution level. An action has to be carried out in a certain sequence, which is as action phases from bottom to the top in the red box in Figure 4.1.

From the perspective of actions phases, several assessment aspects for an operational function can be identified, namely potentiality, opportunity, execution and achievement. The dashed lines in Figure 4.1 indicate that to which action phase is the assessment aspect refers to. During execution, there are different stages that an action can be performed in. First it has to be initialized and then triggered. In complex systems, most functions require constant performance of the action to fulfil their objectives after their triggering. In case of the completion of the action, it has to be terminated according to the goal requirement.

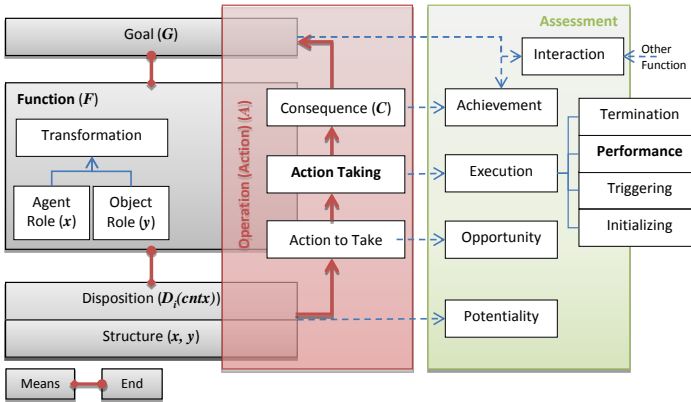


Figure 4.1: Means-end relation for functions and for their assessment

### 4.2.3 Abnormal states and status

For each of the assessment aspect, a binary value (True or False) can be assigned to indicate whether the action phase is reached or not. According to the above discussion, the corresponding function element status can be derived. They are shown in Table 4.1.

Table 4.1: Function status assessment according to action phases.

Assessment	Phases	Status	
		(True)	(False)
Function (role)-Structure	Potentiality	Available	Not available
	Opportunity	Enabled	Disabled
Function-Execution	Initialization	Initialized	Not initialized
	Triggering	Triggered	Not triggered
	Performance	On-going	Suspended
	Termination	Stopped	Aborted
Function-Objective	Goal-achievement	Achieved	Not achieved
Interaction	Interaction	Effective	Ineffective

In the case that the goal achievement is directly related to the performance, a norm is usually assigned to the function according to what kind of performance can provide consequences that fulfil the objective. And in qualitative analysis, based on how far the performances deviated from the norm (how far the consequence deviated from the desired norm), different performance states can be assigned to the function during execution. Note that the function goal can be a certain state or it can be a condition for another function to be performed in the same system. In this case the interaction between different functions is also an aspect to be evaluated.

The action performance and the interaction between functions require special treatment. For the performance aspect, qualitative scales can be assigned to a function to evaluate the efficiency of objective achievement. In general, function states can be either normal state (means that the outcome of the function is within the normal range), or abnormal(that the outcome of the function is beyond normal range). For complex system, there are different levels of control methods to keep the function performance to be close to its norm. Accordingly it is convenient to define different abnormal states based on the level of effort of controllability. For example, the abnormal states can be either deviation, abnormal, or critical. This is summarized in Table 4.3. Deviation means the function state is slightly deviate from the normal state but within the normal range, abnormal means that the function states is beyond normal range but within a certain limitation defined by the system, and critical means the function

states is beyond abnormal states and it may cause serious consequences.

Table 4.2: Functional performance assessment.

Assessment	Context	States
Performance	Singular	Normal, Deviation, Abnormal, Critical

Interaction between functions describes how one function state affects another function state. The interaction is different in nature based on the relationship between different functions. Generally speaking, one function state can influence another function on either status in Table 4.1 or 4.3. Two examples are suggested in Table 4.3.

Table 4.3: Functional influences assessment.

Assessment	Interaction	Influence
Influence of States	Causal relation	to increase, to decrease
Influence of Status	Means-end relation	to enable, to disable

During operation, it is the functions' performance states that are the subject being assessed, and the assessment is bounded by the enablement (Opportunity) of a function. When a function is disabled, the performance evaluation process ceased because the function loose the opportunity to goes into execution and the functional structure of the system may be subject to change. This indicates a mode shift which will be introduced later in this chapter. For MFM function, a set of flow function performance state is summarized in Table 4.4.

Table 4.4: MFM flow function abnormal performance states.

Flow Functions	Abnormal performance states
source	low low, low, high, high high
sink	low low, low, high, high high
transport	low low, low, high, high high
barrier	leak
storage	low low, low, high, high high
balance	sourcing, leak, block

Except balance functions and barrier functions, the other flow functions may have two categories of abnormal states: high states or low states. The abnormal states in transport function refers to the flow rate while the abnormal states in storage function refers to the volume. The states of source and sink function refers to their potentiality. A function can be still enabled but in a critical performance sate, upon which situation, high high and low low states are defined. The high high and low low states refers to the boundaries of a function's performances in MFM.

For balance function, sourcing refers the abnormal states in the in-port flow balancing, and the leak refers to the abnormal states in the out-port flow balancing. Block state of a balance function refers to the boundaries of the balance performance. If a balance is in block state, then all the transport function that is connected to the balance function are in low low states.

## 4.3 Causal reasoning

Causal reasoning is the ability to identify causality: the relationship between a cause and its effect. Because MFM decomposes a complex system in both means-end and whole part dimensions, the cause-effect in both dimensions has to be considered. MFM constructs the model by using building blocks that correspond to functions and goals. It describes energy and mass flow structures in a physical system with different level of decompositions, and provides an abstract representation which is independent of individual components in the physical systems. However their functionality is truthfully represented.

Reasoning in MFM models is based on dependency relations between states of objectives and functions. Each function can be either enabled or disabled. For any enabled functions a list of performances state is drawn in Table 4.4. Two to three MFM functions that connected together through causal relations is called a MFM pattern. With the MFM syntax introduced in Chapter 3 as constrains, there is a finite set of MFM patterns. These MFM patterns together with a hypothesis of function performance states are used for MFM causal reasoning.

### 4.3.1 Causal reasoning on part-whole dimension

On the part-whole dimension, the cause-effect relation is modeled by using causal roles between flow functions. As introduced in [67], there are two types of causal influences in MFM along the part-whole dimension.

The first type of influences is called a direct influence, which describes how transport functions influence other flow functions. Because of the nature of a flow structure, the state of a transport function will always influence the mass or energy flow in the flow structure in both its upstream and downstream directions, thus influence all the functions that are connected to them.

The other type of influences is called an indirect influence, which describes how the transport function is influenced by other flow functions. Because the non-

transport flow functions presented in a flow structure may or may not have an active influence on the mass or energy flow in the flow structure, their effect on the flow states are described by using the MFM causal roles. As already introduced in Chapter 3, a non-transport flow function can have either a influencer role or a participant role to one of the transports that are connected to it.

Balance function is a special flow function because it has the ability to balance the flow, thus it will propagate the flow state from one transport function that is connected to it to other transport functions, if assuming the balance is not in abnormal state. Therefore, there are special influence rules concern balance functions as explained below.

Barrier is a function which does not have a directional property on it. The barrier function has a binary status of whether it is enabled or disabled. Thus the state of a barrier function is not considered in this section.

### **Direct influence without balance function**

Direct influence is a cause-effect relation between a transport function and other flow functions. After considering the MFM syntax, it is easy to deduce that only source and storage can be the upstream functions for transport, while only storage and sink functions can be the downstream function connected to a transport. Both influencer and participant relations describe the indirect influences, but these relations do not affect the direct inference. A consequence (effect) inference will start from a proposition (either evidence or a prediction) of the transport state under the assumption that the non-transport function is enabled.

Firstly, we consider how a transport function state will influence its upstream functions. When a transport function is in a “high” flow state, the possible consequence is that its upstream function is in a “low” state because the transport draws more mass or energy out of its upstream function than in the normal situation. Considering pumping water from a tank, if the flow rate of the outlet water is higher than normal condition, then a possible consequence is that the water tank will have a lower volume than normal. A reasoning rule example can be stated as follow:

IF a transport “tra1” has a “low” state, THEN a possible consequence for the abnormal state is that its upstream source function “sou1” will have a “high” state.

To the contrast, if the transport has a “low” state of the flow rate, then the

possible consequence is that the upstream function will accumulate more volume than its normal condition. In the extreme situation that if the transport have “high high” or “low low” state, the possible consequence to its upstream functions will be “low low” or “high high”.

The consequence reasoning rules for the four MFM patterns are shown in Table 4.5. In this section the, all the tables has a first row to indicate the composition of the MFM patterns. The middle column shows the symbols of the MFM patterns while the other columns show the abnormal function states. Column in a table which is marked in red all indicates the initial abnormal states, the other column of state is the deduced states. Brackets with non-transport function indicate whether the function has an influencer or a participant role. In direct influence, causal roles do not affect inference.

Table 4.5: Consequence reasoning rules for direct influencing downstream.

source/storage (in/pa)	pattern	transport
low low		high high
low		high
high		low
high high		low low

Considering the four MFM patterns which link a transport function to its downstream functions as shown in Table 4.6, “high” volume of the upstream source or storage is a possible consequence for a “high” flow downstream transport, while “low” flow rate of the transport function will possibly result in a “low” volume in the downstream function. In the extreme situation that if the transport have “high high” or “low low” state, the possible consequence to its upstream functions will be “high high” or “low low”.

Table 4.6: Consequence reasoning rules for direct influencing upstream.

transport	pattern	(in/pa) sink/storage
high high		high high
high		high
low		low
low low		low low

The root cause reasoning follows the same pattern, when reasoning about the root cause based on direct influence, the inferences start from an abnormal state of an upstream source function or storage function, or a downstream storage function or a sink function. One example of the reasoning rules can be stated

as:

IF source function “sou1” has a “high” state, THEN a possible cause for the abnormal state could be its downstream transport “tra1” has a “low” state.

Table 4.7: Cause reasoning rules for direct influencing downstream.

source/storage (in/pa)	pattern	transport
high high		low low
high		low
low		high
low low		high high

The root cause reasoning of direct influence with downstream transport is summarized in Table 4.7. The root cause reasoning of direct influence with upstream transport is summarized in Table 4.8.

Table 4.8: Cause reasoning rules for direct influencing upstream.

transport	pattern	(in/pa) sink/storage
high high		high high
high		high
low		low
low low		low low

One may notice that in the direct influence the separation between four level states, does not give any additional in result than the two level abnormal states. However, this is not true in the indirect influence.

Indirect influence without balance function


To reason about indirect influence, it is necessary to distinguish between the influencer or participant relation.

First, upstream source functions or storage functions with an influencer role are considered. When reasoning in downstream direction, “high” states of the upstream source or storage will result in “high” states of the downstream transport, while “low” states of the upstream source or storage will result in “low” states of the downstream transport. Considering a potential source in this case, when the source function has a high potential, it will push out mass or energy in a higher flow rate. One of the reasoning rules can be described as follow:

IF a source “sou1” has an “influencer role” to its downstream transport AND has a “low” state, THEN a possible consequence for the abnormal state is that its downstream transport function “tra1” will have a “low” state.

“low low” state and “high high” state of the upstream functions give similar inference results in these two patterns. The other reasoning rules for the two patterns are summarized in Table 4.9.

Table 4.9: Consequence reasoning rules for indirect influencing upstream with influencer relation.


source/storage (in)	pattern	transport
high high		high high
high		high
low		low
low low		low low

The “high” volume in the downstream sink or storage will give a saturation effect, and therefore result in low flow of the upstream transport; whereas a “low” volume will draw more mass or energy from the upstream transport. One of the reasoning rules can be stated as:

IF a sink “sin1” has an “influencer role” to its upstream transport AND has a “low” state, THEN a possible consequence for the abnormal state is that its upstream transport function “tra1” will have a “high” state.

“low low” state and “high high” state of the downstream functions give similar inference result in these two patterns as well. The other reasoning rules for the two patterns are summarized in Table 4.10.

Table 4.10: Consequence reasoning rules for indirect influencing downstream with influencer relation.

transport	pattern	(in) sink/storage
low low		high high
low		high
high		low
high high		low low

When reasoning about root causes for the four patterns in Table 4.9 and 4.10, the inference table in Tables 4.11 and 4.12 are not match the consequence reasoning. This is a very important observation, the reason is that the causal reasoning in MFM has underlying temporal information. In the consequence reasoning, the deduced hypothesis (effect) should not be prior to the initial state, while in



the root cause reasoning, the deduced hypothesis (cause) happened before the present state.

For the root cause reasoning rules to reason about causes for the abnormal state in a transport function with an influencer role attached to its upstream source or storage function, one of the reasoning rules can be stated as:

IF transport function “tra1” has a “high” state AND its upstream source function “sou1” has an “influencer role”, THEN a possible cause for the abnormal state could be “sou1” has a “high” state.

The other inference rules for the two MFM patterns are listed in Table 4.11.

Table 4.11: Cause reasoning rules for indirect influencing upstream with influencer relation.

source/storage (in)	pattern	transport
high high		high high
high		high
low		low
low low		low low

For the root cause reasoning rules to reason about causes for the abnormal state in a transport function with an influencer role attached to its downstream sink or storage function, one of the reasoning rules can be stated as:

IF transport function “tra1” has a “high” state AND its downstream sink function “sin1” has an “influencer role”, THEN a possible cause for the abnormal state could be “sou1” has a “low” state.

The other inference rules for the two MFM patterns are listed in Table 4.12.

