

MODELING GOALS AND FUNCTIONS OF COMPLEX PLANT

Morten Lind
Institute of Automatic Control Systems
The Technical University of Denmark
DK-2800 Lyngby Denmark

ABSTRACT

The purpose of this paper is to describe a modeling methodology called Multilevel Flow Modeling (MFM) which has been developed by the author for the representation of goals and functions of complex process plants. The idea of the methodology is to apply functional concepts to represent a plant on several interrelated levels of abstraction. MFM is currently used for the development of diagnosis and planning systems for operator support in supervisory control and in the conceptual analysis and synthesis of control systems. The paper provides an introduction to the basic concepts of MFM and describes in detail two modeling examples. A short description is also given of the object oriented tool ABSTRACTIONS which has been developed for the implementation of MFM models and the diagnosis and planning applications. Finally, the paper presents a review of previous and ongoing international projects where MFM is used.

1. BACKGROUND

Multilevel Flow Modeling has been developed in order to address modeling problems which are common to different automation design tasks in industrial plants. These tasks comprise the design of the human-machine interface and the design of the automated control systems. The modeling problems addressed are characterized briefly below as a motivation for the more technical sections to follow.

Diagnosis of disturbances and on-line planning of remedial actions in industrial plants are difficult to handle by operators because these tasks require complex interpretations of real time data. Due to their limited resources of time and information processing capacity, operators need to develop efficient strategies for coping with this complexity. This is especially needed when solving diagnostic problems which call for reasoning about the plant functions such as in the case of unforeseen plant incidents. Depending on the nature of the operators task and his/her experience different types of display information and computer supports are required in order to provide efficient guidance to the operator in decision making. Rasmussen distinguish in [Rasmussen86] between so called skill, rule and knowledge based operator behavior. Skill based behavior is appropriate in routine situations and does not involve reasoning processes. But when the operator cannot rely on his highly trained motor skills or on stereotyped (rule based) responses to plant symptoms, knowledge based behavior is required. Such situations occur in the event of infrequent high risk plant disturbances. However, knowledge based behavior is dependent on the use of deep knowledge of the plant and high demands are consequently put on the operator if the interpretation of such complex events is not aided by computer. Rasmussen argue therefore that operators need computer support for knowledge based tasks.

Rasmussen and Lind describe in [Rasmussen81] strategies used by operators in coping with complex supervisory tasks. The main strategy is to use multiple representations of the plant based on a dual decomposition principle using means-end and whole-part concepts. Given these representations, the operators can reduce the need for information processing. But as reasoning about deep knowledge in real time is demanding, operators tend to resort to skill or rule based response patterns if they are not supported by display information structured according to those representations. Therefore, the plant information displayed on the supervisory console should match the types of representations used by operators in order to avoid human error in situations of high risk. As a further consequence, the knowledge bases of computer based diagnosis and planning support systems could with advantage apply the same plant representations. This so-called cognitive engineering of the human-machine interface is accordingly dependent on a modeling of the plant based on means-end and whole-part decompositions.

The description of a plant on several levels of means-end abstractions prove also to be useful in control systems design. Here the problem is to derive proper strategies for decomposing the plant into smaller independent functions, and to synthesize control actions which achieve and maintain those functional structures. These decomposition problems become critical when handling complex plants because the number of alternative decompositions is very large. The representation of the plant using means-end and whole-part concepts provides therefore also a convenient setting for solving control systems design problems in complex plants.

As the same representations are useful for both the design of the human-machine interface and for the design of the automated systems, they offer a conceptual basis for modeling and integrated design of the total plant automation system.

2. MULTILEVEL FLOW MODELING

The aim of MFM is to provide a systematic basis for using means-end and whole-part decompositions in the modeling of complex industrial plant. As seen in the following, the two decompositions will lead to multiple levels of means-end and whole-part abstractions.

By the distinction between means and ends, a system is in MFM described in terms of goals, functions and the physical components. At the same time, each of these descriptions can be given on different levels of whole-part decompositions. The main types of decomposition are illustrated below in fig. 1.

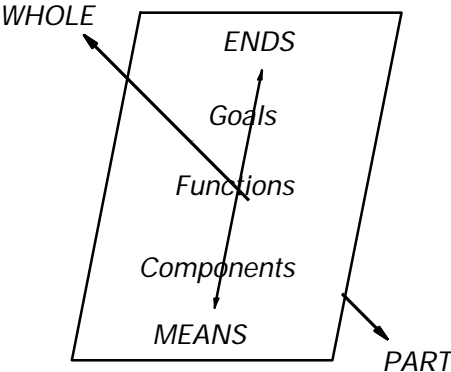


Fig. 1. Types of plant decomposition used in MFM.

We can illustrate the use of the two dimensions of the MFM representations by means of a small example from a central heating system. Even though this system is fairly simple it illustrates well general aspects of MFM especially the use of function concepts. The example is shown in Fig. 2. where the water circulation circuit of a central heating system is described in terms of its goals, functions and its physical components.

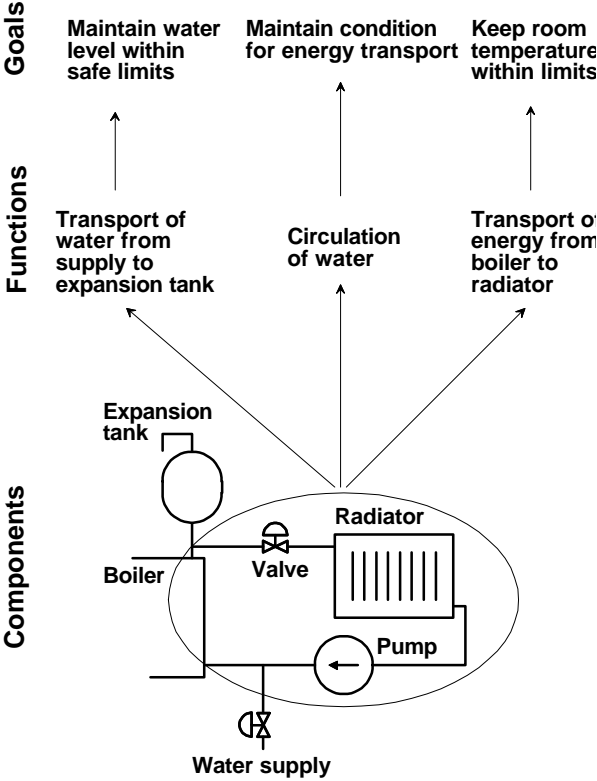


Fig. 2. Goals and functions of a circulation system

It is seen that the physical parts, the components, of the circulation circuit *realizes* different functions. It is also shown that these functions contribute to the *achievement* of system goals. Actually, the functions are each ascribed to the system with a specific goal in view. Thus if we chose the goal of 'maintaining the water level within safe limits', then the relevant function of the circulation circuit is to transport the water from the supply line to the expansion tank. If we, on the other hand, chose the goal of keeping the temperature within limits, then the function of the circulation circuit is to transport the energy from the boiler to the radiator. As the functions describe how the behavior of the components are useful for the achievement of various purposes or goals, we cannot meaningfully separate the ascription of the functions from the selection of goals. The functional ascriptions are dependent on a predefined context of one or several goals.

