Fundamental principles of alarm design

US Tolga[1], JENSEN Niels[2], LIND Morten[3], and JORGENSEN Sten Bay[4]

1. Department of Chemical and Biochemical Engineering, Technical University of Denmark, Lyngby DK-2800, Denmark (tus@maerskoil.com)

2.Safepark Consultancy, Kannikestræde 14, DK-3550, Slangerup, Denmark (niels.jensen@safepark.dk)

3. Department of Electrical Engineering, Technical University of Denmark, , Lyngby DK-2800, Denmark(mli@elektro.dtu.dk)

4. Department of Chemical and Biochemical Engineering, Technical University of Denmark, Lyngby DK-2800, Denmark (sbj@kt.dtu.dk)

Abstract: Traditionally alarms are designed on the basis of empirical guidelines rather than on a sound scientific framework rooted in a theoretical foundation for process and control system design. This paper proposes scientific principles and a methodology for design of alarms based on a functional modeling technique (MFM) which represents a process in terms of its goals, functions and operating requirements. The reasoning capabilities of MFM enable identification of operational situations which threaten to generate an alarm and derivation of potential response scenarios. The design methodology can be applied to any engineering system which can be modeled by MFM. The methodology provides a set of alarms which can facilitate event interpretation and operator support for abnormal situation management. The proposed design methodology provides the information content of the alarms, but does not deal with alarm presentation or display design issues. A hydraulically powered grinding process is employed as an industrially relevant system to show the applicability of the proposed design methodology with promising results.

Keyword: alarm design; alarm generation; interpretation; functional modeling

1 Introduction

Process alarms are used to help operators in coping with abnormal situations by alerting and informing them in the event of critical operating plant situations. According to Abnormal Situation Management Consortium (ASM) [1], an abnormal situation is defined as 'a disturbance or series of disturbances in a process that cause plant operations to deviate from their normal operating state'. An alarm system comprises hardware and software components, which can signal an alarm state, transmit the signal to the process automation system, record the signal, and display a message about the signal to the operator [2]. Alarm systems are an integrated part of modern automation systems, which are used in facilities such as nuclear power plants, aircraft cockpits or air traffic control stations to call the operators' attention to important events [3]. When a process variable passes a limit and/or process equipment is not in a normal state, a signal is generated. This signal is commonly called an alarm. Alarm designers develop process alarm systems assuming that the operator is able to react to each alarm and correct the underlying cause. Presently alarms are generally designed based on commonly accepted guidelines. In the period when alarms were hardwired, the designers tended to design and install alarms only when they were really needed because of their high cost (approximately 1000$ per alarm) [4]. With modern control systems based on advanced ICT automation technology, it has become easy and cheap to add alarms on any process input or output. Consequently too many or irrelevant alarms are often defined without careful consideration of their importance for operation and consequences for the operators workload.

There is accordingly a need for a systematic and scientifically based methodology for alarm design. A semantically sound generic alarm definition is first proposed, and then a functional modeling based approach to the analysis of the process states from suitable available sensor signals is briefly presented. Subsequently four criteria for classification of plant situations are defined which will become the basis for a situation assessment using the reasoning capabilities of the functional models. In addition a methodology for state interpretation is presented, before the alarm design methodology is given. The modeling and alarm design methodology is illustrated on a hydro powered flour production system.

Received date: February 17, 2010
(Revised date: February 3, 2011)

2. Meanings of alarm and functional modeling

2.1 Definition of alarm

There are many types of definitions of alarm in the literature. Here an alarm is defined based upon the following recognition: *"An alarm is a signal signifying to an operator that an abnormal state has occurred"*.