Table 4.12: Cause reasoning rules for indirect influencing downstream with influencer relation.

transport	pattern	(in) sink/storage
high high		low low
high		low
low		high
low low		high high

Indirect influence with a participant means that the transport dominates the flow rate. Therefore, abnormal states from a downstream storage or sink will not give any consequence to its upstream transport, unless the function reaches

a situation state “high high”. When the downstream function in these two patterns become “high high”, the transport will be in a “low low” state due to the saturation.

The MFM patterns and the only inference rule for them is listed in Table 4.13. The rule can be stated as:

IF a sink “sin1” has a “participant role” to its upstream transport AND has a “high high” state, THEN a possible consequence for the abnormal state is that its upstream transport function “tra1” will have a “low low” state.


Table 4.13: Consequence reasoning rules for indirect influencing upstream with participant relation.

transport	pattern	(pa) sink/storage
low low		high high
-		high
-		low
-		low low
-		

Similarly, for the upstream source function or storage function that have a participant role to its downstream transport function, only when the state becomes “low low” indicates that the source or storage is of a near empty state, it is possible for the transport to become “low low” state. The reasoning rules for these two patterns are shown in Table 4.14. The reasoning rule can be sated as:

IF a source “sou1” has a “participant role” to its downstream transport AND has a “low low” state, THEN a possible consequence for the abnormal state is that its downstream transport function “tra1” will have a “low low” state.

Table 4.14: Consequence reasoning rules for indirect influencing downstream with participant relation.

source/storage (pa)	pattern	transport
high high		-
high		-
low		-
low low		low low

When reasoning about root causes for a transport, only the “low low” states may have been caused by a flow function with a participant role. One of the possible causes is that the upstream source function or storage function with a participant role has a “low low” state, the other is that the downstream sink function or storage function with a participant role has a “high high” state. The

root cause reasoning for these four MFM patterns is summarized in Tables 4.15 and 4.16.

Table 4.15: Cause reasoning rule of indirect influencing upstream with participant relation.

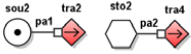

source/storage (pa)	pattern	transport
-		high high
-		high
-		low
low low		low low

Table 4.16: Cause reasoning rule of indirect influencing downstream with participant relation.

transport	pattern	(pa) sink/storage
high high		-
high		-
low		-
low low		high high

Influence through balance function

A balance function ensures that its summed input and summed output flow are equal. When reasoning about direct influence from transport to balance, the transport on the other side of the balance has to be taken into account. We first examine the balance with single in-port and single out-port.

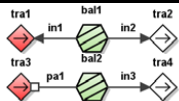
First we examine the MFM patterns in Table 4.17. When a transport function has an abnormal state, and it is linked to a downstream transport through a balance function between them, it is possible for the abnormal state to propagate downstream, when the balance has an influencer role towards the downstream transport. One of the reasoning rules can be stated as:

IF transport “tra1” is connected to a downstream balance “bal1” AND “bal1” has an “influencer role” to its downstream transport “tra2” AND “tra1” has a “ high” state, THEN a possible consequence is “tra2” will have a “high” state, ASSUMING “bal1” is “normal”.

The consequence reasoning rules are listed in the Table.

Similarly, when a transport function has an abnormal state, and it has linked to

Table 4.17: Consequence reasoning rules for indirect influencing upstream.

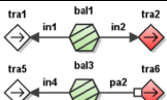
transport	(in /pa)	balance	(in)	transport
high high				high high
high				high
low				low
low low				low low

an upstream transport through a balance function between them, it is possible for the abnormal state propagate upstream, when the balance has a influencer role towards the downstream transport. One of the reasoning rules can be stated as:

IF transport “tra2” is connected to an upstream balance “bal1” AND “bal1” has an “influencer role” to its upstream transport “tra2” AND “tra1” has a “high” state, THEN a possible consequence is “tra1” will have a “high” state, ASSUMING “bal1” is “normal”.

The consequence reasoning rules for these two MFM patterns are listed in Table 4.18.

Table 4.18: Consequence reasoning rules for indirect influencing downstream.

transport	(in)	balance	(in/pa)	transport
high high				high high
high				high
low				low
low low				low low

If the balance function only have participant roles attached to other transport function except the abnormal transport, there is no inference can be drawn from the MFM pattern through a balance function. The abnormal state does not propagate through the balance.

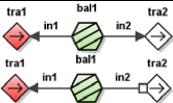
For the root cause reasoning, if a transport with an abnormal state is connected to a balance and the balance has an influencer role upon it, then a cause for the abnormal state of the transport can be because of the abnormal states of another transport which is connected to the balance at the other direction.

In Table 4.19, one of the reasoning rules can be stated as:

IF transport “tra1” is connected to a downstream balance “bal1” AND “bal1” has an “influencer role” to “tra1” AND “tra1” has a “ high” state, THEN

a possible cause is that the downstream transport “tra2” has a “high” state, ASSUMING “bal1” is “normal”.

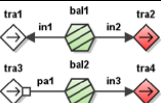
Table 4.19: Cause reasoning rules for indirect influencing upstream.

transport	(in)	balance	(in/pa)	transport
high high				high high
high				high
low				low
low low				low low

In Table 4.20, one of the reasoning rules can be stated as:

IF transport “tra1” is connected to a downstream balance “bal1” AND “bal1” has an “influencer role” to “tra1” AND “tra1” has a “ high” state, THEN a possible cause is that the downstream transport “tra2” has a “high” state, ASSUMING “bal1” is “normal”.

Table 4.20: Cause reasoning rules for indirect influencing downstream.

transport	(in/pa)	balance	(in)	transport
high high				high high
high				high
low				low
low low				low low

**Influence on the same side of balance function**

Balance is a multi-in-port and multi-out-port function, and the transports connected to the same side of a balance function influence the state of each other, if assuming the balance is in normal function and it has influencer role to the transport function. Table 4.21 shows the balance pattern for reasoning in the same side of a balance function.

Because that balance function balance the summed inflow and summed outflow to be equal, therefore, if a out port transport is in a “high” state, that means the transport on the same side of a balance will decrease its in flow rate if the balance has an influencer role to it. The other reasoning rules are all listed in Table 4.21.

However, shown in Table 4.22, even if the transport on the out-port has abnormal state, then no inference can be drawn to conclude the state of the transport

function if the balance only have a participant role on them. One of the reasoning rule in Table 4.22 can be stated as:

IF transport “tra1” and “tra2” are both downstream transport to balance “bal1”  
AND “bal1” has an “influencer role” on “tra2”, AND “tra1” has “high” state,  
THEN a possible consequence is that “tra2” will have a “low” state.

Table 4.21: Consequence reasoning rules for transports on the same side of a balance. (1)

transport	(in/pa) balance (in) normal	transport
high high		low low
high		low
low		high
low low		high high

Table 4.22: Consequence reasoning rules for transports on the same side of a balance. (2)

transport	(in/pa) balance (in) normal	transport
high high		-
high		-
low		-
low low		-

Based on the consequence reasoning, one may deduce the root cause reasoning rules. They are summarized in Table 4.23. One of the reasoning rule can be stated as:

IF transport “tra1” and “tra2” are both downstream transports to balance “bal1”  
AND “bal1” has an “influencer role” on “tra1”, AND “tra1” has “high” state,  
THEN a possible cause is that “tra2” has a “low” state.

However if the balance only has a participant role to the transport in abnormal state, then no root cause reasoning can be deduced for that transport function. This is shown in Table 4.24.

Transports that are connected to the in-port of a balance have the same reasoning rules in both consequence reasoning and root cause reasoning.

Table 4.23: Cause Reasoning rules for transports on the same side of a balance.  
(1)

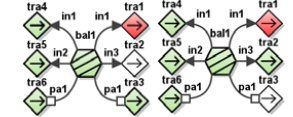
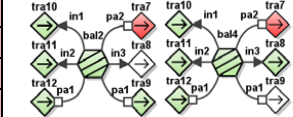
transport	(in) balance (in/pa) normal	transport
high high		low low
high		low
low		high
low low		high high

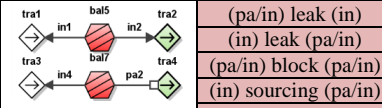
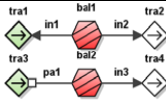
Table 4.24: Cause reasoning rules for transports on the same side of a balance.  
(2)

transport	(pa) balance (in/pa) normal	transport
high high		-
high		-
low		-
low low		-

Influence by balance function

The transport function which is connected to a balance function can also be influenced by the malfunction of the balance. The balance has three abnormal state, namely “sourcing”, “leak”, and “block”. The abnormal state will influence its upstream and downstream transport function separately.

Table 4.25: Consequence reasoning rules for a malfunctioning balance.

transport	pattern	balance	pattern	transport
(not high)		(pa/in) leak (in)		low/low low
high/high high		(in) leak (pa/in)		(not low)
low low		(pa/in) block (pa/in)		low low
low/low low		(in) sourcing (pa/in)		(not high)
(not low)		(pa/in) sourcing (in)		high/high high

In Table 4.25, the MFM pattern for each row is indicated in the balance column. Reasoning rules for the first row in the table can be stated as:

IF balance “bal1” has an “influencer role” to its downstream transport “tra2” AND “bal1” has “leak” state, THEN a possible consequence is “tra2” will be in “low” state OR “low low”. ASSUMING that the upstream transport “tra1”

is not “high” OR “high high”.

The reasoning result when the balance is leaking, assuming the upstream transport is not in a high state, means that the mass or energy flow has unexpected out-port transport function. Thus there are two possibilities for consequence reasoning. Firstly, the designed out-port transport function’s flow rate will decrease according to the reasoning rules for the transports function on the same side of a balance if the balance has an influencer role. Another possibility is that the designed in-port transport function will increase if the balance has an influencer role. While for the same MFM pattern, if a balance is sourcing, it means that the mass or energy flow has unexpected in-port transport function attached. One may deduce the reasoning rules accordingly.

For the root cause reasoning, if a transport has a balance as influencer, the “high” or “high high” on the upstream side can be because the balance is “leak”, while “low” or “low low” can be because the balance is “sourcing”. Another possibility for the “low low” state is that the balance function is “block”. When the balance only has a participant role to the transports, only with “low low” state of a transport can draw hypothesis on the state of a balance. Table 4.26 to 4.29 summarized the reasoning rules.

Table 4.26: Cause reasoning rules for transport function in a balance pattern.  
(1)

balance (in)	pattern	transport
sourcing		high/high high
leak		low/low low
block		low low

Table 4.27: Cause reasoning rules for transport function in a balance pattern.  
(2)

transport	pattern	(in) balance
high/high high		leak
low low		block
low/low low		sourcing

4.3.2 Causal reasoning on means-end dimension

Causal reasoning across means-end dimensions is depend on the means-end description in MFM model. There are three different type of influences. The one related to function performance is the means-end relation of “producer-product”



Table 4.28: Cause reasoning rules for transport function in a balance pattern. (3)

transport	pattern	(pa) balance
high high		-
high		-
low		-
low low		block

Table 4.29: Cause reasoning rule of transport function in a balance pattern. (4)

balance (ba)	pattern	transport
-		high high
-		high
-		low
block		low low

and “mediate” relation. Because these two relations provide a direct shift of perspective when modeling system functions, which means that the functions in different function flow structures represent the function of the same physical structure with different perspective. Therefore, there are direct influence on function states between the two ends of a “pp” or a “mediate” relation. The reasoning rules are summarized in Table 4.30.

Table 4.30: Consequence reasoning rule for function-function means-end relation.

			high high	abnormal	abnormal	transport
			high high			
			low low			
			low low	abnormal	abnormal	transport
			low low			
			high high			

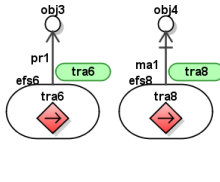
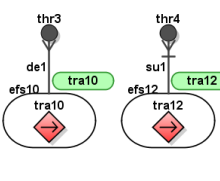
During the modeling procedure offered in Chapter 3, it is identified that “pp” relation in MFM have different semantical meaning. The relation can indicate that the two function linked by the relation is bounded by the same function states or the opposite function states.

Unless causal relations in MFM, means-end relation for inference is directional,

because means-end relation indicates the temporal relation between the means and the end, where means has to be present prior to the end. Thus only the means function’s abnormal states will propagate through means-end relation when reason about consequences. While when reason about possible causes, the reasoning process go from the end function state to deduce the means function states.

The other cause effect consequence inference along means-end relation goes from a function to its objective. As already mentioned in Chapter3, the syntax of MFM offers constrains for modeling these means-end relations. An objective can only be linked to the end of “produce” and “maintain” relations, while a threat can only be linked to the end of “destroy” and “suppress” relations. Any flow functions can serve the means to these four means-end relations and the abnormal states in the flow function will result in the “false” of in an objective, but “true” of in a threat. The consequence reasoning rules are summarized in Table 4.31

Table 4.31: Consequence reasoning rules for function-target means-end relation.

	true	false	objective
	normal	abnormal	Flow function
	true	false	threat
	abnormal	normal	Flow function

The third kind of inference reasoning about how the state of an objective or threat can influence the functions that they support through a conditional relation. As an objective can only link to a “enable” relation, and a threat can only link to a “disable” relation, semantically, it is easy to understand that the true state of an objective will result in the enablement of the function, and true state of an threat will result in the disablement of the function. The consequence reasoning rules are summarized in Table 4.32.

Table 4.32: Consequence reasoning rules for function-target means-end relation.

	disable	enable	flow function
	false	true	objective
	disable	enable	flow function
	true	false	threat

The root cause reasoning rules for the means-end relations can be deduced accordingly for all means-end relation has directional indication when using for causal reasoning.