The principles of the whole-part decomposition can also be illustrated. For example we could aggregate (the inverse of decomposition) the three goals into a super ordinate goal, a whole, saying that 'the central heating system should operate properly'. Furthermore, as another example, we could decompose the function of transporting energy from the boiler to the radiator into several connected transport functions each describing the functions of the heat transfer between the burning air-gas mixture, the piping and the water in the boiler. Finally we could decompose the circulation circuit into the pump, the boiler, the valve, the radiator and the piping. Even though these decompositions (and aggregations) can be done

independently, they are strongly coupled if the descriptions of plant components, functions and goals should be related as means to some ends i.e. if they should combine into a proper MFM model. As an example illustrating this dependency, it would not be meaningful to associate the individual components of the circulation circuit with any of the functions mentioned in the example. The functions are the result of the behavioral *interactions* between the components. However, in spite of these constraints of realization and achievement between the descriptions it will often be possible to choose between alternative levels of decomposition. Eventually, the criteria for choosing between alternatives depend on the application of the model i.e. if it is used for diagnosis or for planning. These semantic and pragmatic aspects of MFM modeling are discussed in [Lind93], [Larsen93] and [Jørgensen93].

Often there will be many alternative realizations of the same function and alternative ways of achieving the same goal. Thus, the water circulation function can be realized by different behaviors of the components in the circulation circuit. The water circulation can be caused by the revolution of the pump impeller or it can, under certain conditions, be caused by a difference in temperature between the hot water leaving the boiler and the cold water entering from below (so-called natural circulation).

In conclusion, we can from this simple example make some general observations of the nature of MFM models. First of all it is seen that the means-end and whole part decompositions in themselves lead to a multiple of interdependent representations of the same system linked by many-to-many relations of realization and achievement. Secondly, as MFM specifically address the dependency of functional descriptions on a context of goals, each plant goal or subgoal will in principle define its own separate starting point for application of the two types of decomposition. The full implications of this does actually not show up in the example. We will need the machinery of the formalized MFM concepts for discussing this important and unique feature of MFM.

Most plant systems have the features described above and the nature of the many-to-many relations of realization and achievement between components, functions and goals are fundamental to the understanding of complex systems. They are therefore important for solving the tasks of a plant or a control systems designer or a plant supervisor in charge of on line plant resource management. Multilevel Flow Modeling provides formalized concepts to describe these relations.

2-1. Goals, Functions, Behavior and Structure

Before we introduce the basic concepts of MFM we will discuss how the two concepts of goal and function are distinguished from the concepts of structure and behavior. We already talked about behavior above but as there is some confusion in the literature on the exact nature of the distinction between function and behavior, it would be useful to clarify how the distinction is made in MFM.

The distinctions between structure, behavior, function and goals can be made by a slight elaboration of the means-end aspect of fig. 1. This elaboration is shown in fig. 3.. The level of components in fig. 1. is in fig.3. represented by the structural and the behavioral levels in combination. By this we mean that plant knowledge on the component level comprise both a structural aspect (plant physical parts and their interconnection in the physical topology) and a behavioral aspect (the physical mechanisms or phenomena responsible for the interactions between component variables). As also indicated in fig. 3., these two levels capture the causality of the system. As a contrasts to these two levels we have indicated that in MFM the levels of functions and goals are representing the designers intentions with the system (MFM is, at the present stage, only dealing with the component level in a very superficial way).

These two views, the causal and the intentional, are connected with two different scientific domains, the natural sciences (causality) and the social sciences (intentionality). This is one of the reasons for the confusions regarding the definition of the concept of function. Some define function to be equivalent to behavior whereas others (including MFM) define functions as purely intentional concepts (see e.g. [Lind90a] for a discussion of some of these distinctions).

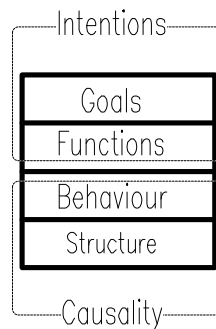


Fig. 3. Causal and intentional aspects of systems

As mentioned in [Achinstein83] it is also necessary to distinguish between design-functions, use-function and service-functions. These distinctions are elaborated further in [Lind93]. Functions in MFM describe the intentions of the designer (i.e. design functions) and the models *explain* why the plant equipment is there i.e. MFM models describe plant teleology. An attempt, sufficient for the present purpose, to capture this meaning is presented below.

***Definition:** Functions represent the roles the designer intended a system should have in the achievement of the goals of the system(s) of which it is a part.*

In conclusion, it is important not to blur the distinction between behavior and function as this is necessary in order to be able to characterize a system as an artifact [Simon84] i.e. to make a distinction between systems designed for a human purpose and a purely natural phenomenon.

2-2. Relations between MFM and other Research in Functional Modeling

Research in qualitative reasoning has developed methods to derive behavior from structure [deKleer84][Forbus81][Kuipers84]. The relations between function and behavior has been recognized in this research but is hidden as assumptions introduced to resolve the inherent ambiguities in the behavioral models generated from structure. Keunecke has recognized the need of making these assumptions explicit by developing concept for the representation of the intended behavior i.e. the functions [Keunecke91]. This provides a constructive link between structure, behavior and function. These links has been further strengthened by Woods in his Hybrid Phenomena Theory where also concepts for the representation of basic physical phenomena has been introduced [Woods93] and methods to generate ordinary differential equations from qualitative knowledge are given.

MFM offers new aspects to the research in this area by introducing goals as a necessary concept for the representation of man-made physical systems and by pointing out that goals and functions are distinct concepts that cannot be isolated conceptually when used. Furthermore, the links between levels of description are strengthened by MFM due to the semantics constraints of the means-end and the whole-part decompositions.

2-3. Categories of Means and Ends

When modeling industrial plants we need to distinguish between different categories of means and ends. There is one distinction which is especially important. It is illustrated in fig. 3. and makes a separation of the means and ends related to the production of products based on materials and energy, and the means and ends related to the management of changes and disturbances in the production. The distinction is of course not novel as it corresponds to the common sense distinction between two type of processes involved in running plants namely the processing of raw material and energy and the processing of information.

The means of production comprise the raw materials, energy and the plant equipment. The ends or goals of the production are the specifications to the product and the operational requirements of the equipment.

The means of change management comprise the instrumentation, the sensors and the actuators, and the knowledge and methods used by the agents (computers or people) in plant management and control. The ends or goals of change management comprise the specifications to the performance of the agents comprising response characteristics of the controllers, goals of the diagnostic processing and the planning. As indicated in fig. 3. equipment used for the production of products can also participate in the management of changes. Pumps are good examples of such equipment. As such equipment participates in two different goal contexts they will accordingly also have different functional representations. This is also reflected in common language when a pump is called an actuator. Actuation is the function of the pump in the context of achieving goals of control.

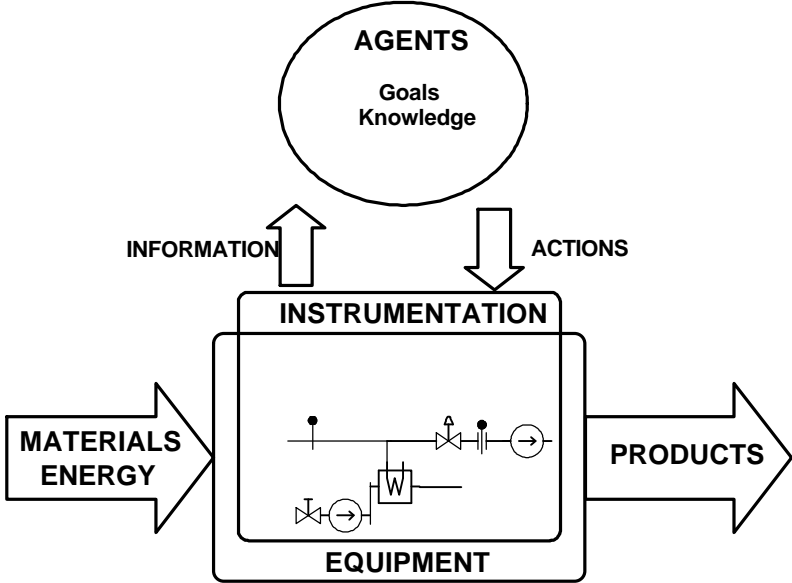


Fig. 4. MFM represent two categories of means and ends

Thus even though the distinction is not new it is important when applying concepts of goals and functions in plant modeling. In the following sections we will show that MFM provides concepts to model both the goals and functions of production and the goals and functions of change management (control). Furthermore, it will also be shown, by an example, how an MFM model can combine the representations of these distinct categories of means and ends in one single model.

