Modeling Goals and Functions of Control and Safety Systems - theoretical foundations and extensions of MFM

Lind, Morten

Publication date:
2005

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

nks

Nordisk kernesikkerhedsforskning
Norrænar kjarnöryggisrannsóknir
Pohjoismainen ydinturvallisuustutkimus
Nordisk kjernesikkerhetsforskning
Nordisk kärnsäkerhetsforskning
Nordic nuclear safety research

NKS-114
ISBN 87-7893-175-4

Modeling Goals and Functions of Control and Safety Systems -theoretical foundations and extensions of MFM

Morten Lind
Technical University of Denmark

October 2005

Abstract

Multilevel Flow Modeling (MFM) has proven to be an effective modeling tool for reasoning about plant failure and control strategies and is currently exploited for operator support in diagnosis [3, 4] and on-line alarm analysis [6].
Previous MFM research was focussed on representing goals and functions of process plants which generate, transform and distribute mass and energy [10, 11]. However, only a limited consideration has been given to the problems of modeling the control systems. Control functions are indispensable for operating any industrial plant. But modeling of control system functions has proven to be a more challenging problem than modeling functions of energy and mass processes. The problems were discussed by Lind [8, 9, 10] and tentative solutions has been proposed but have not been investigated in depth until recently, partly due to the lack of an appropriate theoretical foundation.
The purposes of the present report are to show that such a theoretical foundation for modeling goals and functions of control systems can be built from concepts and theories of action developed by Von Wright [23] and to show how the theoretical foundation can be used to extend MFM with concepts for modeling control systems. The theoretical foundations has been presented in detail elsewhere by the present author [12, 14] without the particular focus on modeling control actions and MFM adopted here.

Key words

Multilevel Flow Modeling, control actions, safety systems, theoretical foundation.

NKS-114
ISBN 87-7893-175-4

Electronic report, October 2005

The report can be obtained from
NKS Secretariat
NKS-775
P.O. Box 49
DK - 4000 Roskilde, Denmark

Phone +45 4677 4045
Fax +45 4677 4046
www.nks.org
e-mail nks@nks.org

Modeling Goals and Functions of Control and Safety Systems

-theoretical foundations and extensions of MFM

NKS-R-07: Barriers, Control and Management

Morten Lind
Ørsted•DTU, Automation
Technical University of Denmark
mli@oersted.dtu.dk

October, 2005

Contents

List of Figures

List of Tables

Chapter 1

Introduction

Multilevel Flow Modeling (MFM) has proven to be an effective modeling tool for reasoning about plant failure and control strategies and is currently exploited for operator support in diagnosis [3, 4] and on-line alarm analysis [6].

Previous MFM research was focussed on representing goals and functions of process plants which generate, transform and distribute mass and energy [10, 11]. However, only a limited consideration has been given to the problems of modeling the control systems. Control functions are indispensable for operating any industrial plant. But modeling of control system functions has proven to be a more challenging problem than modeling functions of energy and mass processes. The problems were discussed by Lind [8, 9, 10] and tentative solutions has been proposed but have not been investigated in depth until recently, partly due to the lack of an appropriate theoretical foundation.

The purposes of the present report are to show that such a theoretical foundation for modeling goals and functions of control systems can be built from concepts and theories of action developed by Von Wright [23] and to show how the theoretical foundation can be used to extend MFM with concepts for modeling control systems. The theoretical foundations has been presented in detail elsewhere by the present author [12, 14] without the particular focus on modeling control actions and MFM adopted here.

1.1 Why are models of control purposes required?

The overall purpose of control systems in process plants is to manage material and energy balances to optimize production and to ensure safe operation. Requirements to the goals and functions of control systems originate in the plant design process and comprises the basis for engineering control systems solutions. Information about control goals and functions is also necessary for operators dealing with diagnosis and counteraction of disturbances in complex plants because control systems modify the behavior of the plant under control. Without knowing the purposes of the control systems the operator would therefore have difficulties in both isolating

the causes of plant malfunction and to understand how the control systems affect the result of manual interventions. However, information about control purposes is only represented incompletely in the plant specifications and in the human machine interface. The information cannot be derived directly from programming code, from process and instrumentation (P&I) diagrams or from display mimics. Programming code describe how the control problem is solved in software and not the purposes of the control system. P&I diagrams and mimics represent physical connections between plant components and control and instrumentation equipment and contains only limited amount of information about purposes.

1.1.1 Control systems engineering

Control systems designers may claim that they can read information about control purposes from process schemes and P&I diagrams. However, this information is not explicit in the diagrams but is inferred by the expert based on his knowledge about the design problem. It is therefore difficult to validate the information about control purposes and to communicate the information to other designers and to the plant operator.

The need for information about control purposes in systems design is often accommodated by informal descriptions and other means of communication but methods for formalized representation are required. Without formalized representations it is not possible to ensure consistency of control systems design specifications. The lack of explicit representation or documentation of control purposes is also a problem when retrofitting old control systems with new technological solutions. New information technology will often facilitate the implementation of more intelligent solutions to a control problem. But if the only documentation available is the code or informal functional specifications the intentions of the control systems designer are hidden. It can therefore be very difficult to infer what the designer had in mind and to take advantage of the possibilities offered by the new information technology.

The overall relations between plant operational requirements and the purposes of control systems were discussed by Lind [7]. The work presented here provides improved modeling tools to express these relations. The notion of generic control tasks introduced in op.cit. is also extended with a theoretical foundation.

1.1.2 Human supervisory control

The lack of explicit representation of control system purposes in display mimics is a particular problem for operators trying to understand the behavior of an automatic control system. Explicit representations are here required in order to construct human machine interfaces that can support the operators in reasoning about control problems and to design databases for intelligent decision support systems.

Explicit information about control system goals and functions is necessary for the operator both in situations that require manual intervention and in supervising

the operation of the automated control functions. If only the means of control are known (i.e. the control algorithm and the physical structure of the automated controls) it may be difficult for the operator to find alternative solutions to a control problem. The plant condition or the causal structure may have changed during a disturbance so that the control algorithm or strategy does not longer apply in the situation and other courses of action are required. Information about the ends and the means of control and their status should therefore ideally be available to the operator at the interface.

The abstraction hierarchy

Rasmussen's abstraction hierarchy [20] is proposed by the cognitive systems engineering community as a conceptual framework for representing means and ends of control in HMI design. However problems in using the abstraction hierarchy (AH) for this purpose have been reported by several researchers (see e.g.[16]). Especially work domains with embedded controls has proven to be difficult to represent in the AH. The problem was analyzed by Lind [13, 15] and was shown to reside in the lack of distinctions in the AH between process and control hierarchies and in a lack of understanding of their complex interrelations.

It should be emphasized that the research presented here is not a solution to the AH problem which is rooted in foundational problems of the AH itself. We will show that means-end modeling of embedded control can be done using MFM when extended with the concepts presented here. We will also show that MFM can account for the complex relations between process and control hierarchies.

1.1.3 Intelligent automation

An intelligent automation system should also be able to deliberate about the means and ends of control. An automation systems designer chose the control solution from a set of possible alternatives which have different merits depending on the circumstances. In situations where the control system fails, the intelligent automation system should in a similar way reason about the control problem and possibly reconsider the design problem including an evaluation of the current state of control and a choice between possible alternative solutions. In order to do that the intelligent automation system should have knowledge about the intention and the different means available for control.

1.1.4 Safety systems engineering

Modeling of goals and functions of safety systems is a problem which is of particular interest for industry managing risky productions like e.g. energy or petrochemical plants. The problem is here to model systems whose purpose is to prevent a situation which is undesirable either in itself or because it has possible adverse consequences. We often refer to these safety systems as means of prevention or

counteraction and intuitively it seems therefore obvious that means-end concepts would be applicable for analysis and design of these kinds of system. Several approaches have been developed to model the goals and functions of safety systems [5, 2, 21, 22]. But in spite of the value of these approaches for the practice of safety engineering they suffer from being informal and by the lack of firm theoretical foundations.

The aim of MFM research has been to develop a formalized approach to the modeling of goals and functions of complex industrial plants. But, it has not until recently been entirely clear how goals and functions of control systems should be represented in MFM. Since many control systems have safety functions it has therefore not been possible to make formal representations in MFM of advanced principles for safety management in complex systems such as safety chains and defense in depth.

Chapter 2

The Challenges

The modeling of goals and functions of control systems is a challenging problem for three reasons. The first reason is that the process functions for mass and energy generation, transformation and distribution in an industrial plant are entangled with the functions of the controls. The second problem is that a control system often has multiple purposes and that the purposes often are indirectly related with the real purposes. The third problem is that it is not obvious what levels of abstraction that would be appropriate for defining the goals and functions of the control system. We will treat the three problems in more detail in the following.

2.1 Entangled functions

The entanglement of process and control functions means that it is not possible to separate entirely the modeling of process goals and functions from modeling the goals and functions of the control systems. The interdependency is deep and subtle because the behavior of a control system is directed towards fulfilling objectives that are defined in terms of the states and operating objectives of the process (the object) under control. Conversely, the process should be defined as an object of control i.e. having inputs and outputs and as being dynamically constrained by the controls. This is necessary because the efficiency and safety levels required of plants today cannot be achieved without the use of control systems. Goals and functions of the plant process and the controls should therefore be described within the context of the other as illustrated in figure 2.1.