4.3.3 Reasoning propagation

In MFM, there is no isolated function or objective. All system objectives and functions are either linked by causal relations or means-end relations. That is to say, MFM model is formed by combining MFM patterns. This enable the propagation of the reasoning process. A hypothesis of abnormal state of a function can propagate to either its upstream function or its downstream function. In this way, if the reasoning process starts with one function, a reasoning path can be generated.

And because most of the MFM functions is parts of two or more MFM patterns (except source and sink function who does not serve as main-function), the reasoning path will branch out. All the reasoning result for one session of reasoning activity (either consequence reasoning or root cause reasoning) will generate multiple hypothesis paths, and all the hypothesis reasoning path will form a tree structure.

If the reasoning start with any function in a MFM model, and both root cause reasoning and consequence reasoning is performed, the reasoning result will form a bow-tie structure, so that all possible cause-effect paths deduced involving one MFM function can be generated.

#### 4.3.4 Rule Based System for MFM Consequence Reasoning

All the reasoning patterns and inference formulas introduced previously can be implemented into a rule-based system as reasoning rules.

Existing rule-based system development environments offers inference engines with reasoning algorithm that can perform the reasoning automatically. A rule-based software tool has been developed by the author based upon the previous implementation of MFM workbench, using Jess (Java Expert System Shell) programming.

A reasoning rule contains two parts. Jess uses an enhanced version of the Rete algorithm to process rules. Rete is a very efficient mechanism for solving the difficult many-to-many matching problem. Jess has many unique features including backwards chaining, inheritance capability, and working memory queries. It is suitable for applications when rules needed to be fired repeatedly based on newly generated information.

In Jess rules, the left-hand side (LHS) of the rules contain the conditions that need to be matched, while the right-hand side (RHS) of the rules produces the inference result if the left-hand side is matched. When running Jess applications, LHS of the rule need to be matched with knowledge based facts. For MFM reasoning, the LHS contains two parts, one is the MFM reasoning patterns, and the other is a proposition indicating a state of one of the functions in the examined pattern. The reasoning engine will try to search the fact base for facts that satisfied all the conditions specified on the LHS, and when a match is found, the rule will be activated. Then the RHS suggests a new proposition according to the inference formula. The proposition that implemented in the software including the following information:

1. the information of the inferred function and state;
2. justifications that the inference based;
3. the rules that are used; and
4. the assumptions associate with the inference.

All of above information is necessary to test the availability and truthfulness of the proposition.

The reasoning software works in two distinguishable steps. One is proposition generation and the other is reasoning maintenance. After a trigger (starting node) and the evidences (abnormal states) are registered to the reasoning system, the inference engine will first generate further propositions based on the rules (encoded patterns and formulas), and then test the availability of the propositions with all the assumptions. Sophisticated strategies and dependency structures are included to test the propositions and retract the false or conflicted ones. All the propositions, after being generated and validated, are organized in a tree structure so that several casual paths can be identified. The assumptions and the dependency structures are useful for interpreting the reasoning result.

Another advantage of using Jess as programming language except its fast algorithm is that it is fully integrated with Java program and can reason about Java objects (as Jess facts) directly. The rule-based system developed by the author is now integrated with the MFM model editor software (MFM Suite), a Java based model building tool developed by Thunem [70] whereby the reasoning result can be displayed graphically with the models.

The reasoning system modules are shown in Figure 4.2. To reason about the cause effect by using MFM models, three basic knowledge bases are required: MFM reasoning rules, the MFM models, and the reasoning propositions.

MFM reasoning rules are independent, which means the rule-base remains the same for all reasoning activities of the same kind for all MFM models. For modularization, MFM root cause reasoning rules and consequence reasoning rules are implemented in different rule bases so that the reasoning process can be initiated separately.

The MFM models has to be loaded to the system before any reasoning process can be done. The MFM models has a special internal representation in the knowledge base, which contains MFM entities and MFM relations. All of MFM entities and relations are defined based on their types (source, objective, influencer etc.) and are assigned with a unique name. All the connectivity information of the model is documented as the property of MFM relations. The transport functions has the special property to identify flow directions. Flow function structures is also defined as MFM entities with unique names and information about the functions that they contained is also documented.

Because the MFM has a set of specific syntax, the syntax verification module is also implemented as a set of reasoning rules. After syntax verification, MFM models are stored in a knowledge base and those information should be available for all the reasoning activities. This knowledge base remains constant during reasoning propagations thus it is called a static data base.

During MFM reasoning, The reasoning processes are initiated by at least one propositions inserted about MFM function states as trigger evidence. The propositions including two different types. One is evidence, which is the functions state according to interpretation of the physical system. The other type are predictions (propositions based on consequence reasoning) or postdictions (propositions based on root cause reasoning). The knowledge base contains information of deduced function states is called dynamic data base, since the information is changing during the reasoning.

The MFM reasoning procedure is demonstrated in Figure 4.2. Since the rule base is already programmed in the system, the reasoning starts with the loading of a MFM model and verification of the syntax. After the syntax has been checked and the model has been properly stored in the knowledge base, evidence is inserted in the dynamic knowledge base. This initiates the reasoning process by call upon the reasoning engine to start firing reasoning rules according to the MFM patterns it recognized from the static database, the function states propositions it recognized from the dynamic database. When a rule is fired, a suggestion of new proposition will be generated. This suggestion will be tested with all the existing propositions to test that whether there's a conflict between the newly suggested proposition and the already validated propositions. If a conflict is found, the newly suggested proposition will be abandoned, and the proposition which result in the newly suggested one will be searched and retracted as well. The reasoning process will be continue until no new rules can be fired. The reasoning result will be collected and stored in a tree structure and presented in the user interface.

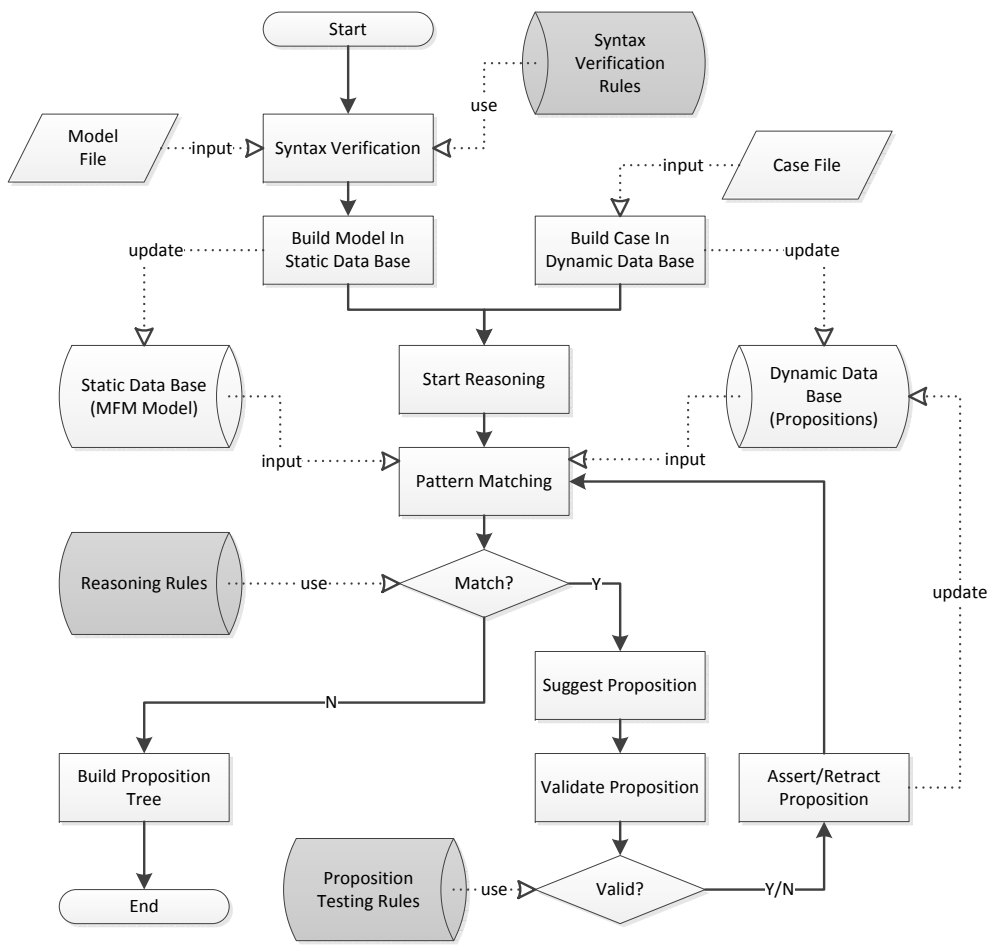


Figure 4.2: Reasoning procedure for developing rule-based system.

## 4.4 Operational Mode

Mode is a system level description about plant operation and it gives context for system analysis. Operational mode is a concept which is closely related to operational situation but the relation between mode and situation is similar to the relation between function and action. Operational mode and operational situation should be defined in the same sphere of the conceptual space, however, the distinguish between the two is also important for situation assessment.

### 4.4.1 The concept of mode

Lind defines modes in [74] as that a mode is the means or the manner (the ways) by which a purpose is reached. Follow this definition, Lind specified the modes of a system in relation to the means-end modeling framework. In the means-end dimension, between each pair of the end and its means, the relation has an interpretation in terms of mode as shown in Table 4.33.

Table 4.33: End-means relation Interpretation in terms of mode.

End $\leftarrow$ Means	Interpretation in terms of mode
goal $\leftarrow$ objective	meeting an objective is a particular way to reach a goal (the purpose)
objective $\leftarrow$ function	performing a function is a particular way to achieve an objective (the purpose)
function $\leftarrow$ role	performing a role is a particular way of contributing to a function (the purpose)
role $\leftarrow$ structure	providing a structure is a particular way to realize a role (the purpose)

Each of the mode interpretations in Table 4.33 leads to two complementary mode types. One type assumes that the end is given and specifies the alternative means (end to means). The other type assumes a given set of means and specifies the end which they achieve (means to end). MFM models are by definition multilevel representations and the mode types defined above would in most practical cases produce hierarchical mode structures, which is to say one mode may include a combinations of sub-modes of various types. As an example, an objective mode could include several function modes. Lind defines a set a mode which can be represented by using MFM models. However, in the current version of MFM modeling facilities, the means-end abstractions only defines three level of concepts: objective, function, and structure. Since the means-end relation follows the rule of transitivity, modes based on those three level of concepts can



be abstracted according to the MFM modes definition. This is shown in Table 4.34.

Table 4.34: End-means relations in MFM and corresponding modes types.

End←Means	Purpose	Mode type
objective←function (produce, maintain, destroy, suppress)	To reach the objective	<b>Function-objective mode (end-to means)</b> A mode is here defined as a set of system functions used to realize a given objective. A mode would then be described the objective and a flow or control structure and there could be different alternative structures for the same objective each characterizing a particular process or control mode for the system.
		<b>Objective-function mode (means to end)</b> A mode is here defined by an objective which is served by a set of given functions. There could be several objective-function modes because different alternative objectives may be served by the same set of functions.
function←structure (realize)	To realize a function	<b>Structure-Function mode (end to means)</b> A mode is here defined as a set of physical components which realize a given function (through fulfill a particular role). Different components can realize the same function. Each set of components and the function would define a mode. This mode concept is useful for describing redundant components in the system.
		<b>Function-Structure mode (means to end)</b> A mode is here defined by a set of functions which is realized by the same component or components configuration.

During operation, it is efficient to analyze the system from a top-down manner which means that the operational situation is defined by the top level of objective and to analyze the alternative means to achieve it. Also the operational situation is defined by goal(objective) fulfillment, that is to say the situation is corresponding to a function-objective mode in MFM, and different structure-function modes, is enclosed in one situation. When considering operability of a

special components to fulfill other function goals out of design perspective, the function-structure modes and objective-function modes are useful because the analysis of modes provide alternative functionality of the system components.

#### 4.4.2 Mode shifts and definition of operational situation

The MFM mode types defined above can be used to characterize transitions during different plant phases through means-end relations. [74] A transition could be between modes of same type, for example between two function-objective modes when there is a transition between alternative function sets for the same objective. If the primary objectives remains the same in the system, however, the objectives are unfulfilled, a mode change is required either from function-objective relations or the structure-function relations. In the later situation, an example could be that a redundant component has to be used to realize the same function (the structure-function relation changes) so that the same objective fulfillment can be restored. In the former situation, the function structure has to be changed (the function-objective mode changes) for no structure combinations can realize the same function structure. When the function-objective mode changes, the physical structures may have to be re-configured as well. The mode change may be very complex and require a full understanding of operation constraints.

The modes transitions indicate the operability of a system, which means they indicate the changes of actions for fulfill the objective, or the structures who serves a role in the action. On top of the changes of functional perspectives, there is also the suggestion and command for the mode shift which is of great importance for situation assessment. Considering another situation, if the primary objective cannot remain the same in the system after an objective failure, new objectives has to be defined so that the current available functions (who can be realized by the available structures) can realize them. The change of objectives indicate a shift of perspective in a system level, which marks a new situation. All levels of the means-end structure need to be changed according to the new objectives. In this light, MFM can be used to organize operational knowledge of the system, by representing a system in different operational modes. The modes shifts is used to define operational situation in the assessment procedure in next section.