2-4. The Basic MFM Function Concepts

In MFM plant functions are represented by a set of mass, energy, activity and information flow structures on several levels of abstraction. The levels are interdependent and form means-end structures. Mass and energy flow structures are used to model the functions of the plant and activity and information flow structures are used to model the functions of the operator and the control systems.

These flow function concepts and their associated symbols are shown in Fig. 5. Using these concepts it is possible to represent knowledge of complex process plant which capture the intentions of the plant and control systems designer. This type of knowledge is useful for forming high level heuristics for solving problems of diagnosis, planning and design. The use of a rather small set of basic function concepts provide in addition a certain cognitive economy. At the present stage of development MFM is restricted to the modeling of continuous plant. Comprehensive discussions of the MFM concepts are given in [Lind90a] and [Lind93]. The relations between MFM models and other model categories are discussed in [Lind92].

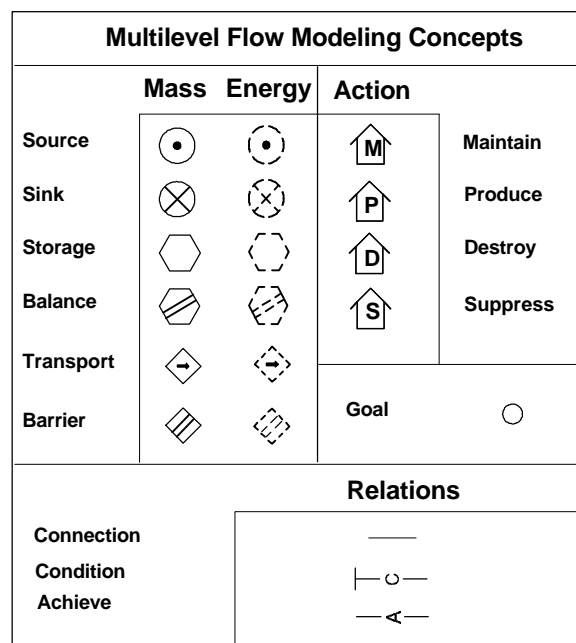


Fig. 5. Multilevel Flow Modeling Concepts

It is seen from fig. 5. that MFM distinguish between functional concepts for the representation of mass and energy processes and functional concepts for representing the function of actions (control). Furthermore a set of relations are also defined. These relations are used to describe various relations between functions and goals in plants. The achievement relation is a means-end relation and the condition relation is used to describe that the existence of a function can be conditional on a plant state. Those state becomes goals for other plant subsystems. The connection relation is used to interconnect flow functions into so-called flow structures. The use of the relations will be explained in the examples described later.

The following sections will introduce the functional concepts. Especially, the concepts used for modeling the function of actions will be discussed at length. This emphasis is required because these concepts may seem more abstract than the concepts used for modeling mass and energy functions.

2-4-1. Mass and Energy Functions

It is seen that the concepts used for modelling the functions of mass and energy processes in the plant are taken from thermodynamics. However, it should be noted that they should not be considered simply as instances of physical mechanisms. They should be interpreted as more general functional notions. The barrier functions are used to model systems whose purpose is to prevent the transfer of mass (mass barrier) or energy (energy barrier).

2-4-2. The Functions of Actions

The MFM concepts for modeling the function of actions corresponds to the basic roles agents can have when engaged in goal directed activity and activity flow structures represent higher level patterns in their interaction. One of the examples described below illustrates the use of these functions.

These concepts have been developed from a logical basis. In order to introduce this logical basis it should be realized that, from the point of view of the achievement of production goals, the activities of plant control comprise the observation and analysis of changes i.e. disturbances and upsets in the system, and interventions in the system intended to make planned changes in the state of the system. Since the purpose or functions of the activities of the agent therefore are to make or counteract changes it seems natural to use a classification of changes as a basis for the definition of the functions of control. VonWright(1963) has developed such a classification of so-called elementary changes which he has used for the classification of (intentional) actions. These classifications provides the direct basis for our definition of so-called elementary functions of actions. These functions will be analogous to the flow functions used for modeling energy and mass functions (source, sink, transport, storage....).

2-4-2-1. Elementary changes.

The four types of elementary change defined by VonWright are the four types of change and not-change which are possible with regard to a given (atomic) state of affairs and a pair of successive occasions p and q . VonWright introduces a so-called *schematic description* of a change by the symbolism pTq meaning that the state p is transformed into state q . Using this symbolism four types of elementary change can be defined by: pTp , $pT\sim p$, $\sim pTp$ and $\sim pT\sim p$. The change description pTp means accordingly that the state p is maintained¹, $pT\sim p$ means that the state p is destroyed, $\sim pTp$ means that the state p is produced and $\sim pT\sim p$ means that p is suppressed.

2-4-2-2. Elementary Acts.

We can now introduce VonWright's notion of an elementary act. By an *elementary act* is understood an act the *result* of which is an elementary change. The correspondence between elementary act and elementary change is therefore one to one.

VonWright use the symbol d for acting and the schematic descriptions of the four types of elementary act are $d(pTp)$, $d(pT\sim p)$, $d(\sim pTp)$, $d(\sim pT\sim p)$. Note that $d(pTp)$, etc., are schematic representations of sentences which describe acts, just as pTp , etc. are schematic

¹ We use the term 'maintain' instead of the term 'preserve' used by VonWright(1963b). This does not change the meaning but facilitate the use of simple symbols for representation of management functions in MFM.

representations of sentences which describe changes, and p , etc., are schematic representations of sentences which describe (generic) states of affairs.

In order to explain the nature of the four types of action we will assume that p represent the state 'the valve is open'.

We will first consider $d(\sim pTp)$ which describes the act of changing or transforming a $\sim p$ world to a p -world. With the state p in our example it describes the act of opening the valve. Thus $d(\sim pTp)$ whose generic meaning is 'the production of p ' in the example represents the sentence 'the valve is being opened'. The expression $d(pT\sim p)$ describes the act of 'the destroying of p '. With the example it describes the act of closing the valve. The act $d(pTp)$ describes that the world does not change in the feature described by p on two successive occasions i.e. it means 'the maintenance of p ' i.e. in our example situation it would describe the act of 'keeping the valve open'. Finally $d(\sim pT\sim p)$ describes the world unchanged in the feature described by $\sim p$. This act therefore

Condition of action	Action	Result of action
$pT\sim p$ p is but vanishes unless maintained	$d(pTp)$ p is maintained	pTp p remains
$\sim pT\sim p$ p is not and does not happen unless produced	$d(\sim pTp)$ p is produced	$\sim pTp$ p happens
pTp p is and remains unless destroyed	$d(pT\sim p)$ p is destroyed	$pT\sim p$ p vanishes
$\sim pTp$ p is not but happens unless suppressed	$d(\sim pT\sim p)$ p is suppressed	$\sim pT\sim p$ p remains absent

Table 1. The elementary acts (VonWright, 1963b)

represents 'the suppression of p '. In the example with the open valve this act would represent a situation where the valve is closed but will open unless an agent does not keep it closed. The valve could be a pneumatic valve designed to open in the event of loss of air. In the event of air loss the operator could manually suppress the opening of the valve by is keeping it closed.