A control system is subordinate to the plant it is controlling because its actions are directed towards ends defined by plant operational requirements. It is therefore a means of achieving or maintaining plant goals and functions and not an end in itself. The problem of modeling control goals and functions cannot therefore be formulated without considering plant operating objectives and information about intentions of the process designer. Ideally, control goals and operating objectives should be in a one-to-one correspondence. For example, if the operating objective or goal of a plant is to maintain a constant specified product composition, the

control-system objective could be to maintain, say the flow-rate ratio between two materials entering the process.

The logical correspondence between goals for plant operation and control goals was identified by the author in [9]. Here we will extend the analysis to also include the relationship between plant and control functions as they presently can be expressed within the framework of MFM.

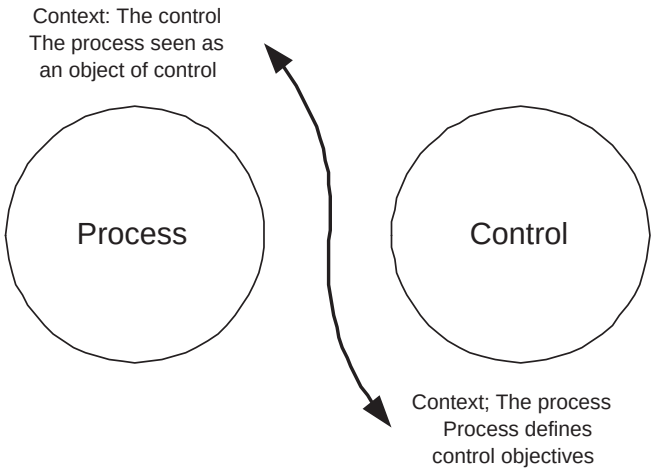


Figure 2.1: Process and control systems as the context of the other

Actually all functional descriptions in MFM are bound to a context of goals and purposes in this way. For example, the function of a pump in a plant cannot be described without considering the pump as embedded in a context of use or purpose. In turn, the pump define the context for the description of the other parts and subsystems of as sources and sinks of the fluid pumped. However, a control system is embedded functionally at a deeper level than e.g. a pump because its behavior is goal directed based on internal representations of the previous states and goal states of itself and its environments (the process). A pump does not possess internal representations of its own state and the environment (provided of course that it is not an intelligent pump equipped with an embedded control system).

The functional embedding is reciprocal so that ascriptions of goals and functions to a subsystem will influence the goals and functions ascribed to other subsystems and vice versa. The syntax which rules the combination of elementary flow functions in flow structures is an expression of this inherent reciprocity [8]. We shall see in the following that other functional patterns or regularities emerge in MFM models when control systems are introduced because they, due to their representational capacities, can determine the causal direction of how changes of functional states propagate through the plant.

2.2 Multiple and indirect purposes

Another difficulty is that control systems in some cases produce or maintain a state or condition S_1 in the process under control in order to prevent another harmful condition S_2 to remain or happen. The control purpose can in such cases appear to be ambiguous or difficult to define. This problem typically appear in situations where a control system in addition to its main purpose also is the solution to a safety problem. Often it cannot be deduced from the implementation of the system that the purpose is to prevent condition S_2. Information about the harmful condition cannot be derived from the implementation because it relates to a hypothetical situation which is not supposed to arise. The fact that the hypothetical situation is prevented is in the mind of the designer who knows that a harmful condition could occur if the control system was not installed. This information is not expressed in the design specifications which only represents the solution and not the nature of the problem.

Such an approach to safety can be dangerous if plant conditions changes so that e.g. maintaining S_1 no longer ensure the prevention of the harmful condition S_2. Information about the control goals and functions would therefore be necessary for an intelligent agent who must reason about the ends and means of control in the counteraction of disturbances in a complex system. Especially when plant disturbances can violate design assumptions.

A similar problematic situation arises when the controlled plant variable is only indirectly related to the variable of interest for the controller. The reason may be that it is impossible or costly to measure the variable of interest and another causally related variable is used instead as an indicator. In such cases a change in the indicator variable should be both sufficient and necessary for a change to occur in the variable of interest.

2.3 Levels of abstraction

A third general difficulty is to choose levels of abstraction in the representation of control functions. Control systems can, as other systems, be described on various levels of means-end abstraction. Traditionally it is described as a signal or information processing system. But by such a representation the emphasis is on the means used for control and not on the purpose served in the process under control.

A particular problem is to distinguish the purposes of control systems based on the principles of feed back and feed forward. The names of both control principles refer to the direction of information flow concerning the influence of disturbances on the control action. In a control system based on feed forward the effect of directly observable disturbances are compensated a priori by a suitable counteraction derived from the observation. In the case of feed back a disturbance is compensated post hoc by evaluating its effect on the controlled plant variable and by intervening with an appropriate control action. Descriptions of the two control principles refer

to the flow of information in the control system but does not describe to what end or purpose these principles are used. Feed back and feed forward are accordingly terms that refer to the means of control.

We will show in the following that action theoretical concepts can be used to provide representations of control system purposes which do not involve information or signal processing concepts. Control purposes and information flows are accordingly descriptions of the control system on two separate (but related) levels of end-means abstraction. But, even though description of purposes and information flow are separated into different levels of abstraction each of these descriptions alone is insufficient to give a full account of all aspects of the functions of control systems. The two descriptions provide merely two different perspectives on the control system. We will show in the following that it is meaningful to distinguish the two types of descriptions and that the descriptions of control purposes support reasoning processes.

Another related difficulty (which will not be dealt with in detail here) is the problem of shifting between describing a system as a control system or as an object of control. The choice of perspective depends on the role the system have in relation to its environment in different situations (see e.g. [15] for an example).

Chapter 3

Action Theoretical Foundations

Recent research by Lind [12, 14] has established an action theoretical basis for modeling control and safety functions in MFM. We will first give a brief outline of the theory and use it to derive a logically complete set of elementary control actions. From these elementary control action we will then derive MFM modeling concepts for control. It will be assumed that the reader is familiar with "standard" MFM as described in Lind [10, 11]. The extension of MFM with causal roles proposed by Petersen [19] is also assumed known because the roles are necessary in order to represent control functions in MFM. A summary of standard MFM concepts and the extensions are shown in appendix A.

The action theory provides also a foundation for defining the flow functions (source, sink, storage, transport etc.). These applications of the theory are described by Lind [14] but will not be discussed here. The action theory is generic and therefore more basic than MFM but cannot substitute it. The action theory lacks a domain ontology to define world states and thereby the domain dependent features which makes MFM a powerful tool for modeling complex industrial systems.

The action theoretical framework is derived by the present author from the work of Von Wright [23] by several extensions. These extensions are presented in detail in Lind [12, 14]. Only results relevant for the topic of the present paper are presented below.

3.1 Von Wright's elementary action types

The purpose of VonWright's theory is to provide a logical definition of the concept of action. The theory is based on the concept of change being defined as a temporal succession of two states. Formally a change is defined by a schema $[\, pTq \,]$ where T is a temporal operator (then), p is a proposition which is true before the change and q is a proposition which is true after the change. An action implies a change of the state of affairs. But it is not only a change of state it has also a counterfactual aspect because the change would not occur unless the action was done. This means that

the logical definition of an action also must refer to the hypothetical (not actualized) state of the world that would exist if the action was not done. In this way an action can be defined by extending the change schema [pTq] to the schema [$pTqIr$] where I (instead) is an operator relating the actualized state q with the hypothetical state r.

Von Wright defined a very limited set of elementary action types from this preliminary conceptual analysis by only allowing the states to be described by a proposition p and its negation $\neg p$. With this restriction there are only eight possible types of actions as shown in table 3.1. In the table we distinguish between interventions and omissions. An omission can be understood as an intentional not-doing so that even if the agent had the capability and the opportunity to intervene he decided not to intervene in the world. In addition to the schema each elementary action type in table 3.1 has also a corresponding description. The action with the schema [$\neg pTpI\neg p$] has accordingly the description [$produce\ p$].