The signal has double significations:

1) it alerts the operator, arise attention, warn and give notice , and
2) it indicates danger, malfunction, error condition, process deviation, and unexpected event

The first signification is on the perceptual level whereas the second signification is based on the operators' expectations, experience (*i.e.* norms) or knowledge, and so it is on cognitive level. On this basis a new definition of alarm is proposed as: *"Alarm is a signal which signifies to the operator that an abnormal state needs a response."*

Here the term 'response' is used to define a required reaction. The expression 'abnormal state' comprises process deviation, error condition, malfunction, and neared or overrun limits. The expression 'abnormal state' must be interpreted in terms of functional concepts. For this purpose the following definition is applied for 'abnormal state' as *"An abnormal state is a state which threatens or prevents the accomplishment of a goal."*

Thus a generic definition of alarm becomes: *"An alarm is a signal which signifies to the operator that a response requiring state threatens or prevents the accomplishment of a goal."*

2.2 From abnormal states to functional modeling

The word 'normal' has its roots in the concepts of a 'norm'. An abnormal situation is accordingly a situation which does not comply with a norm. Norms are expressed by criteria for what is good, acceptable, desirable or required. They can be derived from specifications of how things ought to be, i.e. from an intention or purpose. However, norms can also be defined by referring to an experienced situation representing how things usually are when they are acceptable or considered good. In a process life cycle perspective these two ways of defining norms are connected because a best practice can be transformed into requirements and norms. Norms, requirements and purposes for action can be represented by 'functional modeling' [5], which provide concepts for formalized representation of purposes, goals and functions of physical designs. Functional concepts are for the same reasons closely connected to concepts of failure. It is therefore obvious that functional modeling can play a central role for development of a scientific basis for alarm design. Previous approaches to alarm design have also emphasized the importance of functional concepts [6,7], however without suggesting the scientific approach as presented in this paper.

Larsson [8], Fang and Lind [9] and Gofuku and Tanaka [10,11] have used a functional modeling method called Multilevel Flow Modeling (MFM) [12] for fault diagnosis and counteraction planning. Those works developed principles for reasoning on system failures but did neither explicitly consider the problem of alarm design nor classified development stages of a safety critical situation.

3. Design principles and methodology

3.1 Semiotics on alarm design and Multilevel Flow Modeling

The design principle of alarms can be built on basic principles of sign interpretation from the field of semiotics and on a functional modeling method MFM. Semiotics studies deal with 'signs' and their interpretation of any subject from all aspects. In the present context the branch of semiotics, which originally deals with the interpretation of signs by biological organisms, is of particular interest. Morris [13] developed a theory of sign interpretation which explains how the meaning of signals received by an organism interacting with an environment depends on the phase of the 'action'. This theory can be applied to alarm interpretation and has been adopted for this purpose in combination with functional modeling to design of human machine interfaces and to intelligent control [12, 14].

MFM is a modeling methodology which has been developed to support functional modeling of process plants involving the interactions of materials, energy

and information flows [6,7]. Functions are here represented by elementary flow functions interconnected to form 'flow structures' representing a particular 'goal' oriented perspective of the system. MFM is founded on fundamental concepts of action [15] and each of the elementary flow functions can thus be seen as 'instances' of more generic action types [6]. The perspectives represented by the flow structures are related by 'means-end relations' and comprise together a comprehensive model of the functional organization of the system. The basic modeling concepts of MFM include objectives, flow structures, as set of 'functional primitives' (the flow functions with causal roles) and a set of means-end relations representing purpose related dependencies between flow structures. The functions, the flow structures and the 'relations' are interconnected to form a hyper-graph like structure.

3.2 Example: an overshot water mill

An overshot water mill shown in Fig. 1 is used as an example of process system to illustrate the principles and the methodology for alarm design. A water mill uses a water wheel to drive a mechanical process for flour or lumber production. The water used by the mill is diverted from a river along a channel known as the flume. A sluice gate on the flume is used to control the amount of water flowing into the mill. The wheel is rotated by the falling water striking and filling the buckets of the wheel, making it heavier than the other empty side. The weight turns the wheel which in turn rotates the drive shaft with a toothed wheel. By means of the horizontal toothed wheel, the angle of rotation changes which in turn rotates the spindle and drives a runner stone. The runner stone is the upper part of the millstones which spins above the stationary bed stone creating the grinding action. The runner stone has a hole near the centre into which the grain is fed. The grain is ground between these two stones, moves through to the outer edge and passes as flour through the casing. By means of the grinding action, the shells and the flour are separated. Two intervention possibilities are assumed to be available to the miller in this kind of system: (i) changing the water flow rate to the water wheel by means of the sluice rate, and (ii) manipulating the feed rate of the grain to the runner stone.