The four basic actions can, as pointed out by VonWright, only be done provided some conditions are fulfilled. As an example; it is not possible to do 'the maintenance of p ' if not p is and will vanish unless maintained. Thus the act of 'keeping the valve open' is only possible if the valve is already open and the valve will close if the act is not done. It is realized that these conditions are of a logical nature as they are intrinsic to the definition of the act. The conditions for each type of act are discussed in detail by VonWright (1963) and are summarized in table 1.

2-4-2-3. Elementary Management Functions

As mentioned above we can use the four elementary actions to represent functions provided by control. To each category of action corresponds an elementary function of an agent engaged in the handling of changes in a system. The correspondence between elementary acts and elementary management functions is as follows:

- $d(pTp)$: (the maintenance of p) - represent the function of an agent maintaining the state p i.e. the function of the agent would be 'regulation'. The agent function only as a regulator if the state p is but vanishes unless maintained i.e. if the system is disturbed.
- $d(\sim pTp)$: (the production of p) - represent the function of an agent achieving the state p i.e. the function of the agent would be 'servoing'. The agents function is only servoing if the state p is not and does not happen unless produced.
- $d(pT\sim p)$: (the destroying of p) - represent the function of an agent which is destroying the state p i.e. the function of the agent is to trip or shut the system down. The agents function is only to trip the system if p remains unless destroyed.
- $d(\sim pT\sim p)$: (the suppression of p) - represent the function of an agent which is preventing that the state p is occurring i.e. the function of the agent would be 'interlocking'. The agents function is only interlocking if p is not but happens unless suppressed.

The symbols shown in fig. 6. are used to represent the functions of control. An example of their use will be described later.



Fig. 6. The symbols used to represent control functions.

The functional descriptions of agents introduced above does not reflect how the function is accomplished i.e. the means used for their realization. Accordingly no mention is made of feedback and feed forward structures often used to realize control functions. These structures are from a functional view merely to be considered as different means for *realizing* control functions. Note also that because the functional descriptions does not specify the nature of the state p , we can use the functional concepts to model agents engaged in such diverse activities as the control of a mission, to keep a robot on a planned path, to manage the change of configurations during start-up or shut down of a power plant or to describe the function of the thermostat regulating temperature in a central heating system.

The terms 'regulation', 'servoing', 'tripping' and 'interlocking' could therefore be used with a much wider meaning than they usually are within control engineering. However, we will use the more abstract notions of 'maintain', 'produce', 'destroy' and 'suppress' and let the nature of the state of the goal proposition p determine the specific meaning. In this way a potential source of misunderstanding is destroyed. But unfortunately we may at the same time produce a risk of not being understood .

2-4-2-4. Composition of Elementary Control Functions.

The elementary control functions described above can only describe the most basic functions of control. More complex functions can be obtained by a composition of a number of elementary functions (examples are shown in the example above). The problems of compositions of elementary control functions will not be investigated here as it is a topic of research in its own right. The logic of action developed by VonWright seems to be a promising basis for this. However, a few initial observations will be made from the logical structure of the elementary control functions.

2-4-2-5. Economy or flexibility of expression.

First of all we can observe that four elementary functions according to the definitions above can be reduced to two because the following relationships holds:

maintain $\sim p \Leftrightarrow$ suppress p
produce $\sim p \Leftrightarrow$ destroy p
destroy $\sim p \Leftrightarrow$ produce p
suppress $\sim p \Leftrightarrow$ maintain p

These equivalences gives a certain freedom in the modeling which can be useful and the redundancy will therefore not be removed. They may be useful in modeling situations of conflict e.g. where a production goal p is maintained by one agent and another agent is suppressing p . The same situation could on logical grounds also be described as a situation where the latter agent is maintaining $\sim p$. In the latter case the model would include both p and $\sim p$ and it would not be immediately obvious from the model that the agents are in conflict (the goals would be represented as two separate nodes in the model). Of course the model language could be extended to handle this situation also by introducing means of expressing the logical relations between p and $\sim p$. In conclusion, the choice between the alternative ways of representing the same functions seems to be a matter of convenience. However, to aim for flexibility of expression seems to be better than aiming for a minimal number of concepts.

2-4-2-6. Sequencing, Concurrency and Activity Flow Structures.

The elementary control functions can be combined into sequences. However, due to strong logical relations between the elementary control functions the number of possible sequences is restrained. The number is extremely limited because each function has a condition to be satisfied and because the condition should be the result of the preceding function in the sequence. From table we can derive the following two possible sequences:

produce p - maintain p
destroy p - suppress p

The functions are furthermore dependent due to their conditions such that the following pairs of functions must be concurrently present:

(maintain p , destroy p)
(produce p , suppress p)

These dependencies means that the function of maintain p is always present concurrently with destroy p and produce p is always present together with suppress p . The reason for these constraints on the combination of the control functions is of course that we are only considering a single state p .

The conditions for the functions given by VonWright are important because they define conditions for the mutual fitness of a set of composite functions involved in e.g. a plan. If a condition is not fulfilled the function cannot be achieved. The conditions ensure therefore a smooth unbroken flow of activities of the agents performing the functions. The pairs of functions are therefore linked by using the connection relation in MFM (the connection

represent a relation of fitness as mentioned earlier). These structures of connected control functions will be called *activity flow structures*.

As the elementary functions can be used to model control systems and operators in knowledge based systems they seem to be an interesting basis for the modeling of a wide variety of systems. This is the main reason why they are proposed as the basis for the modeling of control functions.

Below we will illustrate the concepts for modeling control functions with a concrete example of a two variable control system.

3. MODELING EXAMPLES

In the following we will illustrate the use of MFM concepts by two representative examples. The first example provides a detailed description of an MFM model of a conventional power plant. This model gives an impression of the typical complexity of an MFM model and demonstrates that MFM is applicable for the modeling of large systems. The second example is a two variable process control system. The latter example show how mass, energy and activity flow structures are combined in an MFM model.

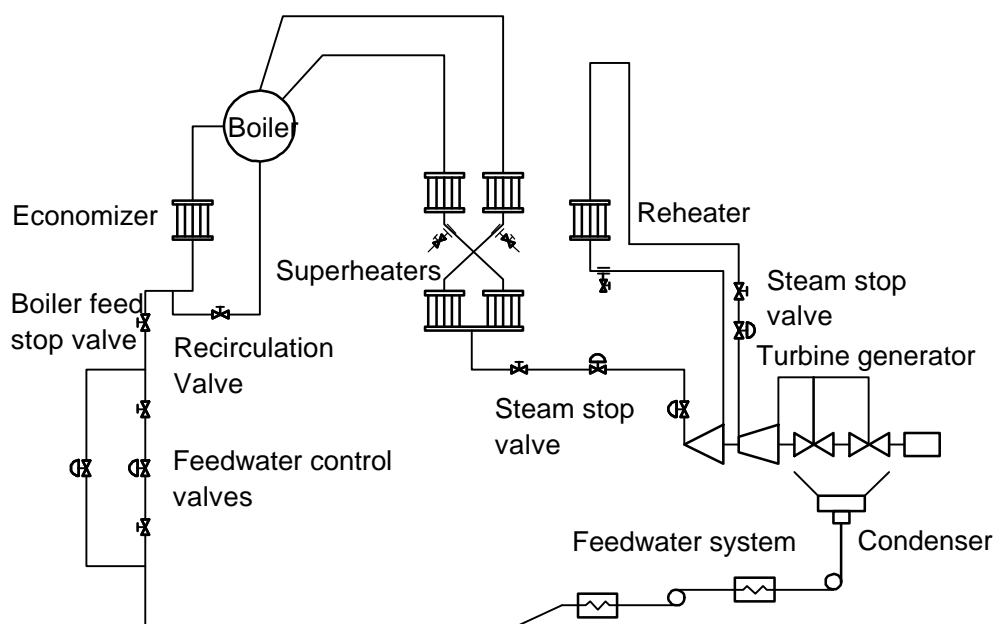


Fig. 7. The Power Plant Boiler

3-1. MFM model of a power plant boiler

The power plant boiler used in the example is described in [West72] and is shown in Fig. 7. An MFM model of this plant is described in [Larsen93] and is shown in Fig. 8. The following sections will explain the model in detail based on the description given by [Larsen93]. When reading the explanation, the reader is encouraged to consult figs. 7 and 8.