Interventions		**Omissions**	
Schema	**Description**	**Schema**	**Description**
[$\neg pTpI\neg p$]	[$produce\ p$]	[$\neg pTpIp$]	[$let\ p\ happen$]
[$pTpI\neg p$]	[$maintain\ p$]	[$pTpIp$]	[$let\ p\ remain$]
[$pT\neg pIp$]	[$destroy\ p$]	[$pT\neg pI\neg p$]	[$let\ p\ disappear$]
[$\neg pT\neg pIp$]	[$suppress\ p$]	[$\neg pT\neg pI\neg p$]	[$let\ p\ \ remain\ absent$]

Table 3.1: Von Wright's elementary action types [23]

3.1.1 Interpretations of the elementary action types

It may seem unnecessary to have as many as eight elementary action types since they can be reduced to four by simple logical substitutions. The possibility of a reduction can be demonstrated by considering the schema of one of the action types e.g. [$\neg pTpI\neg p$]. By substituting p with $\neg p$ in this schema we get the schema [$pT\neg pIp$] which is the action type described by [$destroy\ p$]. Note however, that the description [$produce\ \neg p$] obtained by substituting p with $\neg p$ in the description [$produce\ p$] is semantically distinct from the description [$destroy\ p$]. The reduction is therefore not desirable even it is possible on purely logical grounds. This can be explained by comparing the two descriptions [$produce\ \neg p$] and [$destroy\ p$]. They refer to the same physical action (defined by the schema) but have different meanings defined by the descriptions. The description [$produce\ \neg p$] refer to the action of an agent who wants to *promote* a new state $\neg p$ whereas [$destroy\ p$] refer to the action of an agent who is *opposed* to the situation defined by p (and therefore destroy it). The descriptions of an action can therefore be used to distinguish between intentions of agents which perform the same physical action (defined by the schema) but having different intentions (defined by the descriptions). This leads to the interpretations of the elementary action types shown in figure 3.1.

It should be noted that the verbs used in forming descriptions (i.e. produce, maintain, destroy and suppress) have ambiguous meanings if used in a natural language context. Here they are used in a strictly technical sense with only one meaning as defined by the corresponding action schema and by the references to the actual or the hypothetical (counterfactual) states made in the corresponding descriptions.

It is realized that the distinctions between promotive and opposive actions which are introduced above are highly relevant for the representation of safety related actions. Since the purpose of safety related actions is to prevent or suppress plant states which are undesirable they clearly belong to the category of opposive actions.

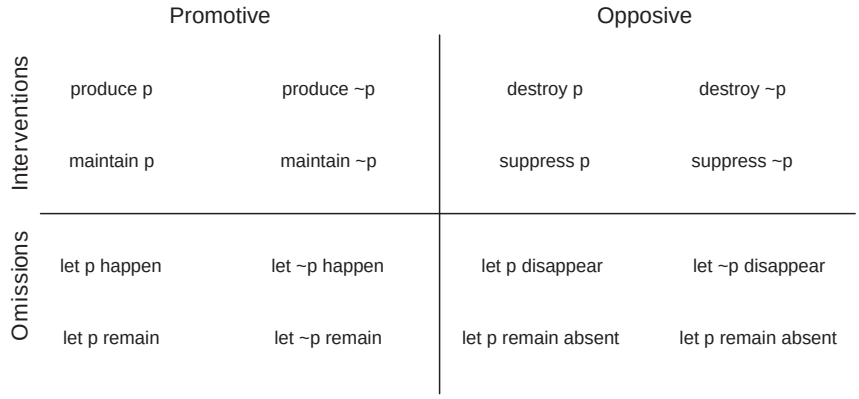


Figure 3.1: Interpretations of the elementary action types

3.1.2 Elementary control actions

The elementary interventions shown in table 3.1 corresponds directly to established control engineering concepts as shown below in table 3.2. Tripping and interlocking are safety related control actions whereas steering and regulation only are indirectly related to safety.

Intervention	**Control action**
$[\,\neg pTpI\neg p\,]$	steering
$[\,pTpI\neg p\,]$	regulation
$[\,pT\neg pIp\,]$	tripping
$[\,\neg pT\neg pIp\,]$	interlocking

Table 3.2: Corresponding elementary interventions and control actions.

The distinction between action schema and descriptions introduced above can also be applied to the control actions as shown in figure 3.2 so that we can distinguish between two purposes of the same control action. Note that the choice of

description of a control action (its purpose) depends on the context. A control action can therefore be given different descriptions if the modeling problem require that the action is interpreted in different contexts.

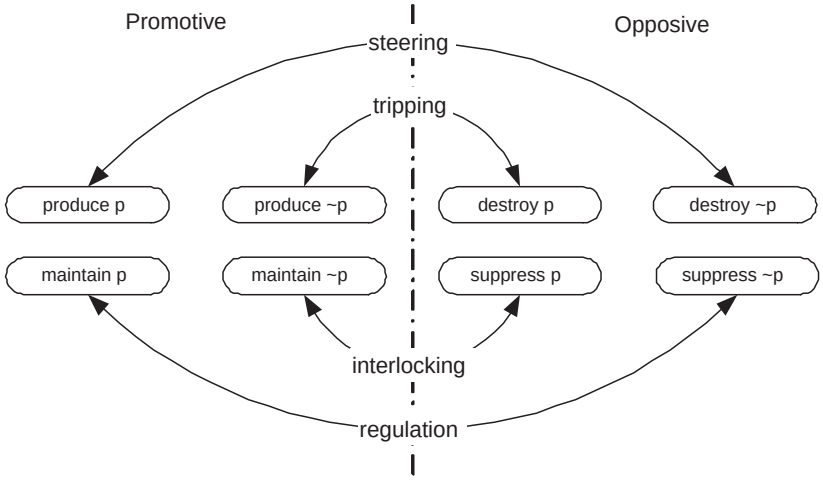


Figure 3.2: Interpretations of control actions

A description of a control action assume the existence of an agent. It represents information of the purpose or intention behind the agents action which is not accessible for direct observation. The information must be communicated or inferred from other information about the context of the action. The action schema, on the other hand, represents observable aspects of the action. We could say that the schema represents *what* the agent is doing whereas the description gives the reason *why* the agent perform the action (the intention or purpose). The description and the action schema therefore constitute representations of the action on two distinct semantic levels which imply two different frames of interpretation. It should be noted that the relation between the two levels is uniquely defined by the systematic principles of interpretation presented in Lind [12].[1]

3.1.3 Disturbances

We have used the elementary action types to define elementary control actions but this does not provide a full account of their semantics. That something is missing can be seen by realizing that the intervention types also can be used to categorize actions which we would not see as control actions. For example translocation of objects in space (move-to, keep-at, move-away-from and keep-away-from a location) can also be defined as instances of the elementary intervention types. But these actions cannot be considered as control actions unless the agent is able to determine the position of the object irrespective of other counteracting causal agents.

[1]This result can be obviously extended to other elementary actions as well

The effect of a counteracting agent is usually called a disturbance in control engineering. The very purpose of control is namely to determine the state of the system under control in spite of other counteracting factors.[2]

This aspect of determination (or causation) of a control action is expressed by the action schema which define the relations between the initial s_i , the actualized s_r and the hypothetical state of affairs s_h. But we need also to represent the corresponding counteragent who is defeated by the control agent. The question is now how to do this?

This question has a simple answer because the not actualized outcome of the counteragents actions for each of the control action types is defined by the hypothetical state of affairs s_h in the action schema in table 3.2. We can therefore construct a schema representing the (defeated) action of the counteragent for each of the cases as shown in table 3.3. It seen that the analysis comprises both control actions where the counteragent attempts to disturb the current state of affairs (regulation and interlocking) and control actions where the counteragent resists changes (steering and tripping). Note that the counteragent also can be seen as the internal source of the dynamics of the process under control. We have also introduced formal descriptions of the counteractions representing possible intentions of the counteracting agent.[3]

Control action	**Counteraction**	
Type	**Schema**	**Description**
steering	$[\,\neg pT\neg pIp\,]$	$[\,resist\ p\,]$
regulation	$[\,pT\neg pIp\,]$	$[\,attempt\ \neg p\,]$
tripping	$[\,pTpI\neg p\,]$	$[\,resist\ \neg p\,]$
interlocking	$[\,\neg pTpI\neg p\,]$	$[\,attempt\ p\,]$

Table 3.3: Corresponding control actions and (defeated) counteractions

The elementary action types are generic and the discussion of counteractions is accordingly also relevant for other types of action than control actions. However, note that an important difference between ordinary actions and control actions is that some control actions are goal determined. This means that goal changes will have a causal effect on the control action and that a deviation from the goal caused by the counteragent will be compensated by the control agent.

[2]Following Morris [17] value oriented semiotic analysis of actions control actions are associated with the value dimension of dominance. Control actions are thereby distinguished from acts of observation (value dimension of detachment) and acts of assimilation (value dimension of dependence)

[3]Other interpretations of the counteractions are possible in the same way as actions in general can be given different descriptions depending of the intention of the agent

3.2 An example

Let us take a simple example for illustration of the different interpretations of control actions. Assume that we have a controller regulating the level x in a tank at the reference value x_0 as depicted in figure 3.3. The action schema representing the function of the regulator would be $[\ (x = x_0)T(x = x_0)I\neg(x = x_0)\ ]$. According to the results above we can now define two possible purposes of the regulator.

The first possible purpose is defined by the description $[\ maintain\ (x = x_0)\ ]$. Here a constant level at x_0 is considered desirable and the control system is a means for promoting this situation. We can directly see by the conventions of the diagrammatic representation in figure 3.3 that the target value for the regulator action is x_0. The label "regulator" refers to the function of the loop which is "to regulate" the tank process. But the label is only attached to the box for explanatory purposes. The diagram does not provide an explicit representation of neither the purpose nor the function of the feedback loop. In an engineering calculation, the regulator box would refer to an algorithm for calculating the control signal from the error signal. In a means end analysis, the algorithm would not be considered a purpose or an end but a means of control and therefore define *how* the control is achieved.