3.3 MFM model of a water mill

The process alarm design is based on the MFM model of the water mill as shown in Fig. 2. The main skeleton of an MFM model is its *"objective tree"*. Figure 3 shows the objective tree of the example MFM model. The flow structure S3 as shown both in Figs. 2 and 3 represents the functions involved in supplying water to the water wheel, where the water is transported through the sluice (represented by tr7) into the buckets (represented as a sink si4).

When the water flow is achieved then O3 is fulfilled and the water wheel is moving. Thus (following the "producer-product relation" connecting S3 with so2) the energy in the water is converted to rotational energy represented by the flow functions so2, tr4 and si3. Furthermore, when O2 is achieved rotational energy is available for the grinding, which is represented by the flow function bl1 in the grain structure S1. The supply of grain is represented by source so1 and the transport tr1 and the flour produced is transported to the consumer (si2).

The fulfillment of main objective (O1) depends on the fulfillment of all other objectives. The objective O3 is independent while O2 depends on O3. The objective tree as shown schematically in Fig. 4 is a hierarchy. In general however it may be a heterarchy with multiple top goals and sub-goals.

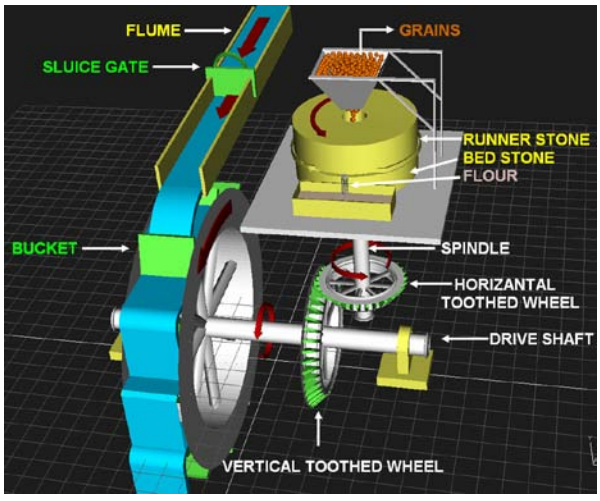


Fig. 1 The overshot water mill.

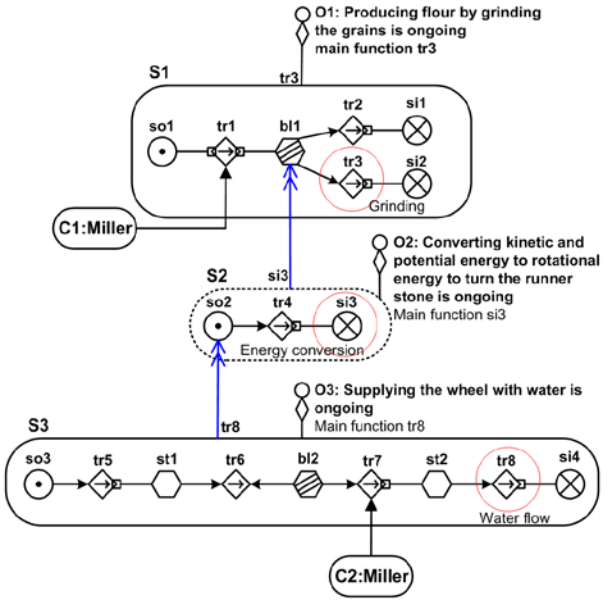


Fig. 2 A simple MFM model for the overshot water mill.