When building MFM models, the initial step is to identify the goals for the system. This is necessary because functional descriptions have no meaning without a previously defined goal context. The description below corresponds to this general model building strategy, but it is not reflecting how the model was built. Developing an MFM model is a highly iterative process [Lind90a].

First, we will describe the plant goals G_0, \dots, G_{10} and explain how they relate to the flow structures Structure1, Structure2 and Structure3. Secondly, we will describe the flow structures.

3-1-1. The goals and the related flow structures

The main goal G_0 of the power plant boiler is to generate electricity and it is achieved by the flow functions represented by Structure1. The functions of this energy flow structure are provided by the burner, boiler, turbines and generator. Structure2 describes the mass flow functions involved in the fuel combustion process, and Structure3 describes the mass flow functions provided by the plant components in the water and steam circuit.

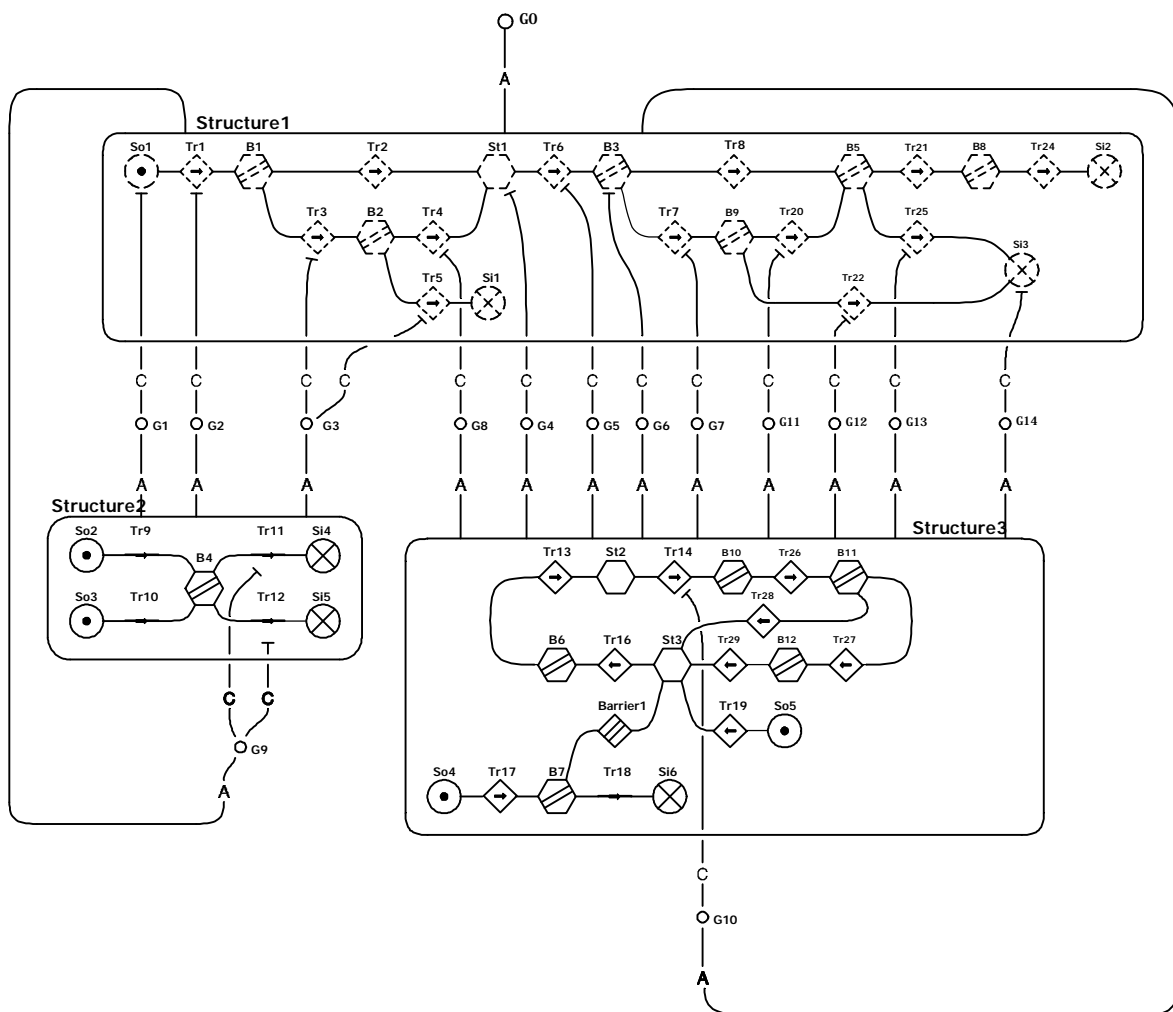


Fig. 9. An MFM model of the power plant example.

Structure2 supports three goals named G_1, G_2 and G_3 i.e. these goals are achieved by this structure. They are all supporting the provision and transport of energy at the first stages of Structure1, the top-level energy flow. G_1 is the goal of providing a proper ratio between the air and fuel flows (in order to ensure combustion). G_2 is the goal of having a flame and G_3 expresses that a flow of combustion gases is needed to carry the heat into the economizer. Related to G_2 is G_9 , which is the goal of having a chemical reaction between the fuel and the oxygen. This goal is achieved by structure1, specifically by means of the energy transport Tr_1

which again is supported by the goal G2. The two goals G2 and G9 thus support each other. In physical terms this means, that when a flame is first established, it is self-supporting. This circularity in the MFM model illustrates the fact that abstraction levels in an MFM model often combines into cyclic networks of goal and means (i.e. in general they are *not* tree structured or hierarchical). Such cycles is the source of start-up problems. In the specific case considered, the flame is needed to ensure transport of energy in the boiler and this transport is a necessary means to maintain the combustion processes i.e. the flame. We therefore need to start the combustion process by another means than the flame, and indeed this is the purpose of the ignition system (not included in the model).

Structure3 is used for achieving five goals G4, G5, G6, G7 and G8 which all support the transport of energy from the boiler to the turbine. G4 expresses the need to maintain a minimum level of water in the boiler and G5 is the goal of having a steam flow from the boiler to the turbine. The energy conversion in the turbine only works properly if the vacuum system is operating, and thus G6 expresses the need to having the vacuum system in operation. Cooling is of course needed, too, and G7 is the goal of having the cooling water at a proper flow, while G8 is the goal of having a feed water flow. One of the functions of structure3 is also conditioned by a goal. The function is Tr14, the mass transport which is provided by the steam piping from the boiler to the turbine. This flow is conditioned by the goal G10, which expresses the need to maintain a pressure in the boiler. This goal is therefore achieved by structure1. This part of the model comprise also a cyclic component.