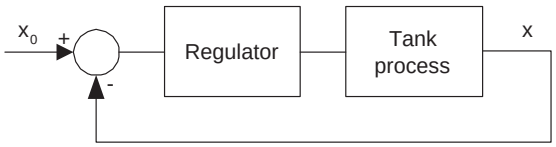


Figure 3.3: Using feedback to implement the purpose:$[\ maintain\ (x = x_0)\ ]$

The other possible purpose of the control system in figure 3.3 is defined by the description $[\ suppress\ \neg(x = x_0)\ ]$. Here the control system is a means to oppose situations where the level x is not at the reference value x_o (including situations where the level is greater or equal to the height of the tank). The control system may for example be described by the function it serves in safe operation of the tank process (avoiding undesirable states as e.g. spill over). Note that in this case the purpose cannot be represented using the symbology of the feedback loop in figure 3.3. There is here a clear distinction between the control purpose and function and the implementation (the feedback loop). The feedback loop represent *how* the control function is achieved.

Either or both of the descriptions can be used depending on the purpose of the tank process the plant designer had in mind. The descriptions chosen can also depend on the scope of the modeling problem and therefore also the types of functional descriptions that should be included (compare e.g. the distinctions between design, use and service functions introduced by Achinstein [1]). The designer provided the regulator in order to maintain the tank level at x_0 (the design function) without being concerned about a possible spill over which is an operational

problem. But the operator may use the regulator (switch it in auto) as a means of avoiding this in critical situation. This means that the regulator for the operator would have the purpose of preventing spill over.

3.3 Doing, bringing about and actuation

The proposition p in the action schema and descriptions designate the state of affairs which is of relevance for the agent. The choice of p is therefore essential step in the analysis of the semantics of an action. But often it is not clear how to chose an appropriate p. The problem can be illustrated by considering the act of opening the inlet valve to a water tank. In such a case we can choose between several possible propositions to characterize the action. The following possibilities p_1, p_2 and p_3 can be suggested:

- p_1: the valve is open
- p_2: the flow of water is increased
- p_3: the water level is increased

The three state of affairs defined by the propositions are obviously causally connected because an open valve would cause the flow of water to be increased which in turn would cause the water level to increase. The choice of proposition to characterize the action is a matter of defining what should be considered its result and its consequences. Von Wright make a related distinction between doing and bringing about. The doing refer to the direct outcome of the action, its result, whereas bringing about refer to a consequence of the action.

This distinction between doing and bringing about is important for the modeling of control actions because it is often is impossible directly to control (determine) a state of affairs which is of interest. Let us define this state by the proposition p_d. The control action would in such cases be directed at realizing a state of affairs p_a which is causally connected with the state defined by p_d. Using Von Wrights distinction we would then say that the purpose of the control action is to bring about p_d by doing p_a. The distinction between doing and bringing about is directly related to the distinction made in control theory between the controlling and the controlled variables (p_a refer to the controlling variable and p_d refer to the controlled variable). The controlling variable characterize the state of the equipment used to actuate the process under control (the actuator) and we need therefore also to be able to represent the function of actuation. As shown later this will be done in MFM by a new relation called an actuation relation.

Chapter 4

Control flow structure

Von Wright's Action theory and the extensions proposed by the present author provides accordingly a formal foundation for the definition of elementary control action types. In the following we will show how these results can be used to extend MFM with concepts for representation of control functions and their composition into control flow structures. As mentioned above, the action theoretical results are generic and apply to any domain of action. It is not the purpose of MFM to cover all domains but to provide an effective and expressive modeling tool for production plants. We need therefore to integrate the action theoretical results with existing MFM concepts i.e. to define concepts and corresponding symbols for representing control functions.[1] These symbols will be combined to form control flow structures.

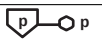
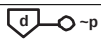
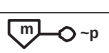
	Promotive		**Opposive**	
Type	**Symbol**	**Explanation**	**Symbol**	**Explanation**
Steering		The purpose is to produce p		The purpose is to destroy $\neg p$
Regulation		The purpose is to maintain p		The purpose is to suppress $\neg p$
Tripping		The purpose is to produce $\neg p$		The purpose is to destroy p
Interlocking		The purpose is to maintain $\neg p$		The purpose is to suppress p

Table 4.1: Elementary control functions in MFM (derived from figure 3.2)

The transition from the generic results to MFM concepts and symbols is actually quite straight forward as shown in table 4.1. The elements of the control function symbols are here derived directly from the two components of the action

[1] In order to represent more complex control actions we will also need the analysis of descriptions of composite actions presented in (Lind [14]) and to be able to combine elementary actions into sequences. Furthermore, situations comprising more than one control agent should be considered in order to model goals and functions of multivariable control systems. These topics are outside the scope of the present report.

descriptions; the verb and the proposition. The verb is represented symbolically by an "inverted house" with a label indicating the type. The proposition defining the focal state, is represented by a circle as are goals or objectives in standard MFM (see appendix A for an explanation of focal states). Note that the two elements of the description are related by a connection relation. Another possibility is to relate them with an arrow (similar to a causal role) as shown in figure 4.1 to indicate that the control action is determined by the focal state. With the connection relation the control action is oriented towards but not determined by the focal state. This distinction is important when reasoning about control.

Figure 4.1: Control determined by the focal state (goal).

Control functions are combined with the standard MFM concepts as shown in figure 4.2. The control function f_i is related to a flow function f_j in flow structure S_2 through an actuation relation r_2. The focal state node g_2 is connected with the flow structure S_2 by the relation r_3 which can be either a produce, maintain, destroy or suppress relation (see appendix A). The node g_2 defines a constraint $g_2(f_k)$ on the state of flow functions (f_k) in S_2 . The focal state node g_1 is connected with the control flow structure S_1 by the relation r_1 and similar to r_3 it can be a produce, maintain, destroy or suppress relation.

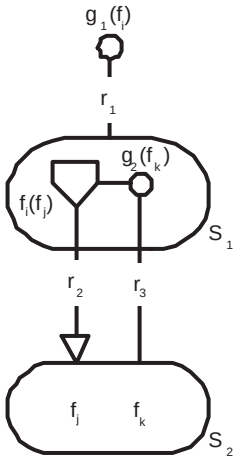


Figure 4.2: The control concept in MFM

Note the distinction between the process and the control goal (focal state). The process goal g_2 defines a desirable state of the *process* whereas the control goal g_1 defines a desirable state of *control*. The control goal therefore expresses the degree to which the process goal (focal state) should be accomplished and the

two goals are therefore closely related (see also Lind [10]). Figure 4.2 may give the false impression that goal g_2 is subordinate to g_1 due to their relative vertical position in the diagram. But this misinterpretation of the diagram is an artifact of its orientation which is arbitrary.

It should be stressed that the "loop" formed by relations r_2 and r_3 in figure 4.2 is composed of conceptual relations and is therefore not a representation of the function or structure of a feedback loop. The concept of feedback is connected with signal or information flow but the control functions shown here do not describe information flow but the intended effect or purpose of the control action on the process under control. As mentioned previously, the processing of information is a means of control and should therefore be represented on a lower level of means-end abstraction (see also Lind [9] and Petersen [18]). The control function represented in figure 4.2 could therefore be implemented by other means than feedback (e.g. feedforward, in which case the control would only be goal oriented and not goal determined). This means that even though the topology of feed-back and feed-forward control structures has no representation on the level of means-end abstraction intended here we can represent the purposes they serve in control of the process (goal orientation and determination).

Control functions and flow functions in the flow structures representing the process under control are interdependent. This means that the inclusion of control functions in a system will influence the description made of process functions. A full account of these interdependencies require further research and cannot therefore be given at the present stage. Examples of the interdependencies will be given later.

4.1 Elementary control patterns

The types of control function f_i and the means-end relations r_1 and r_3 in figure 4.2 cannot be chosen in an arbitrary fashion. Only some combinations of relations and functions makes sense. These combinations are generic and produce a limited set of functional structures in MFM models (eight in all) which we will call elementary control patterns. The patterns are called elementary in order to distinguish them from more complex patterns which can be constructed by composition (see later).

The possible combinations are shown in table 4.2. Table 4.3 show corresponding elementary control patterns for four of the eight possible combinations.