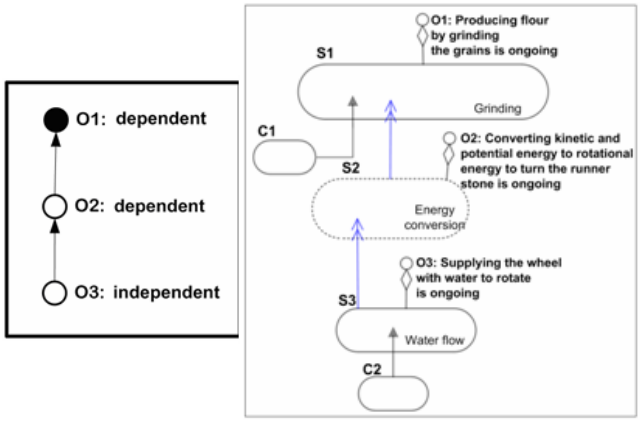


Fig.3 The objective tree for the water mill.

3.4 Flow function circumstances

To enable reasoning for state assessment it is suitable to define four 'condition types' related to the flow functions. The first two are originally proposed by Paasen and Wieringa [16] and Petersen [12], and they are the enabling and establishing circumstances which relate to normal operation. The other two are related to abnormal operation**:** abnormal and failed circumstances.

3.4.1 Enabling circumstances

Enabling circumstances enable flow functions in the flow structures. A flow function is enabled when it has the full potential to contribute to the achievement of its corresponding objective. When a flow function is enabled, it is however not yet interacting with its adjacent flow functions. Consequently, the flow functions in the corresponding flow structures are not yet integrated to be able to achieve their corresponding objectives. Figure 4 demonstrates the enabled functions in the corresponding flow structures. Certain system circumstances must be present for each flow function to be enabled. The set of circumstances which enables the flow functions are labeled as N^n_{xy} for x = flow function type (source: so, sink: si, transport: tr, barrier: ba, storage: st, balance: bl), y = function number (1, 2, 3...) and n = condition number (1, 2, 3…).

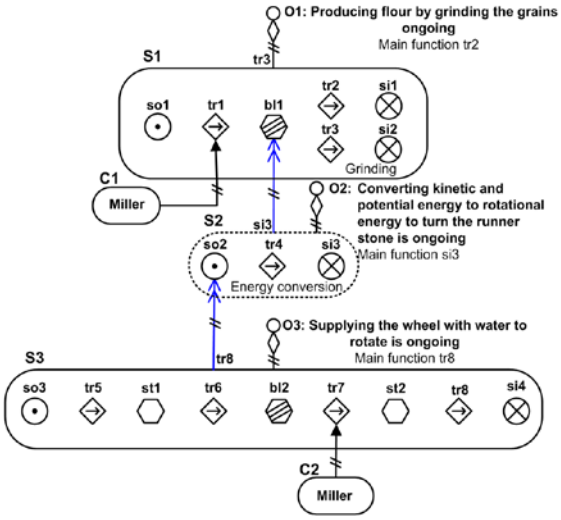


Fig. 4 MFM model of water mill with flow functions enabled

3.4.2 Establishing circumstances

A flow function is established when its state supports and ensures the achievement of its corresponding objective [16]. When a flow function is established, it is interacting with its adjacent flow functions. Accordingly, a flow structure is established when its flow functions are connected. As can be seen from Fig. 5, in this state, the flow functions are connected, and the MFM relations and the objectives are fulfilled. The set of circumstances which establish the flow functions is labeled as S^n_{xy} in analogy with the enabling circumstances. When flow functions are established, they are interacting and dependent of their adjacent functions and MFM relations.

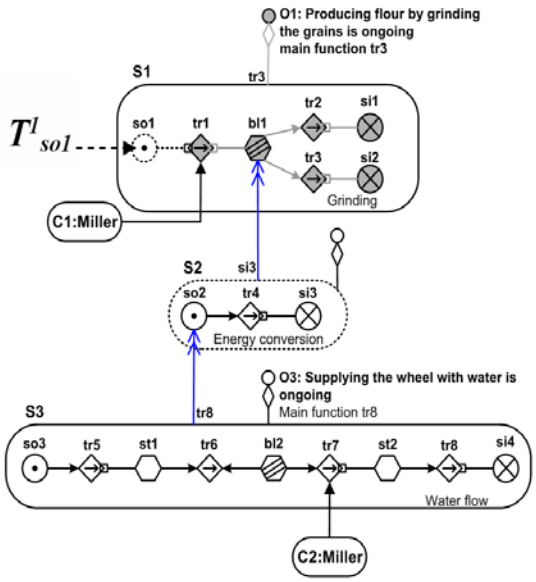


Fig. 5 MFM model of water mill with flow functions enabled and established. Additionally a specific threat is also shown with flow functions in gray.