3-1-2. The flow structures

Resources provided in the plant for goal achievement are represented by the flow functions in Structure1, Structure2 and Structure3. Below we will, without going into too much detail, describe all the flow functions and explain their physical realization.

Structure1 consists of the following functions: The source So1 is the energy source provided by the combustion of fuel and air. This energy is transported by the transport function Tr1 into the balance function B1. Tr1 is realized by (is a function of) the flame, and is hence conditioned by the goal G2. B1 models the balance between the incoming energy flow (Tr1) and the flow of energy into the water in the boiler (Tr2) and the energy flow carried away by the exhaust gases (Tr3). The balance B2 models the energy balance in the economizer, where the heat from the exhaust gases is used to pre-heat the feed water, which provides an energy transport function, modeled by Tr4. The heat eventually carried away from the economizer and "lost" in the chimney is modeled by Tr5. This energy is absorbed by the atmosphere which has the function of a sink, modeled by Si1. The energy transported by Tr2 ends up in the energy storage St1 provided by the water in the boiler. From this energy storage a flow is led by a transport function (Tr6) into a balance (B3) provided by the turbine. From B3 the energy is transported by two flows, one represent the work done on the generator shaft (Tr8) and one representing the residual heat in the steam on the low-pressure side of the turbine (Tr7). These flows end in two energy sink functions. Si2 models the energy sink provided by the generator and Si3 models the heat sink provided by the environment through sea water or the atmosphere.

The functions of Structure2 representing the mass flow functions involved in the management of the fuel and air flows in the burner and fuel supply system. The source function So2 models the oil or coal inventory which, despite its limited capacity plays the role of an infinite source in view of day-to-day operations. In a similar way, the source function So3 models the source of air (oxygen) provided by the atmosphere. From these sources two transport functions lead to the mass balance function provided by the combustion process. The

transport Tr9 models the function of the fuel pumps and pipes and Tr10 models the function of the air blowers and B4 models the combustion mass balance. Tr11 models the outflow of CO₂ and Tr12 models the outflow of H₂O. Only these two exhaust gases are modeled, since they are the basic ones. The sink functions modeled by Si4 and Si5 are both realized by the atmosphere.

Structure3 comprises the functions which are involved in the management of the flows of water and steam around the boiler and the condenser. St2 is the mass storage function that is provided by the boiler, B6 models the mass balance provided by the economizer and St3 models the mass storage function provided by the condenser. The transport functions between the two storage functions are Tr13 which models the feed water system between the economizer and the boiler, Tr16 which models the feed water system between the condenser and the economizer. Tr14 models the mass (steam) transport provided by the high-pressure steam piping, the re-heaters, the turbines and the vacuum system. Tr19 is transport into the condenser of feed water and So5 is its source. The network So4-Tr17-B7-Tr18-Si6 comprises the functions of the cooling water side of the condenser. The source (So4) and the sink (Si6) are both functions of the sea water or water in a cooling tower and the balance B7 is provided by the cold side of the condenser. The transports Tr17 and Tr18 are realized by the cooling water pumps and pipes. The barrier function Barrier1 is provided by the pipes in the heat exchanger of the condenser and has the purpose of separating the possibly polluted cooling water from the feed water involved in the energy production processes.

3-1-3. The means-end relations

The plant functions modeled above in terms of mass and energy flow structures are combined into the multilevel flow model as shown in Fig. 8. Each functional level comprise a level of abstraction in the modeling of the system. The functional levels are connected to the goals by achieve and conditions also called means-end relations. The semantics of means-end relations are important for understanding MFM models as distinct from models of thermodynamic mass and energy balances.

The meanings of achieve and the condition relations can be explained by following the vertical connections in the model in Fig. 8. The energy transport function Tr6 will only be available provided that there is circulation of mass in the feed water and steam circulation circuit. It is therefore related by a condition relation with G5 which express that condition. But G5 is a goal of the functions of the water and steam circuit. G5 is accordingly related with the flow structure Structure3 describing these functions. In this way we get the condition and the achieve relations shown in Fig. 8.

The condition and achieve relations, which interrelate the levels of the model, represent knowledge about the plant which is efficient in diagnosing faults and in planning control actions [Lind88][Larsen93]. The chains of means-end relations in the model provides heuristics for searching through the system on many part whole levels. This type of search would be difficult to formulate (and implement) without a supporting plant representation like MFM. The strength of the MFM representation is that it provides a functional plant decomposition.

3-2. A Two Variable Process Control System

The MFM concepts provided for the representation of control functions (actions) will now be illustrated by an example of a two variable process control system shown in fig. 9.

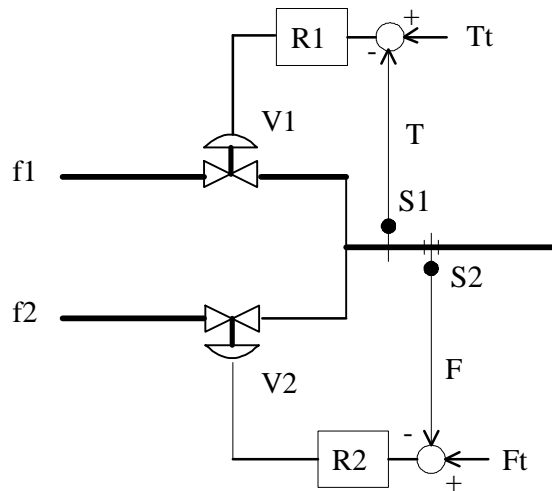


Fig. 9. A two variable process with two feedback loops

The process includes two interacting feedback loops and is mixing a cold (f_1) and a stream of hot water (f_2). The two streams can each be manipulated by means of control valves V_1 and V_2 . The temperature T of mixed water is measured by means of a thermometer S_1 and is regulated by R_1 and V_1 . The total flow of water F is measured by means of a flow meter S_2 and is regulated by R_2 and V_2 . The target value of the flow regulation is F_t and the target value of the temperature regulation is T_t .

The two control loops are designed to be coordinated by means of the causal interactions in the process and by means of the ability of the loops to maintain their targets T_t and F_t . A condition for this is that the loops are stable. If the target temperature T_t is changed, the flow of cold water f_1 will be changed accordingly by the regulator R_1 . A consequence of the change of f_1 will be that the total water flow F also changes. But as the (design) function of regulator R_2 is to equalize F with the target value F_t , the flow of hot water will be changed accordingly. This change will again lead to a disturbance of the temperature loop and thereby potentially create an endless sequence. But as we have *assumed* that the control loops are designed to be stable (otherwise the regulators would not be able to achieve their purpose) the disturbances will eventually be compensated. Reversely, if the target value F_t to the hot water flow is changed, the flow of hot water f_2 will be changed and as this causes a disturbance of the temperature T the temperature regulator R_1 will change f_1 .

3-2-1. The MFM model.

The functions of the control loops can in this example be described by their ability to produce and to maintain states in the system. The former function is a logical necessity of the latter because it is not possible to maintain a state which is not produced. Furthermore, as discussed in [Lind93], the ascription of functions to each of the two control systems will, because of the mutual relation of fitness between the systems, suggest functional ascriptions to the other system. Thus the control loop (S_1 , R_1 , V_1) can only have the (design) function of preserving the state ' $T = T_t$ ' provided the lower control loop is having the (service) function of destroying the same state.