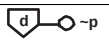
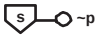
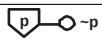
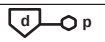
	Promotive			Opposive		
Type	**Symbol**	r_1	r_3	**Symbol**	r_1	r_3
Steering		Maintain	Produce		Maintain	Destroy
Regulation		Maintain	Maintain		Maintain	Suppress
Tripping		Maintain	Produce		Maintain	Destroy
Interlocking		Maintain	Maintain		Maintain	Suppress

Table 4.2: Possible combinations of control function f_i and relations r_1 and r_3

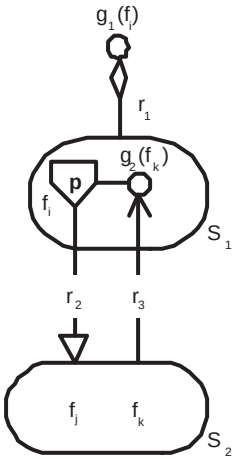
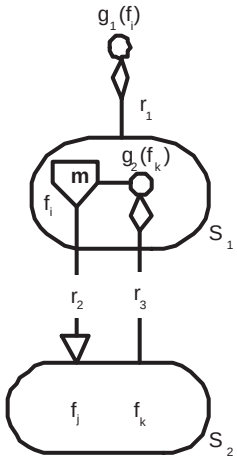
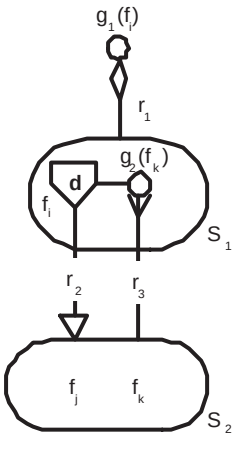
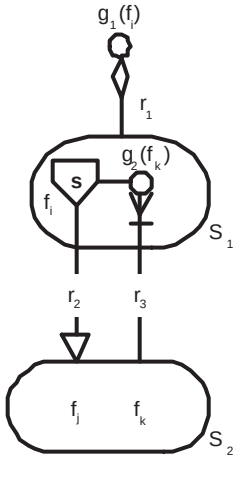
 Steering control (promotive)	 Regulation control (promotive)
 Tripping control (opposive)	 Interlocking control (opposive)

Table 4.3: Elementary control patterns derived from table 4.2

The reading of the patterns in table 4.3 should take into consideration that the models represent goals and purposes of the control systems and not how the control is done i.e. its behavior or structure.

The symbology used in the patterns express the different aspects of control actions. First of all the plant focal state g_2 is connected to the control function f_i in order to show that the control action is aimed at the plant purpose expressed by the combination of r_3 and g_2. This purpose is matched by the control type indicated by the label in the control function symbol f_i. In this way we describe that the control function is a means of obtaining the plant purpose on a par with the functions in the flow structure S_2.

Steering control. The plant purpose is here to "produce g_2". This purpose is matched by the control type p.

Regulation control. The plant purpose is here to "maintain g_2". This purpose is matched by the control type m.

Tripping control. The plant purpose is here to "destroy g_2". This purpose is matched by the control type d.

Interlocking control. The plant purpose is here to "suppress g_2". This purpose is matched by the control type s.

4.2 Complex control patterns

The elementary control patterns can be combined into more complex control patterns. One possibility is to create control chains and another possibility is to create control cascades.

4.2.1 Control chains

Control patterns can include several functional levels in MFM when the levels are related by a producer-product relation (see also [11]). These structures are called control chains. An example is shown in figure 4.3.

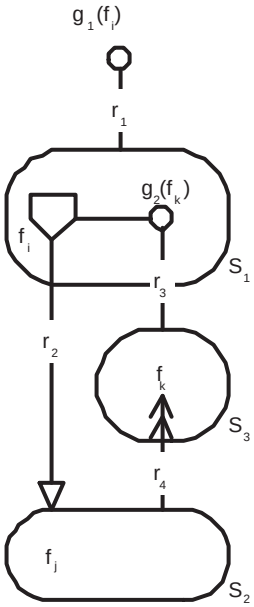


Figure 4.3: A control chain involve one or more functional levels connected by producer-product relations (r_4)

4.2.2 Control cascades

A control function f_l can command another control function f_i through an actuation relation to its focal state (see figure 4.4). In this case we will talk about control cascades because the flow structures created can be used to model goals and functions of cascade control systems.

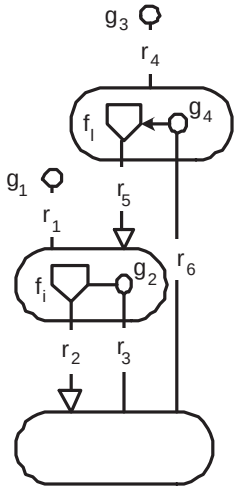


Figure 4.4: The functional structure of cascade control

The relations r_1, r_3, r_4 and r_5 cannot be chosen arbitrarily. Possible combinations are shown in table 4.4.

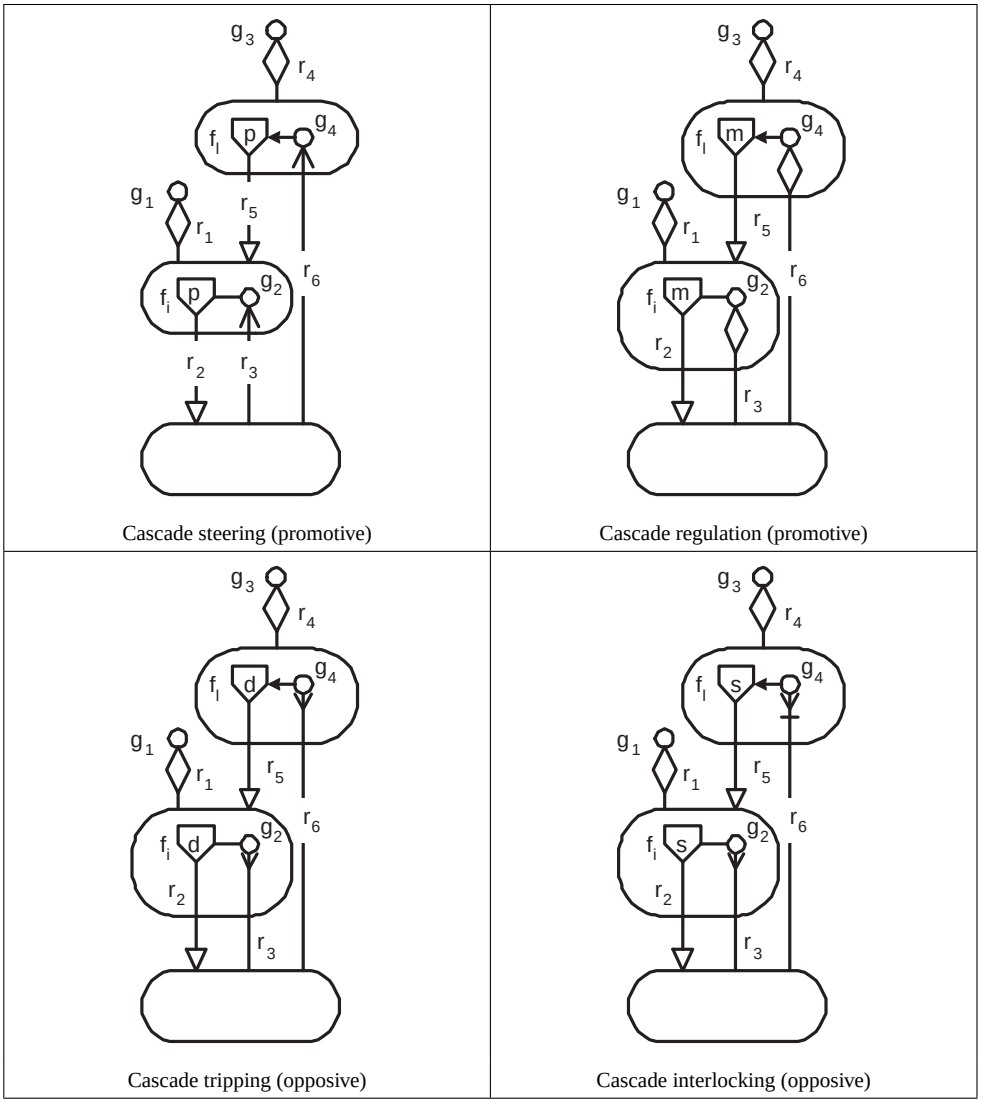


Table 4.4: Cascade control patterns

Cascade steering. The plant purpose is here to "produce g_2". This purpose is matched by the type p of control function f_i. The focal state g_2 of f_i is determined by a control function f_l also of type p. The focal state of f_l is g_4. This means that the aim of f_l is to produce g_4 which is done by commanding f_i to produce g_2.

Cascade regulation. The plant purpose is here to "maintain g_2". This purpose is matched by the type m of control function f_i. The focal state g_2 of f_i is determined by a control function f_l also of type m. The focal state of

f_l is g_4. This means that the aim of f_l is to maintain g_4 which is done by commanding f_i to maintain g_2.

Cascade tripping. The plant purpose is here to "destroy g_2". This purpose is matched by the type d of control function f_i. The focal state g_2 of f_i is determined by a control function f_l also of type d. The focal state of f_l is g_4. This means that the aim of f_l is to destroy g_4 which is done by commanding f_i to destroy g_2.

Cascade interlocking. The plant purpose is here to "suppress g_2". This purpose is matched by the type s of control function f_i. The focal state g_2 of f_i is determined by a control function f_l also of type s. The focal state of f_l is g_4. This means that the aim of f_l is to suppress g_4 which is done by commanding f_i to suppress g_2.

4.3 Reasoning about control

Plant goal failure related to control can be identified from the MFM model by searching through the proposed functional structures. The failure could accordingly be caused by a failed control function, failed actuation (through the relation r_2) or failed functions in the structure S_2.