3.4.3 Disturbing circumstances

A flow function is disturbed when its state may threaten the achievement of its corresponding objective. When a flow function is disturbed, it has the potential to disturb its adjacent flow functions. Accordingly, it can disturb the integration of the flow functions in the flow structure. This will threaten the achievement of the corresponding objective. Such disturbing system circumstances are called '*threats*'. The set of abnormal system circumstances which disturbs the flow functions are labeled as T^n_{xy}. For example T^1_{so1} represents one of the disturbing circumstances in the set of circumstances which *disturb* the source function so1. In Fig. 5, the effect of a disturbing condition on the source function so1 (T^1_{so1}) in the flow structure S1 is illustrated. When T^1_{so1} occurs, it disturbs the source function so1 and its relation to the adjacent flow function tr1 (dotted lines). When so1 is disturbed, it has the potential to disturb its adjacent flow functions tr1, bl1, tr2, si1, tr3, si2 and their MFM relations (both grey). If the integration of the flow functions is disturbed, the state of so1 will threaten the achievement of its corresponding objective O1 (shown in grey). A threat occurs when a flow function is threatened to be brought outside of the intentional operation limits. For every T^n_{xy}, the corresponding threat type must be identified. A given threat T^1_{so1} can cause the source function so1 to be outside its state constraint. Rossig, *et al.*, presents a methodology for identification of threats in HAZOP studies [17, 18].

3.4.4 Disabling circumstances

A flow function is disabled when its state immediately threatens and may prevent the achievement of its corresponding objective. When a flow function is disabled, it disturbs its adjacent flow functions, relations and the integration of flow functions. Consequently, it immediately threatens the achievement of the corresponding objective. Moreover, it has also the potential to disable its adjacent flow functions and relations. Accordingly, if it starts to disable its adjacent flow functions, it will also disable the integration of the flow functions in the corresponding flow structure. This will prevent the achievement of the corresponding objective. Such disabling circumstances are called 'failures'. The set of abnormal system circumstances which disables the flow functions as F^n_{xy} in the MFM model as shown in Fig.6, where F^1_{so2}, represents one of the disabling circumstances (for so2) in the set of circumstances which *disable* the source function so2. When F^1_{so2} occurs, it will disable so2 and its relation to the adjacent flow function tr4. This is shown by the double lines '//' on so2 in Fig. 6. When so2 is disabled, it immediately disturbs and **may** disable all the adjacent functions and MFM relations in S2.

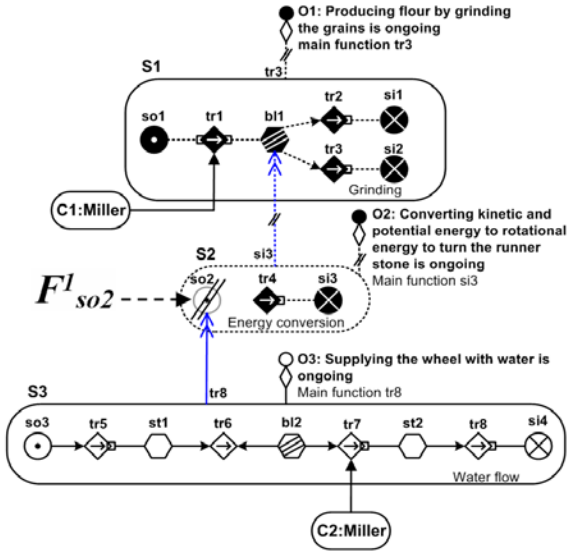


Fig. 6 MFM model of water mill showing the effect of F^1_{so2} on the enabled and established MFM model. The flow functions which are disturbed by the failure are painted black.