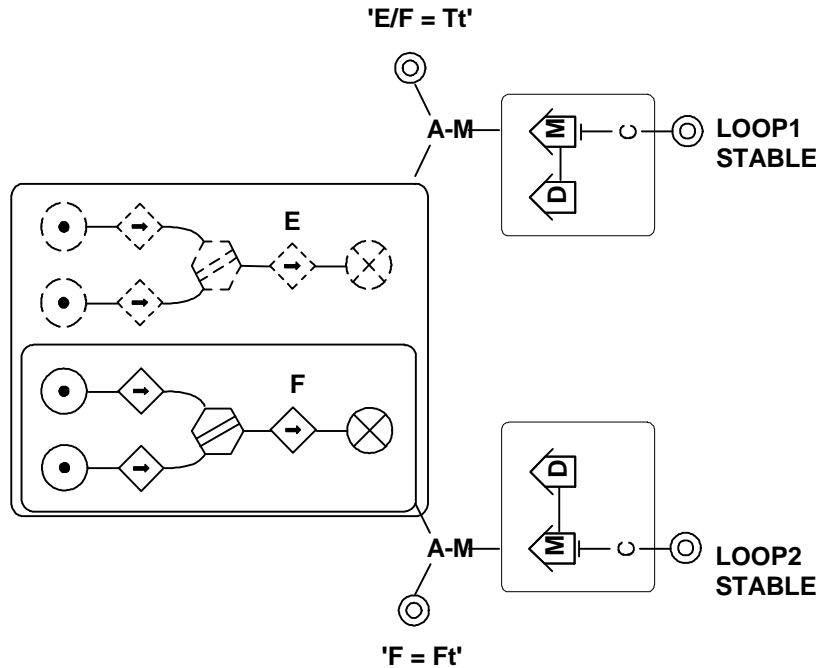


Fig. 10. MFM model of the two variable control system

The same analysis can be used for the other control loop. The functions of the control systems in the example can therefore be described by the function categories shown above and their relations can be described in the MFM model shown in fig. 10.

In the MFM model above we have described the two mass and energy flow structures involved in the mixing of the two streams of water. But in addition we have also included two other structures depicting the control functions involved for each control task. The (design) functions of the two feedback loops were to maintain the total flow F and the temperature T at their target values. But in addition, each of the feedback loops also had the (service) function of disturbing the other loop. These functions are also depicted in the model as 'destroy' functions. The example illustrates therefore how design- and service functions can be combined in a model. The control functions are combined into structures by means of connections and they are conditioned by the goal nodes representing the stability requirements. The connections have the same meaning as when used with flow functions and such structures formed by connected control functions are examples of activity flow structures.

It is realized that above we were able to explain the behavior of the system without knowing the control algorithms in R1 and R2 because we used knowledge about the purpose of the control systems i.e. the functions of (S1, R1, V1) and (S2, R2, V2). We also assumed that the loops were stable because stability is a condition for the control functions to be available. The example demonstrates that this teleology can be expressed by the MFM concepts.

4. MODEL BUILDING

The use of concepts of goals and functions create problems which are peculiar to MFM. One of the problems is to understand the nature of functional concepts, especially the sensitivity of functional descriptions to a specific goal context. The nature of the abstractions made when building MFM models are described in [Lind90a] and [Lind93].

Software tools are required to support the building of MFM models. Only small models can be developed on paper due to the need of iteration. The next sections describe briefly tools developed for this purpose at IACS.

4-1. Tools

An object oriented modeling and reasoning tool, called ABSTRACTIONS, has been developed by the author for the implementation of MFM models and for building diagnostic and planning applications based on MFM [Lind90]. ABSTRACTIONS, which is developed in Smalltalk-80, comprises a set of classes representing basic modeling concepts such as units, structures and aggregates. A set of classes used for building systems which can reason about model knowledge is also provided. MFM concepts are implemented as specializations of the basic modeling classes and diagnostic and planning systems are built as specializations of the classes provided for implementation of reasoning systems.

ABSTRACTIONS has been provided with a graphic interface for direct manipulation of model objects. This interface, called GRACE, enable a user to build models in terms of mouse based operations on icons and provides advanced facilities for navigating through the different levels of a model and for general management of screen information. The graphic interface is also used for design of man-machine interfaces for supervisory control. A comprehensive description of the facilities of GRACE is given in [Osman92].

4-1-1. Reasoning with ABSTRACTIONS

The philosophy of ABSTRACTIONS is to consider models to be the basis for building knowledge based systems. Thus, the classes support construction of plant models as complex as MFM. It is also possible to represent models of reasoning systems. In this way systems can be build which reason about models which are representations of other reasoning systems. The theoretical basis for this metalevel control aspect of ABSTRACTIONS is discussed in [Lind91a] and [Lind91b].

ABSTRACTIONS is a convenient tool for building diagnosis and planning systems for MFM because the modeling classes directly implements the basic modeling dimensions of MFM.

In a diagnostic application of MFM, the reasoning architecture can be obtained by an automated translation of the knowledge in an MFM model into a set of coordinated reasoning systems propagating values in a network of nodes and relations. The translation into a propagation system can be done dynamically [Lind91a].

The capability for diagnostic reasoning is associated with achieve and condition relations and with storage and balance functions. An achieve relation is used to generate hypotheses about a goal from a hypothesis about the flow functions in the structure below (and vice versa). A condition relation is used to generate hypotheses about a flow function from a hypothesis about the supporting goal (and vice versa). The knowledge required for these inferences is defined by rules attributed to the relations. The relations have their own internal reasoning systems. A storage function can be used as a reasoning resource because a disturbed storage level indicate disturbances upstream or downstream in the flow structure. Reasoning rules are defined as methods in the storage objects (the same is done for balance functions).

A variety of diagnostic strategies can be implemented because there are many ways to translate an MFM model into a propagation network. The strategies can be directly related to

the topology of the model. Strategies can therefore be formulated which are very difficult to express in more classical approaches to knowledge based systems such as rule based systems.

5. OVERVIEW OF PROJECTS USING MFM

The theoretical basis of MFM is under development at IACS with an emphasis on fundamental modeling issues. The research cover concepts for modeling systems and tasks, diagnosis and planning strategies for MFM, object oriented tools for model building and interface design and control systems design.. MFM has been applied in two major CEC projects within the ESPRIT I and II framework programmes. In the ESB project (Expert System Builder, ESPRIT I), MFM was used as a technique for representing knowledge about a power plant. A model of a Danish power plant was built and a prototype MFM based diagnosis system was developed using the ESB tools. In KBSSHIP (Knowledge Based Systems Onboard Ships, ESPRIT II), the technique has been further developed for the diagnosis of ship diesel engines. In this project, the focus is on the development of generic MFM models. A C++ implementation of a subset of ABSTRACTIONS has also been developed.

MFM has also been used by research groups in U.S.A., England, Norway, Sweden, Holland, Italy and Japan. In the following we will briefly describe these projects.

Work on MFM in U.S.A. has been done in the early 80'ties by Westinghouse in connection with the planning of a new control room concept for PWR. MFM was used as a basis as for a functional analysis of the PWR plant [Rumancik81][De82].

Duncan and Pratorius in England (and Denmark) made a series of interesting experiments with displays based on MFM [Duncan89]. Their results indicate that human-machine interfaces based on MFM concepts may provide efficient support for operators in diagnosis of complex events.

The Norwegian research on MFM includes an ongoing PhD project done by Walseth at the Technical University of Norway in Trondheim [Walseth92]. Walseth has developed an MFM model of a fertilizer plant i.e. a chemical engineering process. The model is used for diagnosis and is implemented in ABSTRACTIONS.

Another chemical engineering applications of MFM has been done in a PhD project by Larsson at the Technical University of Lund in Sweden [Larsson92]. Larsson has developed an MFM model of a milk sterilization plant. The model is used for diagnosis and has been developed using a MFM toolbox for the real time expert system shell G2.