Note that a failed plant goal also could be explained by a failed evaluation of the goal caused by sensor error. However, this type of error is only represented in control patterns by its effect on the focal state g_2 and it cannot therefore be traced back to its possible sources. In order to do that we need a model incorporating information flow. But as mentioned above we consider information flow structures to represent means of control and therefore leave it out in the control patterns which represent purposes or ends of control.

As mentioned previously we can represent the goal determination of a control action by a causal role. In this way we are able to propagate changes in the system. If the goal fails it will have an effect on the control action so that the goal state is restored.

Chapter 5

Composite flow structures

Flow structures in standard MFM includes only flow functions related to either mass and energy (and now also control). This is however not sufficient for modeling control systems. One of the purposes of control systems is to coordinate or integrate a set of flow functions. The controlled integrated process will then as a whole emerge as a flow function which thereby represent the integrated functions at a higher level of abstraction. We need therefore to be able to relate a set of flow structures comprising a combination of mass, energy and control flow structures with a flow function. This cannot be done in standard MFM as flow functions here only can be related to a focal state (goal) or a single flow structure.

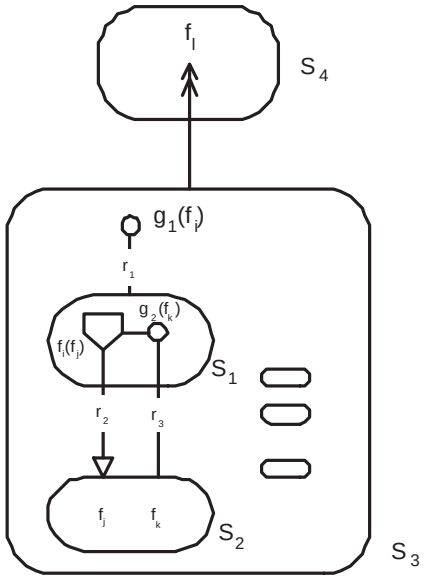


Figure 5.1: A composite flow structure (S_3) integrated into a flow function f_l.

We therefore introduce composite flow structures comprising one or more (possibly related) "elementary" standard flow structures. Composite flow structures

will have the same graphic representation as a standard "simple" flow structure which then is seen as a special case. Functional integration can then be modeled by relating a composite flow structure and a flow function with a producer-product relation as shown in figure 5.1. An example of using composite flow structures to model functional integration is shown later.

A composite flow structure can as an elementary flow structure also be connected to a flow function by a condition or neg-condition relation as shown in table 5.1. Here r_1 can be a produce, maintain destroy or suppress relation.

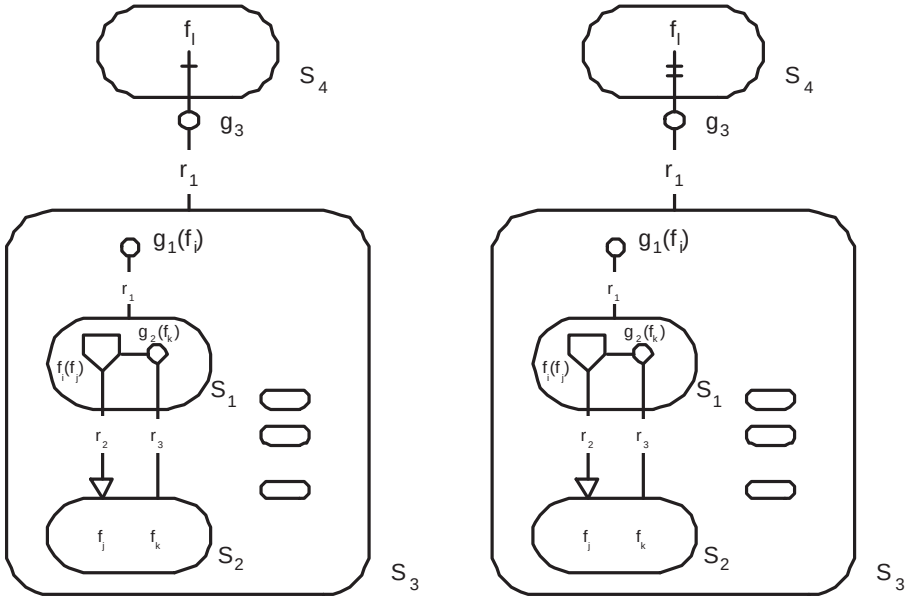


Table 5.1: A flow function f_l conditioned by a focal state g_3 related to a composite flow structure.

Chapter 6

Modeling examples

We will demonstrate how purposes and functions of the control systems can be expressed in MFM by a simple example, a tank process. First we will consider the system without any controls and then it will be extended with different control systems.

6.1 The tank process without control system

The system without control and the corresponding MFM model is shown in figure 6.1. Note that the MFM model includes three active and three passive causal roles. For example, So_1 is an upstream agent for Tr_1 and St_1 is an upstream agent for Tr_3. The barrier Ba_1 in the lower branch of the flow structure represents a safety function of the tank (to prevent the water from spilling over). Note also that the upstream agent role of So_1 in relation to Tr_1 is conditioned by the state of the stop valve (if the valve is closed the role is not available). The two actuation relations Ac_1 and Ac_2 indicate two possibilities of intervention (the actuation function of the valves V_c and V_o).

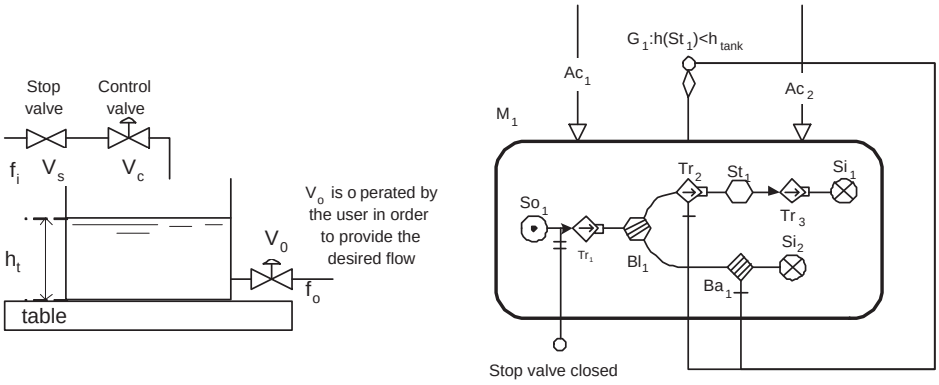


Figure 6.1: MFM model of tank without control system

6.2 Feedback control of input valve

Introducing a level regulator in the tank we get the MFM model shown in figure 6.2. The control function is represented by the concepts introduced above (maintain) and its relations with the flow functions below are indicated. Note in particular that St_1 has a downstream agent role in relation to Tr_2 because the feedback loop change the pattern of causal roles in the system. Actually, one of the purposes of the feedback loop is to modify the causal structure. This demonstrates the reciprocity of functional descriptions mentioned earlier. Note also that a barrier Ba_2 has been included in series with Ba_1. The barrier represents a safety function of the regulator (to prevent spill over) and the two barriers form together a simple safety chain comprising two levels of defense against spill over.

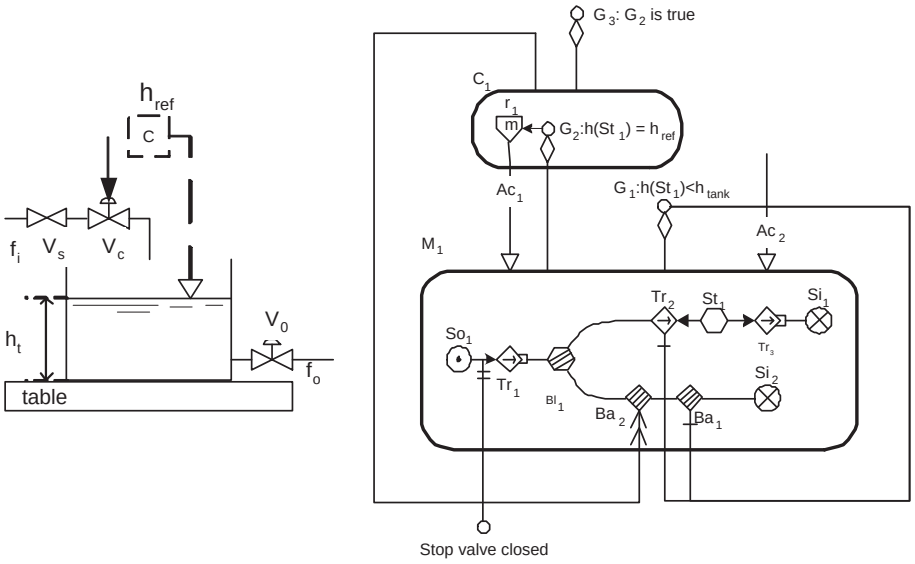


Figure 6.2: MFM model of tank with feedback control of input valve

6.2.1 Functional integration

The model in figure 6.2 can now be extended to the model shown in figure 6.3 by including an additional purpose of the regulator which is to provide a balance of input and output flows to the tank. This purpose is expressed by the balance function Bl_2 in flow structure M_2. Note that a flow function can be shared by several flow structures without a contradiction because each flow structure represent a particular view or abstraction of the system. The balance function Bl_1 (and other flow functions and relations) can therefore be part of both flow structure M_1 and M_2.