The flow functions disturbed by F_{so2} are painted black and the disturbed MFM relations are shown by dotted lines. Since the integration of the flow functions in S2 is disturbed, F_{so2} immediately threatens the achievement of the corresponding objective O2. Since O2 is threatened and si3 influences bl1 (through a producer-product relation), it will disturb the integration of the flow functions in S1 which will also threaten the achievement of O1. In Fig. 6, the threatened and potentially prevented objectives and all the disturbed and potentially disabled flow functions are painted black. The disturbed and potentially disabled MFM relations are shown by dotted lines. The impact of F^n_{xy} on a flow function depends on the type of the flow function and the nature of the disabling condition.

3.5 Signals and their interpretations

When abnormal states occur, they can threaten or prevent the accomplishment of the system goal. Thus, an agent must perceive and interpret these abnormal circumstances to recommend intervention. The supervisory control agent assesses the state of the system caused by events in order to produce or maintain the state of affairs according to the available system information, goals and possible courses of action[14]. In Fig.7, the signal generation by an event, the perception of these signals by the agent, the interpretation process and the possible intervention are illustrated.

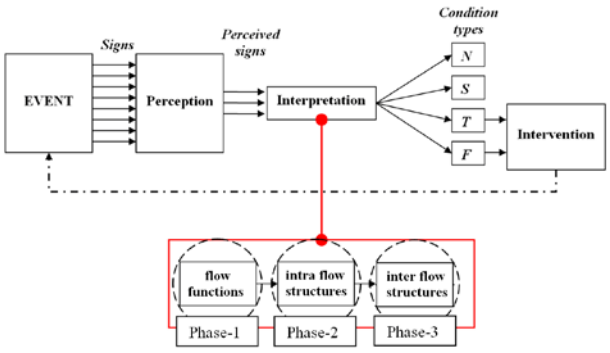


Fig.7 Interpretation of event signals and consequential intervention.

In the principles of alarm design, the interpretation consists of three consecutive phases. The agent perceives signals from the system and the environment. The perceived signals are classified into four types of circumstances (*N*-enabling, *S*-establishing, *T*-disturbing, *F*-disabling) for each flow function in the MFM model. This is the first phase of interpretation shown in Fig.7. In the second phase of interpretation, the state of the main function of each objective is investigated. The main functions are the *focal points* for the interpretation of abnormal states within the flow structures in Phase-2. For example, in the water mill MFM model (Fig.3), the main functions are (in red circles) tr3, si3 and tr8.

In Phase-2, the success of the interpretation process is directly dependent on the agent's reasoning ability, capacity and knowledge about the system. In complex systems, the agent may have many events to perceive and interpret. Thus automatic reasoning support is essential when the control agent is a human operator.

After the state of each objective in a given MFM model is known, the third interpretation phase is completed with respect to the main goal in the MFM model. In this phase, the state of the goal (the main objective e.g. O1 in Fig.2) is investigated by its corresponding main function. The potential inter flow structure propagations can be derived by reasoning about the means-end relations in the model (*e.g.* condition and producer-product relations).

4 Alarm Design

An alarm *"signifies a response requiring state which threatens or prevents the accomplishment of a goal of a purposeful system"*. Thus the circumstances confirmed during interpretation as corresponding to objective 'will be under threat', 'is under threat', 'will fail' or 'is failed' are considered as *alarms*, as listed in Table 1.

Table 1: Notation for alarm types related to goal O*i* (*i* = 1, 2, 3…).

Objective	Interpretation	Alarm
O*i*	O*i* will be under threat	$\widetilde{T}_i$
	O*i* is under threat	T_i
	O*i* will fail	$\widetilde{F}_i$
	O*i* is failed	F_i

In modern control system alarms are generally classified in categories such as message or warning, alarm and emergency, depending on the time available for operator intervention before automatic action takes

over. The categories “will be under threat” and “under threat” used in Table 1 corresponds to ‘alarm’, while the categories “will fail” and “failed” corresponds to ‘emergency’.