Sassen from the Technical University of Delft has developed a diagnostic system for ship machinery and has done experimental evaluations of MFM for human-machine interface design. The diagnostic system is developed by using the real time expert system PERFECT [Sassen91].

The Italian research effort on MFM comprises human-machine interface studies in the mid 80'ties by Businaro and coworkers [Businaro85], and research done at CEC-JRC Ispra in cooperation with IACS. Kjær-Hansen uses MFM concepts in the development of models of decision making processes [Kjær-Hansen92].

The Japanese research on MFM comprises the development of a supervisory control system for BWR nuclear reactors done by Toshiba. The system is based on design principles for cognitive engineering and use MFM for representation of plant knowledge in diagnosis. The MFM based diagnostic function is coupled to a diagnostic module based on physics models [Monta91].

5. ACKNOWLEDGEMENT

The research reported here has been supported by CEC ESPRIT, the Danish Research Council and CEC JRC Ispra (contract: 4937-92-08-ED ISP DK). Morten Norby Larsen did the hard work in developing the MFM model of the power plant as part of his PhD project at IACS.

6. REFERENCES

- [**Achinstein83**]. Achinstein, P.. *The Nature of Explanation*. Oxford University Press. Oxford. 1983.
- [**Businaro85**]. Businaro, T., Di Lorenzo, A., Meo, G. B., Rabbani, M. I. and E. Rubino.. *An Application of MFM method for Nucl. Plant State Identification*. Enl. Halden Progr. Group Meeting on Computerized Man-Machine Communication.. Gothenborg, Sweden. 1985.
- [**De82**]. De, M.K., Rumancik, J.A., Impink, A.J. and Easter, J.R.. *A Functional Design Approach to PWR Safety*. Proc. Intern. Meeting on Therm. Nucl. Reactor Safety, Chicago, USA. 1982.
- [**deKleer84**]. deKleer, J and Brown, J.S.. *A Qualitative Physics Based on Confluences*. Artificial Intelligence, Vol 24, 1984, pp. 7-83.
- [**Duncan89**]. Duncan, K.D. and Pratorius, N.. *Flow Displays Representing Complex Plant for Diagnosis and Process Control*. Proc. 2nd. European Meeting on Cognitive Science Approaches to Process Control. Siena, Italy. 1989.
- [**Forbus81**]. Forbus, K.. *Qualitative Reasoning About Physical Systems*. Proc. Int'l Joint Conf. Artificial Intelligence (IJCAI 7), Morgan Kaufmann, San Mateo, Calif. 1981, pp. 326-330.
- [**Jørgensen93**]. Jørgensen, S. S.. *Generic MFM Models for use in Fault Diagnosis of Shipyards Machinery*. PhD thesis from Technical University of Denmark, Institute of Automatic Control Systems, 1993.
- [**Kjær-Hansen92**]. Kjær-Hansen, J. *Decision Structures of Multiagent Systems*. PhD thesis from Technical University of Denmark, Institute of Automatic Control Systems, 1992.
- [**Keunecke91**]. Keunecke, A. M.. *Device Representation - The Significance of Functional Knowledge*. IEEE Expert, pp 22-25. April, 1991.
- [**Kuipers84**]. Kuipers, B.. *Commonsense Reasoning About Causality*. Artificial Intelligence. Vol 24, 1984, pp. 169-203.
- [**Larsen93**]. Larsen, M. N.. *Modeling Start-up Tasks using Functional Models*. In: Interactive Planning for Integrated Supervision and Control of Complex Plant. Final Report Project: 4937-92-08-ED ISP DK. 1993.
- [**Larsson92**]. Larsson, J. E.. *Knowledge-Based Methods for Control Systems*. ISRN LUTFD2/TFRT--1040--SE. PhD Thesis from Lund Institute of Technology, Department of Automatic Control. 1992.
- [**Lind84**]. Lind, M.. *Decision Models and the Design of Knowledge Based Systems*. In.: Human Decision Making in Process Environments (Eds: Hollnagel, E., Manzini, G. and Woods, D.), Plenum Press, New York. 1984.
- [**Lind88**]. Lind, M.. *Diagnosis using Multilevel Flow Models*. ESPRIT project 96-Expert System Builder. 1988.
- [**Lind90a**]. Lind, M.. *Representing Goals and Functions of Complex Systems*. IACS Rept.no. 90-D-38. 1990.
- [**Lind90b**]. Lind, M.. *ABSTRACTIONS - Description of Classes and their use*. IACS 90-D-380. Tech. Univ. of Denmark. 1990.

- [Lind91a]**. Lind, M.. *ABSTRACTIONS for Modelling of Diagnostic Strategies*. Proc. IFAC Workshop on Computer Software Integrating AI/KBS Systems in Process Control. Bergen Norway. 1991.
- [Lind91b]**. Lind, M.. *On the Modelling of Diagnostic Tasks*. Proc. 3rd European Conf. on Cognitive Science Approaches to Process Control, Cardiff Wales. 1991.
- [Lind92]**. Lind, M.. *A Categorization of Models and its Application for the Analysis of Planning Knowledge*. Proc. POST ANP'92 Conference on Human Cognitive and Cooperative Activities in Advanced Technological Systems. Kyoto, Japan. 1992.
- [Lind93]**. Lind, M.. *Functional Architectures for Systems Management and Control*. In: Interactive Planning for Integrated Supervision and Control of Complex Plant. Final Report Project: 4937-92-08-ED ISP DK. 1993.
- [Monta91]**. Monta, K., Takizawa, J., Hattori, Y., Hayashi, T., Sato, N., Itoh, J., Sakuma, A. and Yoshikawa, E.. *An Intelligent Man-Machine System for BWR Nuclear Power Plants*. Proc. AI91-Frontiers in Innovative Computing for the Nuclear Industry, Jackson, Wyoming. 1991.
- [Osman92]**. Osman, A.. *Graphical Control Environment (GRACE)*. PhD thesis from IACS. 1992.
- [Rasmussen81]**. Rasmussen, J. and Lind, M.. *Coping With Complexity*. Proc. European Conference on Human Decision Making and Manual Control, Delft, Holland. 1981.
- [Rasmussen86]**. Rasmussen, J.. *Information Processing and Human-Machine Interaction*. North-Holland, New York. 1986.
- [Rumancik81]**. Rumancik, J.A. et. al.. *Establishing Goals and Functions for a Plant-Wide Disturbance Analysis and Surveillance System (DASS)*. IEEE Trans. Nuclear Science, NS-28, No.1. 1981.
- [Sassen91]**. Sassen, J. M. A., Riedijk P. C. and Jaspers, R. B. M. *Using Multilevel Flow Models for fault-diagnosis of industrial processes*. Proc. 3rd European Conference on Cognitive Science Approaches to Process Control, Cardiff. 1991.
- [Simon84]**. Simon H.. *The Sciences of the Artificial*. The MIT Press, Cambridge, 1984.
- [VonWright63]**. VonWright, G. H.. *Norm and Action - A Logical Enquiry*. Routledge & Kegan Paul, New York. 1963.
- [Walseth92]**. Walseth, J. A., Foss, B.A. et. al.. *Models for Diagnosis- Application to a Fertilizer Plant*. Proc. IFAC symp. On line Fault Detection and Supervision in the Chemical Process Industries. Delaware, USA. 1992.
- [West72]**. West, K.L. et. al.. *Minimum Recommended Protection, Interlocking and Control for Fossil Fuel Unit-Connected Steam Station*. IEEE Winter Power Group Meeting, New York. 1972.
- [Woods93]**. Woods, E. A.. *The Hybrid Phenomena Theory*. PhD Thesis from Technical University of Norway, Institute of Engineering Cybernetics, ITK rapport 1993: 72-W.