To summarize this section, an operational situation in MFM is defined as the system is operating to fulfill the same set of objectives. A secured situation is when the function-objective mode of the system can maintain the fulfillment of the objectives without function-objective mode shifting in the near future. The mode shift between different function-objective modes or different structure-

function modes are defined as operational modes within the same situation. An operational situation constitutes of all operational modes which maintain the fulfillment of the current system objectives. The operational situation becomes problematic when the mode shift within the situation is required.

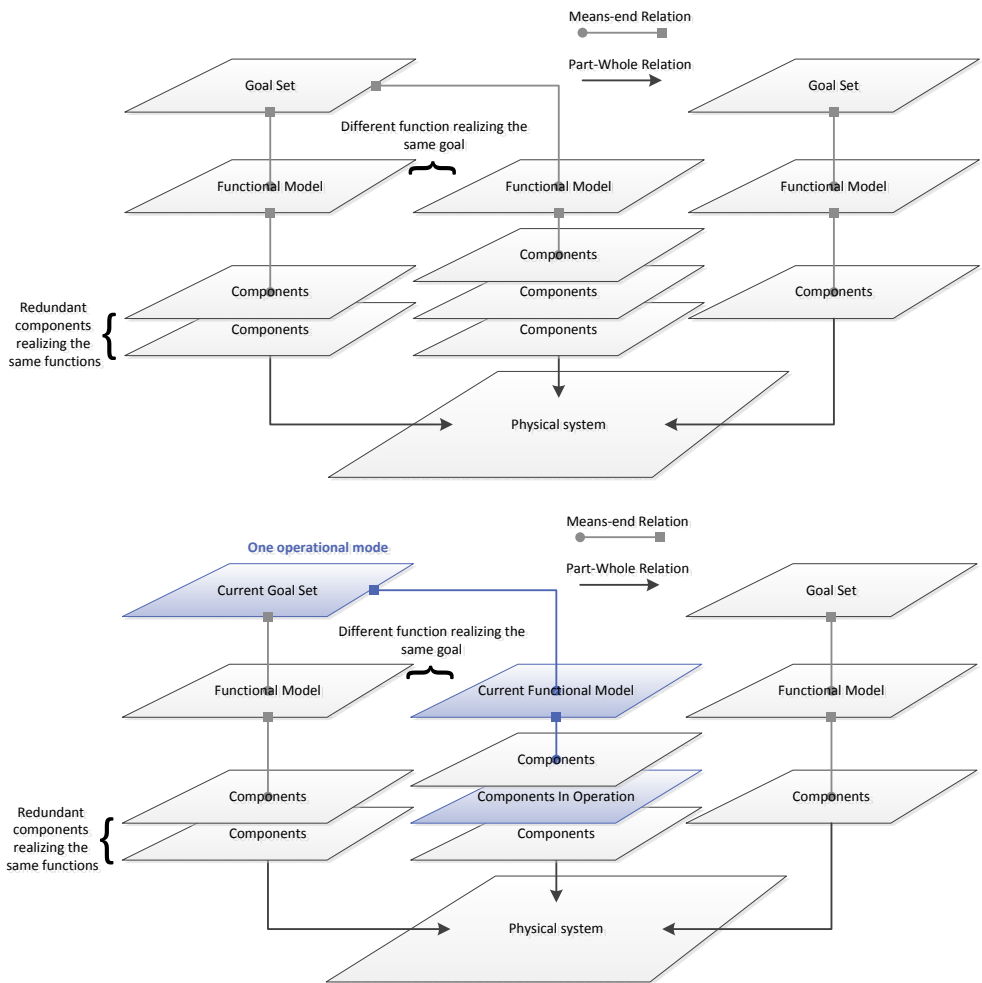


Figure 4.3: Operational modes in MFM.

## 4.5 Representing operational knowledge

From the previous modeling procedure in Chapter 3, it is obvious that building MFM model for a specific system requires a significant amount of process knowledge as well as operational knowledge. For example, to model the means-end relations between the boron injection and removal function structure and the energy source in the energy flow in Figure 3.18, the modeler has to understand that how the operation can be done (the possibility of injection and removal). This knowledge can be used to specify the actuation control roles associated with MFM flow functions. [72] The control actions of manipulating the physical system to achieve the control goal can either be done by using automatic control system or human operator. For boron control in PWR plant, both manual and automatic control are available. A set of four MFM control functions is defined in MFM ontology. [59] In contrast to the classical signals and systems perspective, control functions have a special role in the perspective of means-end modeling. Control function structures represent a system's operational intention structures explicitly while the intentional structure for operation is only implied in the process function representations. Comparing the human operation and the automatic control added to the process, though the means and media for assessing situation and response are very different, the operational intentions are the same. Therefore, the author of the present thesis also propose to use the MFM control functions to model human operator action.

By using the same control functions to represent automatic control action and possible operator action together also serves the purpose to help the human operator to understand the automatic control systems. Zhang et al. introduce the idea of representing operational knowledge by using MFM control functions in [75]. This work requires more theoretical support thus the result is not included in this thesis for situation assessment procedure.

## 4.6 Chapter summary

This chapter discusses the intersubjective aspects of a situation and makes the connection between the system goal and functions with different elements in the intersubjective situation. A situation is represented by using MFM models, the assessment procedure requires the assessment standard to evaluate MFM functions status and performances. By using means-end and the relation between functions and actions, a set of MFM function states is defined in this Chapter. Causal reasoning rules is explained in detail in this chapter and the implementation of a rule-based system for MFM causal reasoning is briefly introduced.

The concept of operational mode is explained follow the previous work by Lind [74] and the mode shift is explained. The operational situation is defined based on objective-function mode. In the next chapter, the assessment procedure will be developed based on the concept of situation which is developed in this chapter. A case study will be introduced by using the PWR model.



## CHAPTER 5

# Operational Situation Assessment

---

In the previous chapter, the MFM modeling methodology is extended to be used for representing both the process knowledge, and the operational knowledge. This chapter elaborates further the requirements for situation assessment and demonstrate how the MFM models can be used for this purpose. Firstly, the situation assessment procedure is provided and a case study with the PWR model which is developed in Chapter 3 is used for the demonstration.

## 5.1 Procedure for functional assessment

Section 4.2.2 analyzes what aspects are need to be assessed for an operational function, and based on the action phases, each function status can be reached only by first reaching the previous status. It had been argued that during operational situation assessment, the essential evaluation aspect is the goal achievement of an operational function. Considering a single function, the goal is usually achieved by the stable performance of an action or a successfully performed action. Therefore if the goal is not successfully fulfilled, the execution of the action needs to be examined. If the execution of the action is not properly carried out, the opportunity to take the action and the availability of the physical entities need to be evaluated to determine the status of the function. This is the process of the diagnostic assessment for a single function, which is illustrated in Figure 5.1.

Considering the means-end relation and the action phases, abnormal perfor-



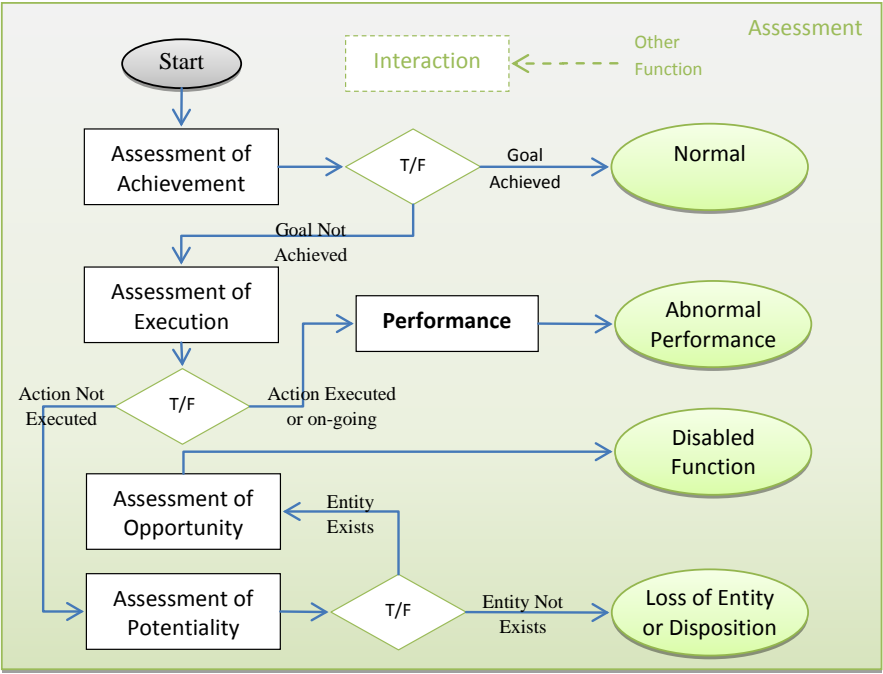


Figure 5.1: Diagnostic assessment procedure for single functions.

mance, disabled function, or loss of physical entity must happen no later than the failure of goal achievements. For an engineering system, various instrumentation systems is deployed and they provide additional observability (for example, detection of mechanical failures or abnormal function performance states) of the system rather than the goal fulfillment. In this case, prognostic assessment can be performed for a single function. For example if the loss of entity can be detected at an early stage, the failure of goal achievement can be predicted if no alternative action is performed. Figure 5.2 shows the prognostic assessment procedure for a single function.

Figure 5.1 and Figure 5.2 explains the assessment of a single function. A function’s status or states can also be influence by other functions due to dependency relations. This influence can happen at any stage of different action phases. For example, a goal of a function can be “to provide potentiality or opportunity of another function”, or “to influence the performance of another function”. In MFM models, the causal dependencies of functions and objectives of a system is represented explicitly, and the functional assessment can be performed in a functional level.

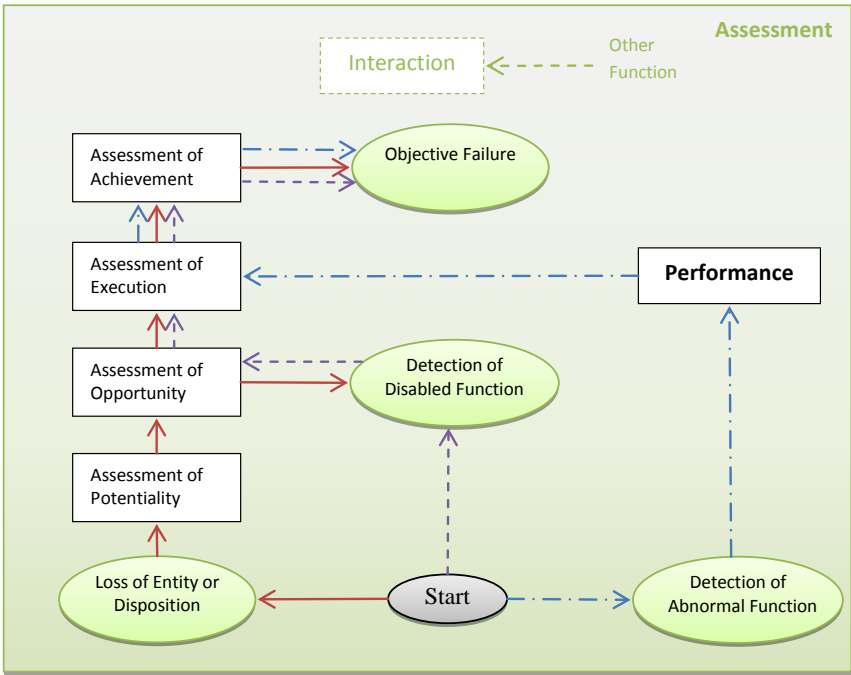


Figure 5.2: Prognostic assessment procedure for single functions.

The situation assessment procedure is initiated by the detection of an abnormal event. It is assumed that prior to this abnormal event, the system is operated in one operational mode, which means a specific set of physical components are in use to perform actions to realize the system functions, so that the system functions are all in normal states to realize the a set of system operational goals. As indicated in Figure 5.2 the detection of the event can be from either means-end level of a single function node. However, the prognostic assessment indicates a possible failure in realizing the functional objective in any case of the detection of the abnormal event.

A single functional performance abnormality will further influence other functions. The analysis can be done by using MFM models to perform consequence reasoning for this operating mode. Mean while, the diagnostic analysis should be done to find the root-cause of the losing of the function, since a single function failure can be a result of any one of the three possible scenarios: abnormal performance, disabled function or loss of physical components. In the third scenario, the function itself is the root cause for the failure in function realization. In the second scenario, the function is conditioned by other subsystem

who realize a function structure in the functional level. Thus further functional root-cause analysis can be performed when the function structure is presented in the MFM model. Otherwise, the function itself can be considered as the root-cause of the failure in the functional level. In the first scenario, the functional performance is dependent on the flow functions in the same function structures in MFM, therefore, a root-cause analysis should be performed to trace the dependency structure backwards to find the root cause in the functional level, and then analysis how the root cause function is realized by physical structures. This is done also by using the MFM model of the specific operating mode.