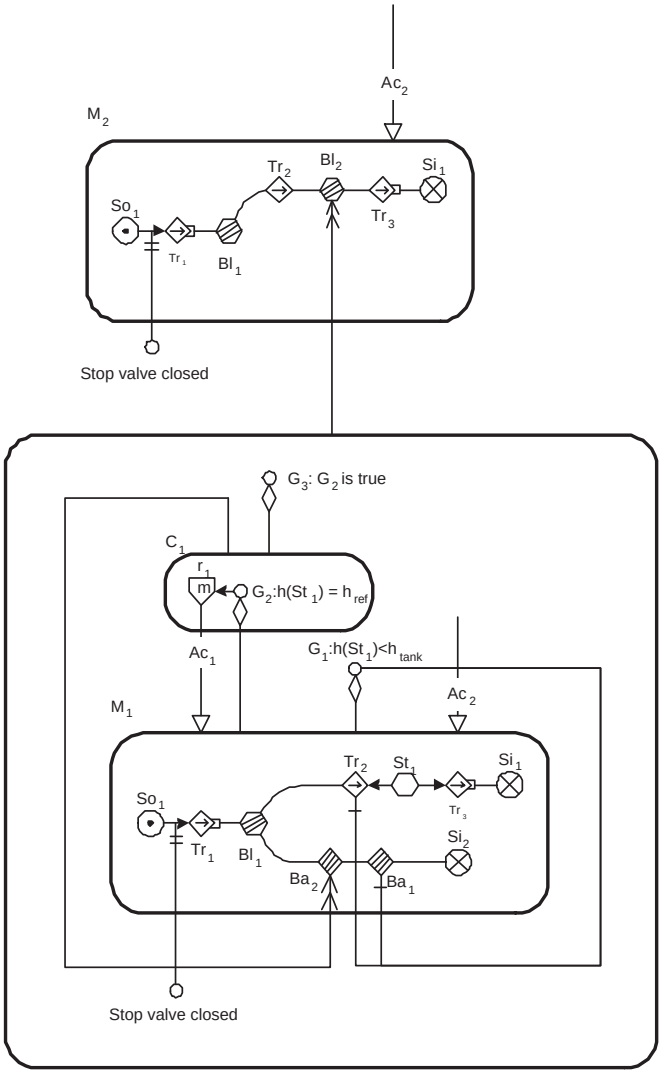


Figure 6.3: Integrated MFM model of tank with feedback control of input valve

6.2.2 Including a safety control system

We can expand the model in figure 6.2 in another direction by introducing a safety control system which closes the stop valve when the water spill over in the tank. The safety control system is represented by the functions in control structure C_2 shown in the expanded model in figure 6.4. The purpose of the safety control system is to destroy the spill over condition. The control is done by closing V_s represented in the model as the conditioning of a causal role.

It is seen that the safety control system includes an additional barrier Ba_3 in flow structure M_1. The safety control system contributes accordingly with a third level of defense against the spill over condition.

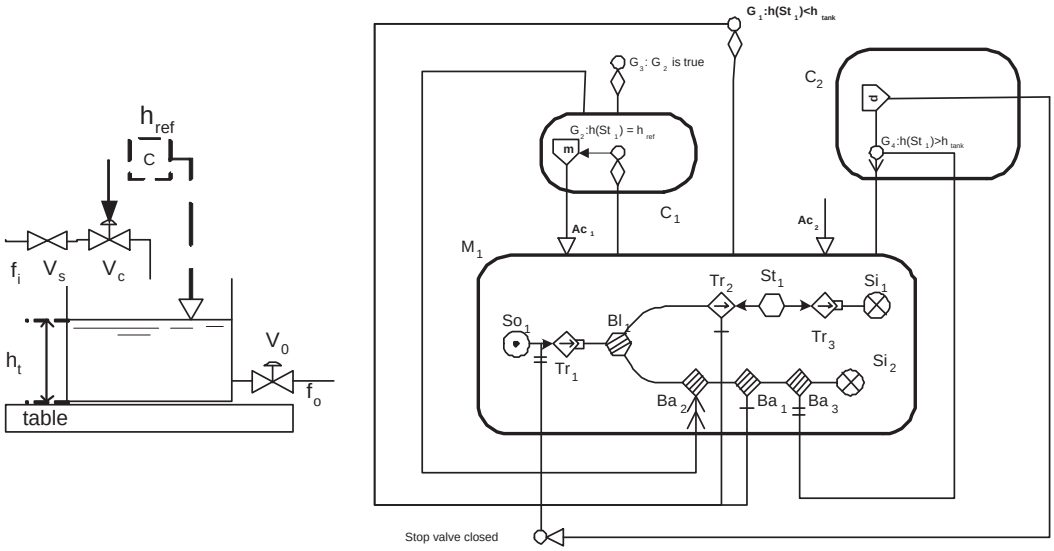


Figure 6.4: MFM model of tank with feedback control of input valve and protection system

Chapter 7

Conclusions

The purpose of the present work has been to develop concepts for modeling goals and functions of control and safety systems in MFM. The development solves a number of problems which has remained unsolved for some time. The following results have been obtained:

- It has been shown that it is both possible and meaningful to separate the purpose of control systems to determine the state of the system under control from the information processing means used for its accomplishment
- It has been demonstrated that the action theory proposed by VonWright [23] and extended by Lind [12, 14] can be used as a systematic basis for the extensions of MFM that were required to model goals and functions of control and safety systems
- Elementary and more complex control patterns have been developed which define how goals and function of control and safety systems are related to goals and functions of the system under control
- It has been demonstrated that MFM with the extensions proposed can handle the entanglement of goals and functions of the control and safsty systems and the process under control
- It has been demonstrated that MFM with the extensions proposed can be used to represent relations between safety and non-safety functions
- It has been demonstrated that MFM may provide a basis for formalized modeling of safety chains and defense in depth

7.1 Suggestions for further work

It should be stressed that the research presented here should be seen as the first concentrated effort to establish a theoretical foundation for modeling control and

safety in MFM. A number of important new results have been generated but the work has also created a number of new problems for further investigation. It has also been necessary to focus the work in order to produce results whose value that could be demonstrated in model examples. The following topics should be investigated in future work:

- The action theoretical foundation should be extended to include the interaction between two or more agents. This extension is necessary in order to derive MFM concepts to model goals and functions of multi-variable controls.
- Concepts should be developed to compose elementary control actions into more complex control flow structures such as sequences and parallel control actions. A particularly challenging problem is here to be able to model start-up and shut-down controls whose purpose is to change the functional structure of the plant
- More complex modeling examples should be investigated in order to validate the proposed concepts and to identify more schemes for functional integration that can express the purposes of more complex control strategies
- The substitution of the achieve relation in MFM with an extended set of relations (produce, maintain, destroy and suppress) necessitates a systematic study of the temporal aspects of MFM models.
- Further studies are required to identify interdependencies between control and process functions (the problem of entangled functions)
- Rules should be developed for means-end reasoning about control functions
- The inclusion of the functions of counter-agents (disturbances) in MFM models should be investigated

Bibliography

[1] P. Achinstein. *The Nature of Explanation*. Oxford University Press, Oxford, 1983.

[2] W. R. Corcoran, D. J. Finnicum, F. R. Hubbard, C. R. Musick, and P. F. Walzer. Nuclear power-plant safety functions. *Nuclear Safety*, 22(2):179–191, 1981.

[3] A. Gofuku, T. Ohi, and K. Ito. Qualitative reasoning of the effects of a counter action based on a functional model. In *Proc. CSEPC'2004*, Sendai, Japan, November 4-5.

[4] A. Gofuku and Y. Tanaka. A combination of qualitative reasoning and numerical simulation to support operator decisions in anomalous situations. In *Proc. 3'rd IJCAI Workshop on Engineering Problems for Qualitative Reasoning*, 1997.

[5] W. Haddon. Energy damage and the ten countermeasure strategies. *Human Factors*, 15(4):355–366, 1973.

[6] J. E. Larsson. Diagnostic reasoning based on means-end models: Experiences and future prospects. *Knowledge-Based Systems*, 15(1–2):103–110, 2002.

[7] M. Lind. Generic control tasks in process plant operation. In *Proc European Annual Manual (EAM'2)*, 1982.

[8] M. Lind. Representing goals and functions of complex systems - an introduction to multilevel flow modelling. Technical report, Institute of Automatic Control Systems, Technical University of Denmark, 1990.

[9] M. Lind. Functional architectures for systems management and control. In M. Lind, editor, *Interactive Planning for Integrated Supervision and Control in Complex Plant. Final report - Project 4937-92-08-ED ISP DK*. Institute for Systems Engineering and Informatics, CEC Joint Research Centre, Ispra Italy, 1993.