The full propagation potential (from so3 in S3 to st1 in S1) of T_{so3}*:lovol* is shown in Fig.8. As seen in the potential propagation path in Fig.8, there are three intervention possibilities labeled as C3, C2 and C1 which mediates si3, so2 and tr1, respectively.

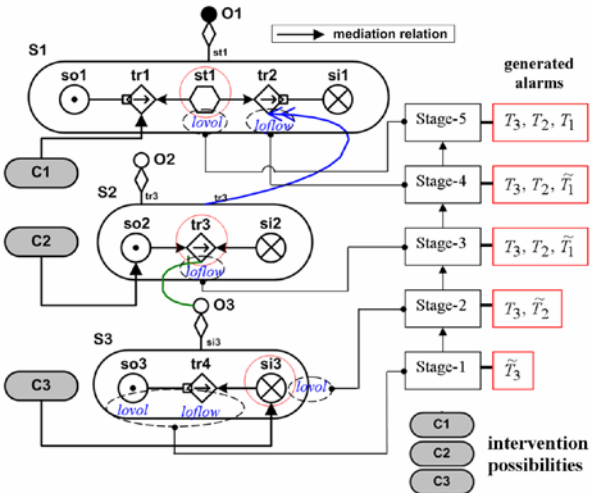


Fig.8 Propagation of an abnormal condition T_{so3}*: lovol* with three intervention possibilities. Alarm types are shown on the right hand side while intervention possibilities C1, C2 and C3.

The above methodology leads to a procedure and set of rules for reasoning based alarm generation and suggested intervention generation. On this basis the systematic alarm design procedure will be summarized as below:

(1) Develop a Multilevel Flow Modeling (MFM) of the given process including explanation of objectives, causal relations and, description of flow functions,
(2) Identify the objective tree (heterarchy) from the MFM model,
(3) Identify enabling-*N* and establishing-*S* circumstances for each MFM flow function and structure,
(4) Identify disturbing-*T* and disabling-*F* circumstances for each MFM flow function and structure,
(5) Identify the main function for each objective concerning the means-end relations,
(6) Identify possible intervention possibilities together with their descriptions,
(7) Identify fixed alarm contents for every objective,
(8) Identify the criticality of the given system, through consequence propagation in dependence of the prediction horizon, and
(9) Apply the procedures and rules for alarm generation following the alarm design principles.

Throughout this paper the water mill has been used as illustrative example. By using the methods presented above the alarms for every objective also has been identified. These alarms contain the information contents for any alarm generated during the interpretation process. The results are most reasonable. The state of the flow functions in the model is easily identified. These alarm design principles also have been investigated on a more realistic industrially inspired example, *i.e.* an industrial heat pump on a distillation column. The investigation also in this case produced most promising results.

5. Discussion and Conclusion

The principles and methodology given in this paper enable an engineer to approach a systematic alarm design upon a scientific basis. The alarm design methodology proposed in this paper can be applied to any engineering system which can be consistently modeled by MFM. The most crucial aspect of the methodology is the interpretation procedure which is performed by the alarm system to support an operator. This interpretation exploits the reasoning capabilities of the MFM models. Several rules can be applied to predict the propagation of disturbing circumstances on a given path by using causal relations [12]. By the reasoning system the propagation of abnormal circumstances can be qualitatively predicted and classified by the proposed alarm design. Moreover, to deal with branching propagation paths, additional rules can be designed for the interpretation process. This alarm design methodology can form an improved basis for diagnosis and counteraction planning [8-10,12].

Changing the alarm sensitivity in an abnormal situation can be used for ‘alarm suppression’. When many alarms are presented to the operator, the alarm sensitivity can be decreased to reveal the overall situation in the plant. That will eventually decrease the number of alarms. In addition, by increasing the alarm

sensitivity, an operator can obtain an idea of how far the present abnormal situation can propagate.

While developing the alarm design principles, it was assumed that the state of each flow function could be identified. The larger the number of flow function states which can be identified, the more reliable the interpretation becomes. As illustrated in both cases and especially in the heat pump case, in engineering systems it is not economically practical to measure the state of each flow function.