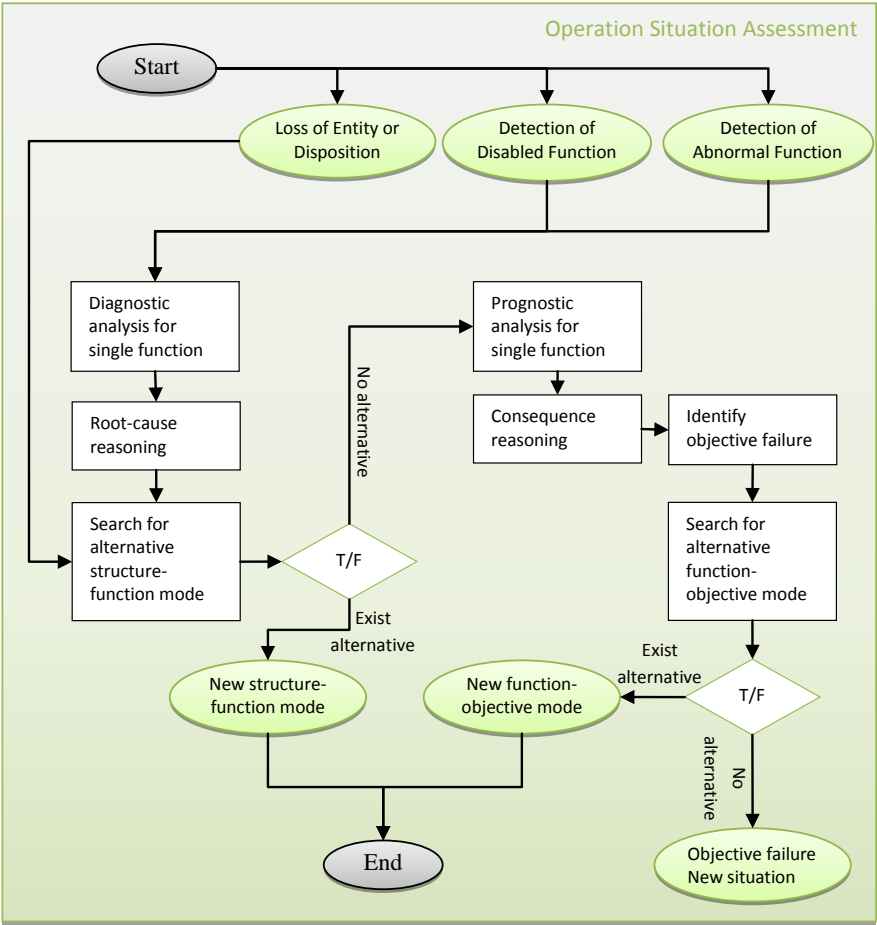


Figure 5.3: Operational situation assessment procedure.

When the situation becomes problematic after an abnormal event happens and

is detected, the diagnostic analysis result is important for indicating how the function-structure operation mode should be changed so that the failed function can be realized by alternative means (physical structures). For example, there might be redundant components who can realize the same functions. Thus those components should be activated so the abnormal function can be re-established and return to a normal state. The operator's task is to activate or to monitor the activation by automatic control system. The procedure may contains several different steps of observations and actions which is beyond the present modeling scope of functional models, thus detailed action plan (operating procedures) should be available.

However, if the root-cause function cannot be re-established and brought back to normal state, the situation assessment should be proceed to analyze the prognostic result. The prognostic analysis will predict further function failure by tracing the dependency relations, and eventually objective failure of the system. In this case, the objective-function mode should be change so that another set of function structure should be selected to realize the same objective. There might be a situation when not all the objectives of the system prior to the abnormal event should still be presented as major objectives. Normally, the safety objective should be the primary concerns in of the system.

Following the above discussion, the situation assessment procedure is summarized in Figure 5.3. It is important to notice that if there's no function-objective operation mode available for the current state of objectives, a change of system objectives is required. Normally, during abnormal situations, the safety objectives should be set as primary objectives so that the plant can be restored and bring back to the normal situation. When the objective structure changes, the dependency relations in MFM can be used to analyze which functions are required to realize the new function-objective mode based on the new objectives. This however, has not yet been automated and implemented in the MFM Suite. Thus some of the analysis in the following sections are done manually.

## 5.2 Function structure relation

MFM models decompose the physical system in multiple dimensions (both means-end and part-whole), so the connections between individual MFM function and physical components are not obvious. One MFM function may be realized by a set of different physical components either in the same time period or in different time periods, while one physical component may provide the means to serve different functions either at the same time or different time. As introduced in Chapter 4, these defines a set of structure-function modes and

function-structure modes.

The function-structure relationship is a fundamental problem related to the theoretical aspect of the functional concepts, which is still an open issue in extending the MFM methodology itself. The functional models without the function-structure connection can be used for system level analysis by itself, when the different nodes for initiating the situation assessment in Figure 5.3 is treated with the same procedure and go through two diagnostic steps and all prognostic steps in parallel. However, the observations for function states is still deeply depending on the states of the physical system. To limit the scope of this thesis, and focus on the functional analysis, a direct connection between function states and the components measurements during operation is established in MFM Suite without considering the complicated mapping from physical structure to its functionalities. The purpose of setting up the connection is to interpret the measurements coming from the process simulation (or potentially a real plant) as function states according to human understanding of the process and the scenario.

Any further analysis in the physical level requires detail modeling between physical structure and MFM functions which is not part of this Chapter but will be discussed as perspective based on the work of this thesis.

After obtaining the function states through measurements from the instrumentation system, MFM model can be used for diagnosis and prognosis as already introduced in the reasoning section in Chapter 4.

### 5.3 Case Study with PWR primary system

In this section, the PWR primary system that is being modeled by using MFM is used as the study case for demonstrating two key points in situation assessment. The first is to show the importance of using functional models in different operational modes. The second is to demonstrate that how the assessment procedure is applied. Note that the model developed in Section 3.2 is used in this section, thus reader may require to refer to Section 3.2 while reading this section.

### 5.3.1 Cause and consequence reasoning for a LOCA situation

In Chapter 3 Figure 3.18, a comprehensive MFM model is developed to representing all the functions of the physical system that is illustrated in Figure 3.12. This model can be used for causal reasoning directly without modeling specific operational modes.

As already explained, to obtain function states from real simulation cases, a process model view has been developed in the MFM software, MFM Suite. The current version of the MFM Suite includes four type of measurements in the process model view, namely: temperature, pressure, volume, and flow rate. Temperature, pressure and volume measurements can be indicators for the state of a storage function in the MFM model depending on the specific modeling case, while the temperature and flow rate measurements can indicate the state of transport function. This will be elaborated further with the PWR example. Note that the current software implementation is specially programmed to interface with the RIPS simulator provided by IFE Halden Reactor Project through an on-line dynamic display system as data buffer. Therefore, the data that is gathered in the process model are not measurements but indicators. The simulator simulate multiple sensor values for the same component. The display system will process the sensor values and visualize the measurements in various graphical representation, including absolute value and the relative value to the alarm boundaries. This offers a short cut for using the indicators provided by the display system and those indicators can be translated in qualitative function state directly by applying the alarm limits set by the display system.

The process model is developed in MFM Suite as shown in Figure 5.4. Various sensor-shapes in MFM Suite are attached to different components based on the simulator displays. The sensor values are directly imported from the simulator. The key indicators are listed in Table 5.1. Figure 5.4 also shows a pop-up window for one of the steam generator pressure sensors and the pressure level in relative to the alarm setting. This sensor indicator is linked to a MFM function shows in the bottom left corner in the figure. The indicators' connection to MFM functions in Figure 3.18 is also listed in Table 5.1.

Note that in the physical system, the low pressure safety injection pump works as CVCS injection pump during normal operation, thus the indicator is associated with two transport function states (tra16 and tra36 in Figure 3.18 in Section 3.2). This shows the first hint of conflict by using a complete model for operational analysis, because there are different structure-function operation modes involve. Another point is that because the cooling loops are represented as one mass circulation in the functional representation as an abstractive view, either of the

Table 5.1: Indicators that are used for the PWR case study.

Components	Measurements(MFM functions)
Steam Generator	Volume( <i>sto4</i> ), Pressure( <i>sto17</i> )
Reactor	Temperature (Cold-Leg( <i>tra18</i> )/Hot-Leg Temperature( <i>tra20</i> ))
Pressurizer	Volume( <i>sto3</i> ), Pressure( <i>sto20</i> ), Temperature( <i>sto22</i> )
Pressurizer Relief Tank	Volume( <i>sto2</i> ), Pressure( <i>sto21</i> )
Reactor Coolant Loop	Flow-Rate( <i>tra11</i> )
Cold-Leg Collector	Volume( <i>stowe</i> )
High/Low Head Safety Injection	Flow-Rate( <i>tra37/tra36, tra16</i> )
VCT Tank	Volume( <i>sto7</i> )
Reactor Water Storage Tank	Volume( <i>sto14</i> )

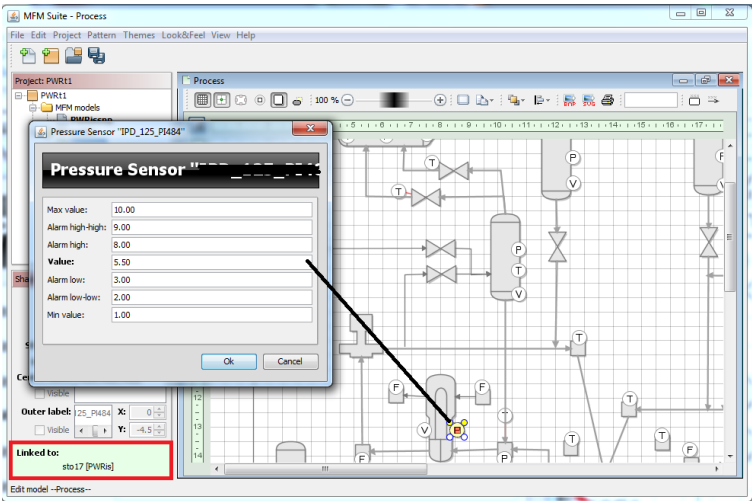


Figure 5.4: MFM Suite screen shot for the process view and sensor value dialog.

steam generator has abnormal states, the associated function state will be set accordingly.

A LOCA situation is tested by using the complete model to perform diagnostic and prognostic analysis. A loss-of-coolant-accident (LOCA) is a mode of failure for a nuclear reactor; if not managed effectively, the results of a LOCA could result in reactor core damage. The nuclear plant’s emergency core cooling system (ECCS) is installed specifically to deal with a LOCA.

Nuclear reactors generate heat and the RCS is used to transport this heat to the secondary system where it is converted it into electrical power during normal power operation. If the coolant flow in the RCS is reduced, or lost altogether, the nuclear reactor’s emergency shutdown system is designed to stop the fission chain reaction. However, due to radioactive decay the nuclear fuel will continue to generate a significant amount of heat. The decay heat resulting from a reactor shutdown from full power is initially only of a very small proportion of the thermal rating of the reactor. The emergency cooling system is designed to step in to replace the RCS and cool down the reactor. If the emergency cooling systems fails to operate, the heat produced in the reactor can increase the fuel temperature to the point of damaging the reactor. There are several level of defense to prevent the loss of emergency cooling capability. First of all, the cold leg collector will response to the pressure drop in the RCS and inject additional coolant into the primary RCS circuit to prevent a total loss of coolant. Then the safety injection pump will use additional water resources from the RWST for the continuation of cooling. If the volume of the RWST turns low level, the coolant leaked to the containment building can be recirculated back into the cooling circuit.

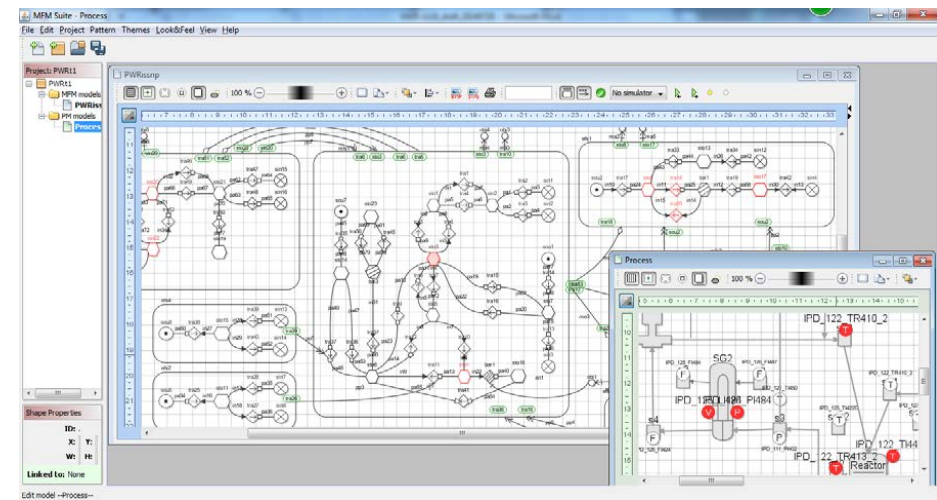


Figure 5.5: Fault propagation between flow structures in a LOCA situation. (Functions with same color indicates the functions is connected through means-end relation to the energy flow.)

There are several different types of LOCA events. In the testing scenario, the LOCA in this test case is simulated to start with a leakage in the main RCS. The consequence of the loss of coolant is that the energy balance will be disturbed and the functions of: *sto3*, *sto4*, *tra18*, *tra20*, *sto20*, *sto22*, and *sto17* in the



MFM model in Figure 3.18 will be affected because of a drop in pressure and volume in the main components. The secondary system will be shut down so the sink function *sin4* become disabled. Through consequence reasoning, the result shows failure in objectives of power production (*obj2* and *obj5* in Figure 3.18). The abnormal functions are also shown in Figure 5.5 in red color. The causes identified through MFM reasoning in Figure 3.18 is there's fault happens from *sou2* to *sin2*. Since the *tra18* is an end function whose state is influenced by the mass flow structure, the root cause reasoning continues to the mass flow level. Also because *sou2* is connected to the boron injection flow structure and the rod control structure, the root cause reasoning is continued in those two flow levels which indicates that the amount of boron *sto9* and the length of control rods insertion *sto10* are in low level. Another possible fault is a low flow value in *tra33* (represent the emergency cooling energy sink) and this function is influenced by the emergency cooling functions in the mass flow.