[10] M. Lind. Modeling goals and functions of complex industrial plant. *Applied Artificial Intelligence*, 8(2):259–283, 1994.

[11] M. Lind. Plant modeling for human supervisory control. *Transactions of the Institute of Measurement and Control*, 21(4-5):171–180, 1999.

[12] M. Lind. Promoting and opposing. NKS-R-07 project report, Ørsted DTU, Technical University of Denmark, 2002.

[13] M. Lind. Making sense of the abstraction hierarchy in the power plant domain. *Cognition Technology and Work*, 5(2):67–81, 2003.

[14] M. Lind. Description of composite actions - towards a formalization of safety functions. NKS-R-07 project report, Ørsted DTU, Technical University of Denmark, 2004.

[15] M. Lind. Means and ends of control. In *Proc. IEEE Conf. Systems Man and Cybernetics*, The Hague, Holland, October 10-13 2004.

[16] A. Miller and P. Sanderson. Modeling "deranged" physiological systems for ICU information system design. In *Proc. HFES/IEA 2000, Human Factors and Ergonomics Society*, San Diego, July-August 2000.

[17] C. Morris. *Signification and Significance*. The MIT Press, Cambridge, 1964.

[18] J. Petersen. Means-end models of safety related organizational processes. In *Proc. International Conference on Probabilistic Safety Assessment and Management PSAM7/ESREL'04*.

[19] J. Petersen. Situation assessment of complex dynamic systems using MFM. In *Proceedings of 8th. IFAC/IFIP/IFPRS/IEA Symposium on Analysis, design and Evaluation of Human-Machine Systems*, pages 645–650, Kassel, Germany, September 18-20 2001.

[20] J. Rasmussen, A. M. Pejtersen, and L. P. Goodstein. *Cognitive Systems Engineering*. John Wiley, New York, 1994.

[21] M. C. Robbins, G. F. Eames, and J. R. Mayell. Nuclear safety chains. *Proceedings of the IEE*, 128C(2), 1981.

[22] W. A. Trost and R. J. Nertney. Barrier analysis. SCIE-DOE-01-TRAC-29-95, Technical Research and Analysis Center, Scientech Inc, Idaho Falls, Idaho, USA, 1995.

[23] G. H. Von Wright. An essay in deontic logic and the general theory of action. *Acta Philosophica Fennica*, 21, 1968.

Appendix A

Standard MFM Concepts and Extensions

The extensions of MFM with concepts and symbols to model control goals and functions has required modifications and extensions of the MFM modeling concepts described previously by Lind [9, 10, 11] and Petersen [19]. The modifications and extensions have mainly been motivated by the insights gained by the derivation of dual interpretations to VonWright's elementary action types. The following modifications and extensions have been made and are included in tables A.2 and A.3 below.

The achieve relation has been substituted by four relations; produce, maintain, destroy and suppress corresponding to the four elementary action types. In this way we can express finer distinctions in regard to the temporal aspects of the means-end relation. We can at the same time distinguish actions where the focus is on the final state of affairs (produce and maintain) from actions where the focus is on the initial state of affairs (destroy and suppress).

Goals are now termed focal states in order to accommodate to the extension of the achieve relation. This change of terms was decided because it seemed not sensible to call a state which is destroyed or suppressed a goal state. It is more meaningful to call it a focal state because of the key role it plays in describing the intention in an action. The same argument applies for a state which is suppressed.

Conditions played an important role in standard MFM and they were always combined with an achieve relation. The substitution of the achieve relation with four new relation types therefore required the introduction of a condition type which can express disablement of a function. This relation is called a neg-condition.

Conditional causal roles. In some modeling problems the existence of causal roles is conditional on certain state of affairs. We therefore have introduced the

possibility of connecting the condition relations with causal roles.

A.1 Flow functions

Name and symbol	Explanation
Storage 	A storage represents the functions of a system which serve as an accumulator of mass or energy. A storage function can have any number of connections and any number of 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 	The 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
Source 	The source represents the function of a system which serve as an infinite reservoir of mass or energy. No physically realizable system can in principle unlimited capability to deliver mass or energy. However, this representation may in many cases provide an adequate abstraction of the physical phenomena considered
Sink 	The sink represents the function of a system which serve 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
Transport 	A transport represents the function of a system which serve to transfer of materials or energy between two other systems. As for the storage function we distinguish between mass and energy transport. A transport function has always two and only two connections and none, one or several conditions. Furthermore, a transport function is associated with a flow direction as indicated by the arrow in the transport symbol. Note that the flow direction is not identical to the directions defined by the causal roles.
Barrier 	A barrier represents the function of a system that serve to prevent the transfer of materials or energy between two systems. Typical examples of systems which implement barrier functions are the cladding on nuclear fuel rods, heat isolating material and a trap in water systems. The function of the cladding in nuclear fuels is to prevent the flow of radioactive materials from the fuel (uranium isotopes) to the cooling water. The function of heat insulating material is to prevent the heat energy to flow. The function (one of the functions) of a trap is to prevent air from the sour system to pass through

Table A.1: Flow functions in MFM

A.2 Vertical relations

Name-symbol	Explanation
Produce 	Objectives are achieved by performing certain functions. Therefore we have a produce relation. The relation is a means-end relation where the objective is the end and the function or systems of functions are the means. When using the (A) relation, the function represent the purpose of the material and energy transformation processes.
Maintain	Objectives are maintained by performing certain functions. Therefore we have a maintain relation. The relation is a means-end relation where the objective is the end and the function or systems of functions are the means.
Destroy	Objectives are destroyed by performing certain functions. Therefore we have a destroy relation. The relation is a means-end relation where the objective is the end and the function or systems of functions are the means.
Suppress	Objectives are suppressed by performing certain functions. Therefore we have a suppress relation. The relation is a means-end relation where the objective is the end and the function or systems of functions are the means.
Condition	An objective can also define a condition that is necessary for the enablement of a function. This conditioning is expressed by a condition relation between the objective and the function.
Neg-Condition	An objective can also define a condition that is necessary for the disablement of a function. This conditioning is expressed by a neg-condition relation between the objective and the function.
Producer-Product	Functions can be related through a relation called a producer-product (PP) relation. This relation is used when the temporal interactions between a set of functions (a process) result in a transformation that again serves another function in the system.
Mediate	Functions can also be related through another causal relation called a mediate (M) relation. This relation is used when a system has the role of being an intermediate between an agent and another system that serve as an object of action.
Actuate	An actuation relation connexts a control function with the flow structure containing the flow function under direct control.

Table A.2: Vertical relations in MFM

A.3 Horizontal relations

Name and symbol	Explanation
Connection	A functional connection provides a contextual linkage of two functions meaning that they relate to the same goal perspective or that they share objects (they change properties that belong to the same object or substance
Sender	A flowfunction F connected at the input of a transport T, is a *sender* if the system realizing F has the role of passively providing substance for the transport T
Recipient	A flowfunction F connected at the input of a transport T, is a *recipient* if the system realizing F has the role of passively receiving substance for the transport T
Upstream agent	A flowfunction F connected at the input of a transport T, is an *upstream agent* if the system realizing F has the role of (actively) driving the transport T
Downstream agent 	A flowfunction F connected at the output of a transport T, is a *downstream agent* if the system realizing F has the role of (actively) counteracting the transport T

Table A.3: Horizontal relations in MFM

Bibliographic Data Sheet **NKS-114**

Title	Modeling Goals and Functions of Control and Safety Systems -theoretical foundations and extensions of MFM
Author(s)	Morten Lind
Affiliation(s)	Ørsted DTU, Automation, Danmarks Tekniske Universitet
ISBN	87-7893-175-4 *(Electronic report)*
Date	October 2005
Project	NKS_R_2002_07
No. of pages	41
No. of tables	11
No. of illustrations	13
No. of references	23

Abstract

Multilevel Flow Modeling (MFM) has proven to be an effective modeling tool for reasoning about plant failure and control strategies and is currently exploited for operator support in diagnosis [3, 4] and on-line alarm analysis [6].

Previous MFM research was focussed on representing goals and functions of process plants which generate, transform and distribute mass and energy [10, 11]. However, only a limited consideration has been given to the problems of modeling the control systems. Control functions are indispensable for operating any industrial plant. But modeling of control system functions has proven to be a more challenging problem than modeling functions of energy and mass processes. The problems were discussed by Lind [8, 9, 10] and tentative solutions has been proposed but have not been investigated in depth until recently, partly due to the lack of an appropriate theoretical foundation.

The purposes of the present report are to show that such a theoretical foundation for modeling goals and functions of control systems can be built from concepts and theories of action developed by Von Wright [23] and to show how the theoretical foundation can be used to extend MFM with concepts for modeling control systems. The theoretical foundations has been presented in detail elsewhere by the present author [12, 14] without the particular focus on modeling control actions and MFM adopted here.

Key words Multilevel Flow Modeling, control actions, safety systems, theoretical foundation.

Available on request from the NKS Secretariat, P.O.Box 49, DK-4000 Roskilde, Denmark.
Phone (+45) 4677 4045, fax (+45) 4677 4046, e-mail nks@nks.org, www.nks.org