On the other hand, the qualitative reasoning capabilities of MFM will reduce the need for measuring the state of all flow functions. However qualitative reasoning will have a limitation that the alarms are more uncertain when measurements are located far (in terms of propagation path) from the root cause. For highly safety critical cases quantitative mathematical models may be combined with MFM to predict the states of observable critical flow functions, when necessary.

The MFM modeling enables a qualitative representation of a system on several levels of means-end abstraction. When large industrial systems such as oil refineries and power plants are considered, a network of objectives for these systems can be developed. Thereafter MFM models can be developed for each objective in the network. Next, specific alarms can be designed for each objective. By this method, the proposed alarm design principles can be used systematically at different abstraction levels. This will enable the operators to cope efficiently with critical abnormal situations affecting the overall operation of large industrial plants or system networks.

References

[1] ABNORMAL SITUATION MANAGEMENT CONSORTIUM: A Joint Research and Development Consortium ,2008, URL: www.asmconsortium.com

[2] DUNN, D.G., and SANDS, N.P.: ISA-SP18–Alarm System Management and Design Guide, Presented at ISA EXPO 2005, McCormick Place Lakeside Center, Chicago, Illinois, October 25-27, 2005.

[3] ENDSLEY, M.R., BOLTE, B., and JONES, D.G.: Designing for Situation Awareness – An Approach to User-Centered Design, Taylor & Francis, New York, 2003, 149-150

[4] KATZEL, J.: Managing Alarms, Control Engineering, Vol. 54(2), 2007, 50-54

[5] LIND, M.: Diagnosis using Multilevel Flow Models - Diagnostic Strategies for the P96 demonstrator. Tech. Report, ESPRIT project P96, Technical Report, 1988

[6] LIND, M.: Modeling Goals and Functions of Complex Industrial Plant, Applied Artificial Intelligence, 8(2) 1994, 259-283

[7] LIND, M.: The Why, What and How of Functional Modeling, Proc. of ISSNP 2007, Tsuruga Japan, July 2007

[8] LARSSON, J. E.: Diagnostic reasoning strategies for means-end models. Automatica, 30(5), 1994, 775-787

[9] FANG, M, and LIND, M.: Model based reasoning using MFM. Proc. Pacific-Asian Conference on Expert Systems (PACES), Huangshan, China, 1995

[10] GOFUKU, A., and TANAKA, Y.: Application of derivation technique of Possible Counter Actions to an Oil Refinery Plant, Proc. 4´th IJCAI Workshop on Engineering Problems for Qualitative Reasoning, 77-83, Stockholm, 1999

[11] GOFUKU, A. and TANADA, Y.: Display of diagnostic information based on display intention. Proceedings of Symposium on Analysis, Design & Evaluation of Human-Machine Systems (HMS 2001) 9. 385-9, 2001

[12] PETERSEN, J.: Knowledge Based Support for Situation Assessment in Human Supervisory Control, PhD thesis, Department of Automation, Technical University of Denmark, 2000.

[13] MORRIS, C.: Signification and Significance, The MIT Press, Cambridge Massachussets, USA, 1964.

[14] LIND, M.: Semiotics and Intelligent Control, Proceedings IFIP WG8.1 Working Conference Organizational Semiotics: Evolving a science of information systems. Montreal, Canada. July 24-26, 2001

[15] VON WRIGHT, G. H.: Norm and Action, Routledge & Kegan Paul, London, 1963

[16] PAASSEN, M.M., and WIERINGA, P.P.: Describing Process Mode Changes with Multilevel Flow Models, Proceedings of the Fifth International Workshop on Functional Modeling of Complex Technical Systems, ISBN 0-9652669-5-8, 27-39, Paris-Troyes, France, 1997

[17] ROSSING, N.L., LIND, M., JENSEN, N., and JORGENSEN, S.B.: A goal based methodology for HAZOP analysis, IJNS Vol.1, No.2, 2010

[18] ROSSING, N.L., LIND, M., JENSEN, N., and JORGENSEN, S.B.: A functional HAZOP methodology, Comp.Chem.Eng. Vol. 34, 244-253, 2010