To summarize the root cause reasoning result, the possible causes for the abnormal functions states along the energy flow through *sou2* to *sin2* in *efs1* can be due to 4 major root cause path: (the functions marked in color in Figure 5.6 shows the connection between functions between different flow structures.)

1. Due to the mass flow functions provided by the RCS (*tra10* influence *tra18*),
2. Due to the mass flow functions provided by the rods insertion (*sto10* influence *sou2*),
3. Due to the mass flow functions provided by the boron injection (*sto9* influence *sou2*),
4. Due to the mass flow functions provided by the emergency cooling (*tra36* and *tra37* influence *tra33*).

This reasoning result shows difficulty to represent the situation precisely because when LOCA happens during the normal production, the emergency cooling and reaction control methods should be activated when the fault is detected rather than to be considered as a root causes before its activation. Although the information gather from the physical system which indicates *sto3* and *sto4* in low states conforms that the real root cause is the RCS system functions in the mass flow level, however, the other functions should not be presented in the system during the diagnosis process.

The consequence of the situation is that the source function *sou2* will be overheated and *obj2* and *obj5* for maintain the cooling of the reactor and deliver

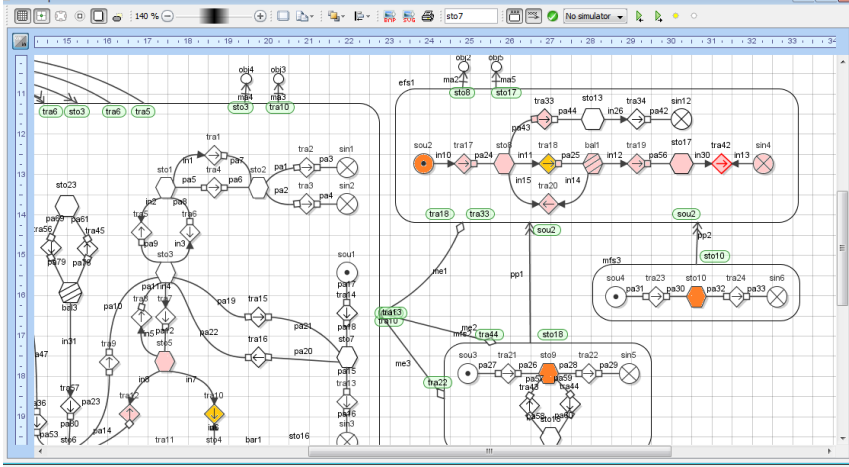


Figure 5.6: Operational situation assessment procedure.

the energy to secondary will fail. It is also worth noticing that after the event of LOCA, the objective for the energy flow structure changes from maintain energy production to maintain the energy removal. This changes indicates a objective-function mode change which indicate a change of situation.

### 5.3.2 Modeling different function-objective modes

According to this analysis using an MFM model of the PWR, it is clear that models for each operational modes should be defines so that the situation assessment then can be done properly. The energy and mass flow of energy production mode should be modeled as in Figure 5.7, where compare to the previous complete MFM model, the emergency cooling system is removed from the operation model. The pumps' energy flow structures are omitted for the purpose of simplification, which means that *efs2*, *efs3* and *efs4* in Figure 3.18 will not be presented in the operational mode models. And the pressurizer also lost the ability to control the pressure, which means that *efs5* in Figure 3.18 will not be presented in the operational mode models.

For the energy flow functions, two additional operation modes can be identified. First one is when the RCS system is not in a complete disabled status, however the pressure drops will activate emergency cooling though cold-leg collector tanks. In this mode, two energy sinks co-exists in the energy flow structure as shown in Figure 5.8. However, the system objective change to maintain the

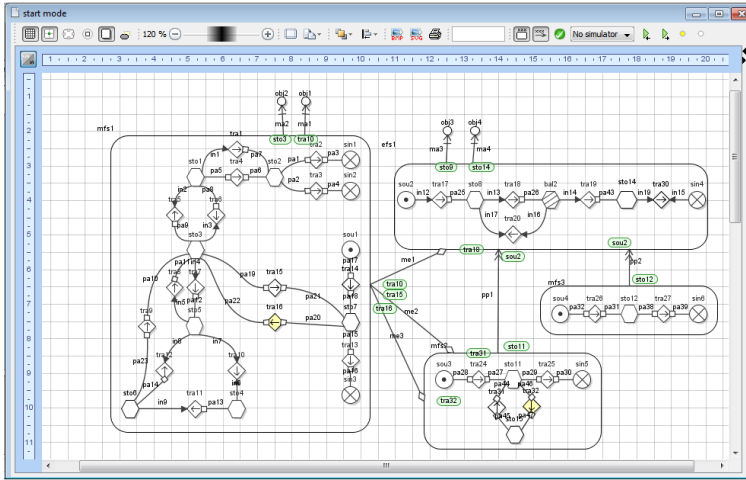


Figure 5.7: Operation mode for LOCA initiative.

energy removal instead of energy production.

The shutdown procedure is automatically initiated and the control rods and boron injection should perform so that the source function in *efs1*, changes from the original energy source to the decay heat. After this action is finished, the flow functions for control rods and boron injection process can be omitted for the source function in *efs1* changed. This will be shown in the second emergency cooling mode in Figure 5.8.

The second emergency cooling mode is when the RCS function is totally disabled because of the shutdown procedure and the emergency cooling pumps are activated. In this mode, only one energy sink presented in the functional level. The function-objective mode changes because that additional mass flow function join forces to serve as functional means to mediate the removal of energy. This operation mode is shown in Figure 5.9

The third function-objective mode is when the cold-leg collector is empty out, and the valves should be close due to operation procedure. So that only the emergency injection from the RWST is still present in the functional model as means to realize the energy removal in the energy level. The model of this mode is shown in Figure 5.10

The last function-objective mode is when the RWST is in a low level, the leakage in the mass flow become a transport function so that the injected water leaked to the containment building can be recirculated and used again. This mode is

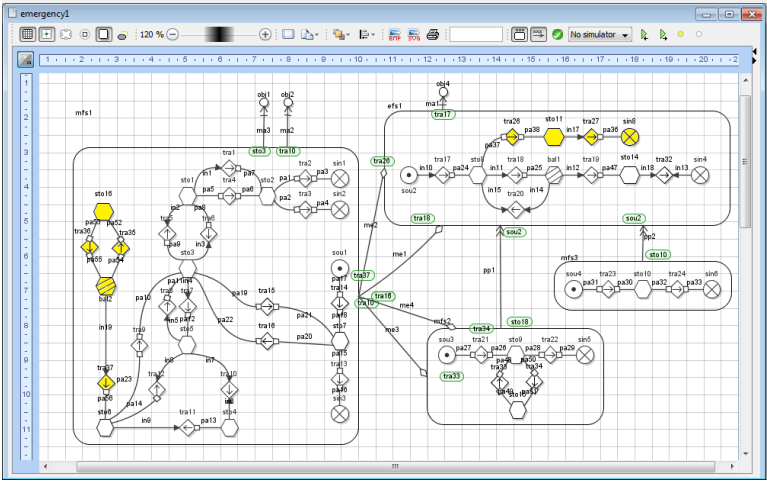


Figure 5.8: Operation mode for the first emergency cooling mode with cold-leg collector activated

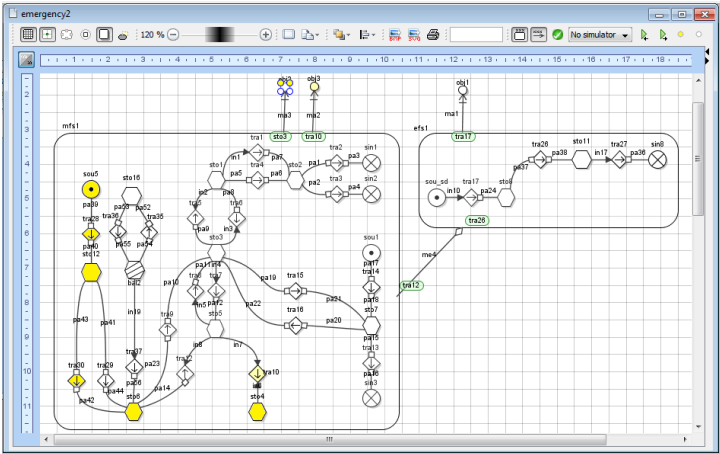


Figure 5.9: Operation mode for the second emergency cooling mode with emergency cooling injection started

shown in Figure5.11.

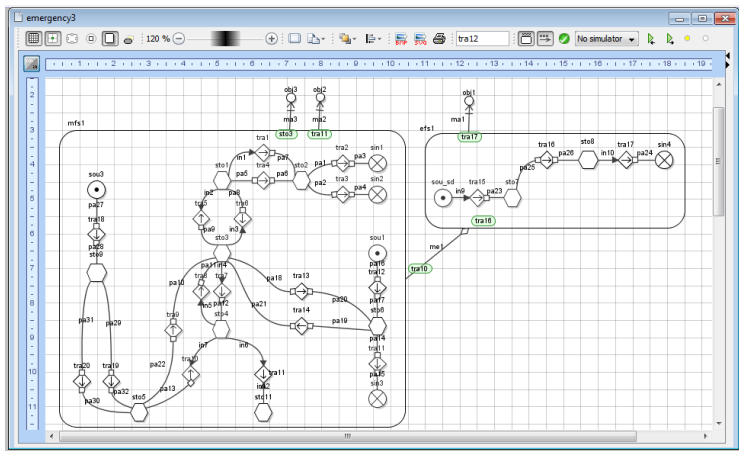


Figure 5.10: Operation mode for the third emergency cooling mode with cold-leg collector valve shutdown.

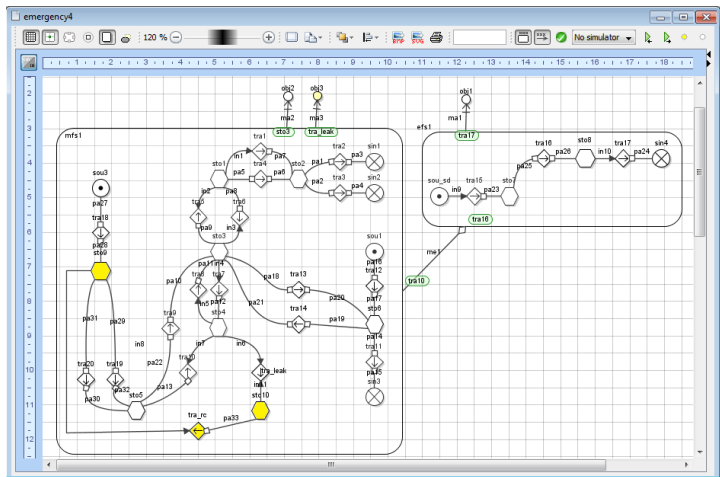


Figure 5.11: Operation mode for the fourth emergency cooling mode with water recirculation from the containment building.

5.3.3 Applying the situation assessment procedure

When the five function-objective modes are developed for the same set of objectives of heat removal in the energy flow, the set of operational modes are all included in one operational situation and the mode changes due to searching for functional alternatives to realize the same set of objective. The situation

assessment still start with abnormal events where, according to the previous cause and consequence analysis in the MFM model, the RCS malfunction is identified. The operator's task during this situation is to monitor the automatic shutdown procedure ensuring that it is successfully deployed. In this situation, the objectives and function structures changes because the loss of functionality and unfulfillment of goals.

The MFM model in Figure 5.7 should be used to replace the previous used PWR MFM model in Figure 3.18. The monitoring tasks for the operator is to ensure that the new function model for the new situation starting mode is in normal state. Note that the function states in the new mode will change because the indicator level limits should be updated whenever the operational mode changes. After the safe shutdown of the reactor, the operator's task changes into monitoring the status of the decay heat removal. The functional model for the system changes whenever there's changes in the functional status. For example, when the *sto16* in the operational mode shown in Figure 5.9 become low state, the operator need to be warned so that the procedure of shutdown the cold-leg collector valve should be done. When the action is performed, the function disappear from the functional model so that a new operational mode is reached. The failure in performing the action will result in other mode change rather than the operational mode illustrated in Figure 5.10.

The consequence of not performing the close valve action will result in the gas generated in the RCS system entering the collector tank which is an undesirable situation. This mode can be modeled in MFM as in Figure 5.12. There will be a reverse transport function in the mass flow level (*tra37* in Figure 5.12).

Operational knowledge can also be modeled together with the process operational mode as introduced in Chapter 4. The action performed by the automation system serves as links between different operational modes models. If Figure 5.7 to Figure 5.11 are numbered as LOCA mode 1 to 5, while Figure 5.12 is numbered LOCA mode 4.1. The mode shifts in relation to the operation can be demonstrated as shown in Figure 5.13.

As defined in Chapter 4, once the plant reached the stable situation, the heat removal will be kept for longer period and no mode shift is required in the near future. This is when the situation is secured.

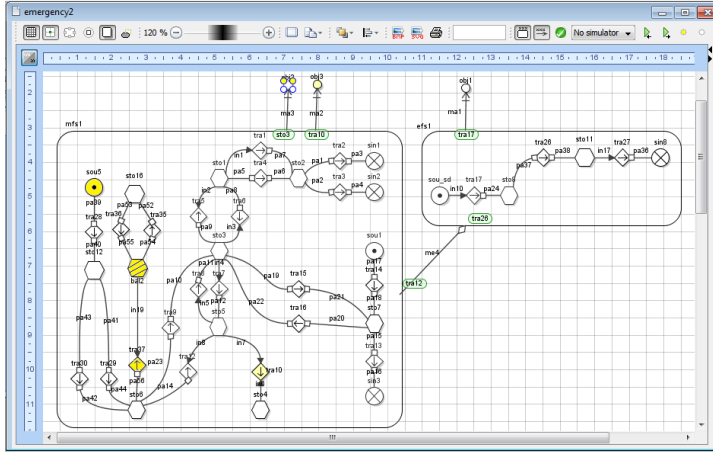


Figure 5.12: Operation mode for the fourth emergency cooling mode with water recirculation from the containment building.

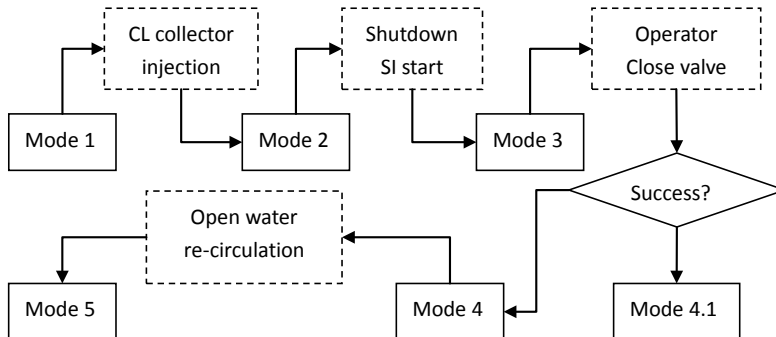


Figure 5.13: The Mode transition through a LOCA shutdown situation.

## 5.4 Chapter summary

In this chapter, the situation assessment procedure based on MFM models is introduced. The procedure includes three primary steps. The first is to detect an abnormal event and to perform cause and consequence analysis to detect the root causes and possible consequences of objective failure. Once an objective failure is detected and no alternative functions can realize the same set of objectives. The system enters a new situation thus new objectives has to be identified. New function-objective mode need to be established by using existing functionalities. the setting up of new stable function-objective mode may go through a series of function-objective mode shift follows control actions and operations. Once the system enters a new stable state of functional-objective mode, the new situation is secured. The PWR primary models is used to demonstrate the assessment procedure and cause and consequence analysis is performed by using MFM models and 5 different LOCA modes is modeled along with the possible mode changes.

The MFM models provide process knowledge about system goal and functions and by using MFM, the concepts of operational modes and operational situation can be formalized so that the model for a specific operational mode can precisely identify the current functional elements. Since MFM models can also be used to reasoning about causes and consequences, it is also support the comprehension and projection of an operational situation.

Software tools need to be developed further to support the full functionality for using MFM to represent operational situation and perform situation assessment. The suggested implementation is listed in the next chapter.





## CHAPTER 6

# Conclusions and Perspectives

---

This thesis has reviewed different perspectives on situation awareness in the human factor studies and uses the knowledge reflectively for system representation and analysis. The human cognitive activities during complex plant operation and how they perceive a situation and what kind of knowledge has to be established in the human mental model for the operators to be aware of the situations has motivated the utilization of functional representation in system level of situation assessment. The thesis has summarized the MFM syntax and provides detail instructions of how to model by using the modeling technique. A PWR primary system is used as a comprehensive modeling case to demonstrate the MFM modeling procedure. Then the thesis investigates the usability of functional modeling approaches to define and model a plant operational situation. MFM modeling is proposed because it is a formalization combining the means-end and part-whole dimensions of a system, so that the MFM models can therefore represent a complex system at several abstraction levels. MFM models also model cause-effect dependencies of functionalities and objectives of the system in different abstraction levels, so the model can be used for causal reasoning. This thesis extends the causal reasoning methods for MFM models and exploits the ability for MFM models to represent operational knowledge and operational modes. Both concepts are of great importance for situation assessment. By applying the extended MFM theory, situation assessment procedure is developed to assess the plant operational situation. The assessment procedure is demonstrated on the PWR model case. Some key contributions and perspective of this thesis is summarized in this Chapter.

## 6.1 Contributions

1. Contribution to definition of the intersubjective aspects of an operational situation:

Various studies suggest that although situation awareness is a subjective concept, support for operator's situation awareness can be improved through system design or external tools in combination with training and education. This indicates the intersubjective aspect of the situation assessment tasks which relies on a formalization of the plant operational situation. This thesis argues that the intersubjectivity of a situation, should be defined through system analysis rather than the operators' task analysis, which is the traditional approach in human factor. This is supported by the ecological display design and functional design methodologies. However, the thesis further argues that the system analysis should be done by using proper functional modeling approach rather than using Rasmussen's abstraction hierarchy [7]. There are several motivations:

- (a) the dynamic information (operability, actions) of the system's functionality should be included in the system analysis.
- (b) The dependency relations should be properly represented so that the cause-effect relations becomes explicit knowledge to support causal reasoning process.
- (c) The means-end and part-whole decompositions should be combined to deal with the system complexity while not losing the cause-effect dependencies between different elements on the same means-end level.

Following these motivations, the functional modeling approach MFM is proposed to be used for situation assessment.

2. Extension of MFM Modeling methodology for using MFM models in situation assessment tasks:

The existing MFM theory supports means-end and part-whole decomposition in the representation of a complex engineering system. The MFM flow functions and control functions are defined based on the concept of actions. MFM also represents cause-effect relations explicitly so that the MFM models can be used for causal reasoning. A previous prototype of root-cause analysis expert system software were implemented by Petersen [2] with an early version of MFM concepts without causal roles representation. This thesis provides a detail methodology for how to implement the cause effect reasoning in MFM by using the new version of MFM models. Firstly, the MFM function states are further formalized based on the assessment requirement for means-end structure. Secondly, the thesis provides a detailed explanation of how to implement reasoning rules for both part-whole and means-end dimensions.

This thesis also extends MFM to represent operational knowledge so that it suggests a differentiation between causal reasoning within an operational mode and between operational modes within an operational situation. This differentiation provides basis for the development of situation assessment procedure based on MFM methodologies.

3. The definition of an operational situation in relation to operational modes: This thesis provides a definition of operational situation based on how MFM models can represent operational modes. The MFM models' ability to represent operational modes based on the means-end structure is critical for using MFM to represent operational situations. The intersubjective aspect of an operational situation is about the operability of the plant during a particular chain of events' happening. How operational modes should be initiated to fulfill the system objective is the crucial knowledge for the human operator to be aware of during abnormal situations.
4. The development of assessing procedure for operational situation: Finally, this thesis provides procedures for assessing operational situations based on MFM models. The procedure starts with the identification of abnormal events and loss of functions in the system. Then root cause reasoning should be performed searching for alternative structure-function modes or function-objective modes. When there are no alternative operation modes for the current set of objectives, it is required to define new objective-function mode based on new system objectives which can be realized by using available functions. A series of function-objective mode change might be necessary to reach a new secure situation. The diagnostic and prognostic components of the situation assessment have been implemented by using rule-based system. The other components of the assessment procedure are not implemented yet. It has been concluded that model different operational modes is critical for situation assessment.

This thesis also provides some minor contributions to the functional modeling methodology and tool implementation. They are summarized as follow:

1. In contribution of MFM modeling procedures: Previous literature provides insights of how to build MFM models and demonstrate MFM models for a various industrial plants. However, there's no comprehensive instructions for how to model the system by using all MFM facilities e.g. means-end relations and causal roles. Chapter 3 provides a comprehensive modeling guide to readers who is interested to use MFM for modeling process knowledge.
2. In implementing rule-based system for model-based reasoning application: The thesis also provides a general framework to implement a rule-based

reasoning system for model-based reasoning application. This is introduced in Chapter 4.

## 6.2 Perspectives

The presented research offers theoretical justifications and foundations for applying MFM, a functional modeling approach, for situation assessment. And this provides a theoretical foundation and provides several perspectives for approaching real system implementation of MFM-based operator support tools.

From the off-line reasoning results, the problem with representing safety functions together with plant process functions can cause the reasoning system to produce incoherent results. Therefore, the addition of different operation mode models is proposed for future study.

The author proposes to use MFM control function to model the transitions between different function configurations between different models. For example, in the model representing the RCS system during normal operation, power production is the only energy sink at the energy level. IF the RCS system fails to realize the heat removal functions, the MFM causal reasoning provide a prediction of objective failure. The control function actuate on flow functions in response to the change of state in MFM objectives. Thus the new function needs to be enabled through control actuation (change of function-objective mode). Under this assumption, the control functions can be used for representing mode shift. However, this requires more study on the means-end decomposition of the control system.

Currently, the MFM Suite's reasoning package cannot handle model transitions. Further study and development is required to support reasoning using multiple models. This problem probably requires control function reasoning to be implemented as an additional reasoning package.

1. The interface for MFM software, the MFM Suite, and the process simulator display system has been programmed so that the information can be generated from the simulated data. The next step of the research should focus on testing of the usability of MFM models for online reasoning. This has not been done in this thesis. The online cause and consequence reasoning requires the handling of temporal information which is an important further research subject.
2. In the MFM Suite, Multiple MFM models can be developed within the

same MFM project. This functionality of the software should be further extended to support MFM operational modes models. The organization of the data structure is not straight forward and requires proper organization.



# Bibliography

---

- [1] F. N. A. I. I. Commission, “The official report of executive summary the fukushima nuclear accident independent investigation commission,” The National Diet of Japan, Tech. Rep., 2012. [1.1](#)
- [2] J. Petersen, “Knowledge based support for situation assessment in human supervisory control,” Ph.D. dissertation, Technical University of Denmark, 2000. [1.1](#), [1.3](#), [2.1.2](#), [2.1.4.2](#), [2.3.2](#), [2.3.3](#), [3](#), [4.2](#), [2](#)
- [3] J. Rasmussen, *Information Processing and Human-machine Interaction: An Approach to Cognitive Engineering*. North-Holland, 1986. [1.1](#), [2.2](#), [2.2.1](#)
- [4] D. Woods and E. Roth, *Cognitive Systems Engineering*, M. Helander, Ed. B. V. North-Holland: Elsevier Science Publishers, 1988. [1.1](#)
- [5] K. Vicente, *Cognitive Work Analysis: Toward Safe, Productive, and Healthy Computer-Based Work*. Lawrence Erlbaum Associates, Publishers, Mahwah, 1999. [1.1](#)
- [6] M. Endsley, “Toward a theory of situation awareness in dynamic-systems,” *Human Factors*, vol. 37, no. 1, pp. 32–64, 1995. [1.2.1](#), [1.2.1](#), [4.1.3](#)
- [7] J. Rasmussen and M. Lind, “A model of human decision making in complex systems and its use for design of system control strategies,” in *Proceedings of American Control Conference*. IEEE, 1982, pp. 270–276. [1.2](#), [1.2.1](#), [1](#)
- [8] J. Dewey, “Logic: The theory of inquiry (1938),” *The later works*, vol. 1953, pp. 1–549, 1925. [1.2.1](#), [4.1.1](#)



- [9] T. Burk, *Dewey's new logic: A reply to Russell*. The University of Chicago Press, 1994. 1.2.1, 4.1.1
- [10] M. Lind, *Foundations of Functional Modeling*. unknown, 2015. 1.2.1, 4.1.1, 4.1.2
- [11] A. A. Nofi, "Defining and measuring shared situational awareness," DTIC Document, Tech. Rep., 2000. 2, 2.1
- [12] M. R. Endsley *et al.*, "Theoretical underpinnings of situation awareness: A critical review," *Situation Awareness Analysis and Measurement*, pp. 3–32, 2000. 2
- [13] E. L. Wiener, B. G. Kanki, and R. L. Helmreich, *Crew Resource Management*. Academic Press, 2010. 2.1.1
- [14] D. J. C. Whitfield and E. W. Hagen, "Human factors in the uk nuclear industry," pp. 70–75, 1992. 2.1.1
- [15] S. J. Lee and P. H. Seong, "Design of an integrated operator support system for advanced npp mcrs: Issues and perspectives," in *Progress of Nuclear Safety for Symbiosis and Sustainability*. Springer, 2014, pp. 11–26. 2.1.1, 2.1.3
- [16] J. T. Reason and J. T. Reason, *Managing the risks of organizational accidents*. Ashgate Aldershot, 1997, vol. 6. 2.1.1
- [17] J. Rasmussen, A. M. Pejtersen, and L. P. Goodstein, *Cognitive Systems Engineering*, ser. Wiley Series in Systems Engineering. Wiley, 1994. 2.1.2, 2.1.4.2
- [18] D. Woods and E. M. Roth, "Cognitive systems engineering," in *Handbook of Human-Computer Interaction*, M. Helander, Ed. Elsevier, 1988, pp. 3 – 43. 2.1.2
- [19] W. C. Elm, J. W. Gualtieri, B. P. McKenna, J. S. Tittle, J. E. Pepper, S. S. Szymczak, and J. B. Grossman, "Integrating cognitive systems engineering throughout the systems engineering process," *Journal of Cognitive Engineering and Decision Making*, vol. 2, no. 3, pp. 249–273, 2008. 2.1.2
- [20] J. Rasmussen, "Skills, rules, and knowledge - signals, signs, and symbols, and other distinctions in human-performance models," *IEEE Transactions on Systems Man and Cybernetics*, vol. 13, no. 3, pp. 257–266, 1983. 2.1.2, 2.1.4.1, 2.1.4.2
- [21] L. Bainbridge, "The change in concepts needed to account for human behavior in complex dynamic tasks," *IEEE Transactions on Systems, Man, and Cybernetics Part A: systems and Humans, Ieee Trans Syst Man Cybern Pt a Syst Humans*, vol. 27, no. 3, pp. 351–359, 1997. 2.1.2

- [22] I. S. Kim, "Computerized systems for on-line management of failures: a state-of-the-art discussion of alarm systems and diagnostic systems applied in the nuclear industry," *Reliability Engineering & System Safety*, vol. 44, no. 3, pp. 279–295, 1994. [2.1.3](#), [3.1.1](#)
- [23] J. H. Kim and P. H. Seong, "Methodology for the quantitative evaluation of npp fault diagnostic systems' dynamic aspects," *Annals of Nuclear Energy, Ann Nucl Energy*, vol. 27, no. 16, pp. 1459–1481, 2000. [2.1.3](#)
- [24] D. Ruan, "Intelligent information systems and applications," *Inf. Sci.*, vol. 142, no. 1-4, pp. 1–6, 2002. [2.1.3](#)
- [25] S. Koide, H. Nishio, Y. Kitamura, A. Gofuku, and R. Mizoguchi, "Operation-support system for large-scale system using information technology." in *ICEIS (4)*, 2003, pp. 430–437. [2.1.3](#)
- [26] J. H. Kim and P. H. Seong, "The effect of information types on diagnostic strategies in the information aid," *Reliability Engineering & System Safety*, vol. 92, no. 2, pp. 171–186, 2007. [2.1.3](#)
- [27] D. B. K. Mica R Endsley, "Level of automation effects on performance, situation awareness and workload in a dynamic control task," *Ergonomics*, vol. 42, no. 3, pp. 462–492, 1999. [2.1.4](#), [2.1.4](#)
- [28] L. Bainbridge, "Ironies of automation," *Analysis, Design and Evaluation of Man-Machine Systems, Proceedings of the IFAC/IFIP/IFORS/IEA Conference*, pp. 129–135, 1983. [2.1.4](#)
- [29] M. R. Endsley, "Situation awareness misconceptions and misunderstandings," *Journal of Cognitive Engineering and Decision Making*, vol. 9, no. 1, pp. 204–32, 2015. [2.1.4](#)
- [30] M. R. Endsley, R. Hansman, and T. C. Farley, "Shared situation awareness in the flight deck-atc system," *AIAA/IEEE Digital Avionics Systems Conference - Proceedings*, vol. 1, pp. E35–1–E35–8, 1998. [2.1.4](#)
- [31] T. B. Sheridan, W. L. Verplank, and T. L. Brooks, "Human/computer control of undersea teleoperators," 1978. [2.1.4](#)
- [32] J. Harrauld and T. Jefferson, "Shared situational awareness in emergency management mitigation and response," *Proceedings of the Annual Hawaii International Conference on System Sciences*, p. 23, 2007. [2.1.4](#)
- [33] K. J. Vicente and J. Rasmussen, "Ecological interface design: theoretical foundations," *IEEE Transactions on Systems, Man and Cybernetics*, vol. 22, no. 4, pp. 589–606, 1992. [2.1.4.1](#)

- [34] J. Rasmussen, "The role of hierarchical knowledge representation in decisionmaking and system management," *Systems, Man and Cybernetics, IEEE Transactions on*, no. 2, pp. 234–243, 1985. [2.1.4.1](#)
- [35] J. L. Paulsen, "Design of process displays based on risk analysis techniques," Ph.D. dissertation, Technical University of Denmark, 2005. [2.1.4.1](#)
- [36] M. R. Endsley, *Designing for Situation Awareness: An Approach to User-centered Design*. CRC Press, 2011. [2.1.4.2](#)
- [37] K. J. Vicente, K. Christoffersen, and A. Pereklita, "Supporting operator problem solving through ecological interface design," *Systems, Man and Cybernetics, IEEE Transactions on*, vol. 25, no. 4, pp. 529–545, 1995. [2.1.4.2](#)
- [38] M. Lind, "Making sense of the abstraction hierarchy," in *Proc. Proceedings of the seventh European Conference on Cognitive Science Approaches to Process Control*, 1999, pp. 195–200. [2.1.4.2](#), [2.2.1](#), [2.2.2.3](#)
- [39] J. Lu, X. Yang, and G. Zhang, "Support vector machine-based multi-source multi-attribute information integration for situation assessment," *Expert Systems with Applications*, vol. 34, no. 2, pp. 1333–1340, 2008. [2.1.4.3](#)
- [40] N. G. Brannon, J. E. Seiffertt, T. J. Draelos, and D. C. W. Il, "Coordinated machine learning and decision support for situation awareness," *NEURAL NETWORKS*, vol. 22, no. 3, pp. 316–325, 2009. [2.1.4.3](#)
- [41] M. Naderpour, J. Lu, and G. Zhang, "An intelligent situation awareness support system for safety-critical environments," *Decision Support Systems*, vol. 59, no. 1, pp. 325–340, 2014. [2.1.4.3](#)
- [42] A. X. Miao, G. L. Zacharias, and S.-P. Kao, "A computational situation assessment model for nuclear power plant operations," *Systems, Man and Cybernetics, Part A: Systems and Humans, IEEE Transactions on*, vol. 27, no. 6, pp. 728–742, 1997. [2.1.4.3](#)
- [43] M. Kim and P. Seong, "An analytic model for situation assessment of nuclear power plant operators based on bayesian inference," *Reliability Engineering & System Safety*, vol. 91, no. 3, pp. 270–282, 2006. [2.1.4.3](#)
- [44] M. Naderpour and J. Lu, *Supporting Situation Awareness Using Neural Network and Expert System*, 2012. [2.1.4.3](#)
- [45] M. Lind and X. Zhang, "Functional modelling for fault diagnosis and its application for npp," *Nuclear Engineering and Technology*, vol. 46, no. 6, 2014. [2.2](#)
- [46] M. Lind, "Functional modeling of complex systems," *Risk Management in Life Critical Systems*, pp. 95–114, 2014. [2.2](#), [2.2.1.1](#), [2.2.1.2](#), [2.2](#), [3.1.4](#)

- [47] L. Chittaro and R. Ranon, "Diagnosis of multiple faults with flow-based functional models: the functional diagnosis with efforts and flows approach," *Reliability Engineering & System Safety*, vol. 64, no. 2, pp. 137–150, 1999. [2.2](#)
- [48] J. R. Searle, *The construction of social reality*. Simon and Schuster, 1995. [2.2.1.1](#)
- [49] M. Lind and X. Zhang, "Functional modeling for fault diagnosis and its application for npp," *Nuclear Engineering and Technology*, vol. 46, no. 6, pp. 753–772, 2014. [2.2.1.2](#)
- [50] M. Modarres, M. Kaminskiy, and V. Krivtsov, *Reliability engineering and risk analysis: a practical guide*. CRC press, 2011. [2.2.2.1](#)
- [51] F. Brissaud, A. Barros, C. Berenguer, and D. Charpentier, "Reliability analysis for new technology-based transmitters," *Reliability Engineering & System Safety*, vol. 96, no. 2, pp. 299–313, 2011. [2.2.2.1](#)
- [52] Y. Hu and M. Modarres, "Evaluating system behavior through dynamic master logic diagram (dmld) modeling," *Reliability Engineering & System Safety*, vol. 64, no. 2, pp. 241–269, 1999. [2.2.2.1](#)
- [53] E. Ferrario and E. Zio, "Goal tree success tree-dynamic master logic diagram and monte carlo simulation for the safety and resilience assessment of a multistate system of systems," *Engineering Structures*, vol. 59, pp. 411–433, 2014. [2.2.2.1](#)
- [54] H. Goode and R. Machol, *System engineering: an introduction to the design of large-scale systems*. McGraw Hill, 1957. [2.2.2.2](#)
- [55] M. Lind, "An introduction to multilevel flow modeling," *Nuclear Safety and Simulation*, vol. 2, no. 1, pp. 22–32, 2011. [2.2.2.3](#), [2.3](#), [2.3.1.5](#), [3](#)
- [56] M. Lind, T. U. of Denmark. Institute of Automatic Control Systems., and DTH., "Representing goals and functions of complex systems : An introduction to multilevel flow modelling," Technical University of Denmark, Tech. Rep., 1990. [2.2.2.3](#)
- [57] J. Marcos, "Integral management of abnormal situations in complex process plants," Ph.D. dissertation, Technical University of Madrid, 2014. [2.2.2.4](#), [3.3](#)
- [58] J. L. De la Mata and M. Rodriguez, "Abnormal situation diagnosis using d-higraphs," in *Proc. of the 20th European Symposium on Computer Aided Process Engineering (ESCAPE 20)*, 2010, pp. 1477–1482. [2.2.2.4](#)

- [59] M. Lind, "Control functions in multilevel flow modeling," *Nuclear Safety and Simulation*, vol. 2, no. 2, pp. 132–140, 2011. [2.2.2.4](#), [2.3.1.6](#), [3](#), [4.5](#)
- [60] M. Lind, H. Yoshikawa, S. B. Jørgensen, M. Yang, K. Tamayama, and K. Okusa, "Multilevel flow modeling of monju nuclear power plant," *Nuclear Safety and Simulation*, vol. 2, no. 3, pp. 274–284, 2011. [2.3](#)
- [61] S. B. Jørgensen and M. Lind, "Modeling operating modes during plant life cycle," *Proceedings of the 17th Nordic Process Control Workshop*, p. 60, 2012. [2.3](#)
- [62] J. Wu, L. Zhang, M. Lind, W. Liang, J. Hu, S. B. Jørgensen, G. Sin, and Z. U. Khokhar, "Hazard identification of the offshore three-phase separation process based on multilevel flow modeling and hazop," *Lecture Notes in Computer Science, Lect. Notes Comput. Sci*, vol. 7906, pp. 421–430, 2013. [2.3](#)
- [63] M. Lind, "A goal-function approach to analysis of control situations," *Proceedings of 11th IFAC/IFIP/IFORS/IEA Symposium on Analysis, Design and Evaluation of Human-machine Systems*, 2010. [2.3](#)
- [64] —, "Modeling goals and functions of control and safety systems in mfm," *Proceedings International Workshop on Functional Modeling of Engineering Systems*, pp. 1–7, 2005. [2.3.1.6](#)
- [65] —, "Knowledge representation for integrated plant operation and maintenance," *7th American Nuclear Society International Topical Meeting on Nuclear Plant Instrumentation, Control and Human-machine Interface Technologies*, 2010. [2.3.1.7](#)
- [66] J. Wu, L. Zhang, S. B. Jørgensen, G. Sin, Z. U. Khokhar, and M. Lind, "Hazard identification by extended multilevel flow modelling with function roles," *International Journal of Process Systems Engineering*, vol. 2, no. 3, pp. 203–220, 2014. [2.3.1.7](#)
- [67] M. Lind, "Reasoning about causes and consequences in multilevel flow models," *Advances in Safety, Reliability and Risk Management - Proceedings of the European Safety and Reliability Conference, Esrel 2011*, pp. 2359–2367, 2012. [2.3.2](#), [4.2](#), [4.3.1](#)
- [68] H. P.-J. Thunem, A. P.-J. Thunem, and M. Lind, "Using an agent-oriented framework for supervision, diagnosis and prognosis applications in advanced automation environments," *Proceedings of Esrel 2011*, 2011. [2.3.3](#)
- [69] H. Thunem and X. Zhang, "Advanced control and automation support "c the continued development of the mfm suite," 2014. [2.3.3](#)

- [70] H. Thunem, “The development of the mfm editor and its applicability for supervision, diagnosis and prognosis,” *Safety, Reliability and Risk Analysis: Beyond the Horizon*, pp. 1807–1814, 2014. 2.3.3, 4.3.4
- [71] J. Wu, L. Zhang, J. Hu, M. Lind, X. Zhang, S. B. Jorgensen, G. Sin, and N. Jensen, “An integrated qualitative and quantitative modeling framework for computer-assisted hazop studies,” *AIChE Journal*, vol. 60, no. 12, pp. 4150–4173, 2014. 3
- [72] K. Heussen and M. Lind, “On support functions for the development of mfm models,” *Proceedings of the First International Symposium on Socially and Technically Symbiotic System*, 2012. 3, 4.5
- [73] W. C. Wimsatt, “Teleology and the logical structure of function statements,” *Studies in the History and Philosophy of Science*, vol. 3, pp. 1 – 80, 1972 1972. 4.2.1
- [74] M. Lind, H. Yoshikawa, S. B. Jørgensen, M. Yang, K. Tamayama, and K. Okusa, “Modeling operating modes for the monju nuclear power plant,” *Proceedings of the 8th International Topical Meeting on Nuclear Plant Instrumentation, Control and Human Machine Interface Technologies*, 2012. 4.4.1, 4.4.2, 4.6
- [75] X. Zhang, M. Lind, S. B. Jørgensen, N. Jensen, and O. Ravn, “Representing operational knowledge of pwr plant by using multilevel flow modelling,” *Proceedings of ISOFIC/ISSNP 2014*, 2014. 4.5







**[www.elektro.dtu.dk](http://www.elektro.dtu.dk)**

**Technical University of Denmark  
Department of Electrical Engineering  
Automation and Control (AUT)  
Elektrovej, Building 326  
DK-2800 Kgs. Lyngby  
Denmark**

**Tel: (+45) 45 25 35 76  
E-mail: [info@elektro.dtu.dk](mailto:info@elektro.dtu.dk)**