

A Pilot Project on Alarm Reduction and Presentation Based on Multilevel Flow Models

Jan Tuszynski (*), Jan Eric Larsson, Christer Nihlwing (**), Bengt Öhman, Antonio Calzada

(* *GoalArt, Lund Sweden; (**) IFE Halden Norway*

(* *Phone: +46 46 192634, Fax: +46 46 192641, E-mail: jan@goalart.com;*

(** *+47 69 212258, Fax: +47 69 212460, E-mail: cni@hrp.no*

Abstract

Three Swedish Nuclear Power Plants, IFE Halden and GoalArt are committed to evaluate alarm reduction methods based on Multilevel Flow Modelling. The MFM-methods promise sought-after intelligence for instrumentation and control systems. Operators and maintenance can be assisted in handling faulty situations of nuclear plants by clear indication of consequential chains of events. The algorithms proposed extract automatically all required information from the central plant knowledge base. This base is given in form of MFM-model, which is graphical form of goals and functions of technical systems. MFM provides a good basis for computer-based supervision and diagnosis, especially in real-time applications, where fast execution and guaranteed worst-case response times are essential. The Pilot Project will evaluate GoalArt's claims that the explicit MFM representation of means-end knowledge and the graphical nature of the models make the knowledge engineering available for plant process engineers. An important part of the project is committed to find best ways of alarm presentation using the new information now available.

1. INTRODUCTION

The problem with alarms is well known in the nuclear industry. US Nuclear Regulatory Guides gave already in 70's clear requirements on alarm reduction, identification of primary alarms, and special treatment of alarms of high priority. The requirements were right but available control technology could not meet them. Technology improved but alarm problems showed up to be more persistent than expected. Periods of different approaches to logic were followed by a panacea of AI-technology with various inference engines, trees, networks and rule handlers. The main problem is still here – research community could not provide generic diagnostic methods suitable for industrial, commercially viable control system implementation. The suppliers of I&C systems addressed basics allowing generation of alarms, but most often lacked generic approaches for sorting and reduction of those alarms. The results are well known, operators are constantly bothered with stray alarms or overloaded with thousands of nearly simultaneous alarms during plant transients. That situation is improving. The I&C branch is well aware now of feasible requirements (e.g. [2]), and research of 80-ies and 90-ies showed up to be not completely empty handed.

This paper shortly reviews basic approaches on alarm handling, and points out the Human Machine Interface (HMI) as a main steering factor for alarm system development. The main purpose of this paper is to report on the Pilot Project run presently in cooperation between Swedish Nuclear Plants (OKG, Ringhals AB and Barsebäck Kraft AB), IFE Halden and GoalArt. The purpose of the project is to prove the suitability of GoalArt's alarm handling for the control room modernisation of nuclear power plants. We introduce the basic concept of Multilevel Flow Models (MFM, ref. [8]) and MFM-based diagnostics. The MFM concepts build on the idea that a knowledge

This is a *preprint* of an article, which was published in the proceedings of the Enlarged Halden Programme Group Meeting, HPR-358, Storefjell, Gol, Norway, 2002, and it is made available as an electronic reprint by permission of IFE Halden and the power plants participating in the project described in the article.

base can be built in MFM graphs, easily extracted from the existing plant documentation. No complex rule bases are needed, as all necessary information (logic) will be handled automatically. The MFM based methods have been developed under the period starting at the end of 1980-ies (M. Lind, [8]), and can be studied today through numerous references ([1], [3], [5], [6], [7] and [10]).

2. BASIC APPROACH ON ALARM HANDLING

2.1 Basic requirements on the system

The main prerogative of all plant diagnostics, including alarm handling, is to serve operators and maintenance with structured information. The structuring means here that the information should be configurable, answering particular enquiries from operators. This requirement on configurability is actually a well-known database problem where every database item should get a property mark allowing data extraction on the particular query. Basic functions required of the event handling system will be accordingly,

- a. to identify the occurring event and set it into the event database
- b. to stamp the event with a time mark
- c. to filter the event
- d. to stamp the event with a property mark
- e. to allow HMI querying of filtered, time and property marked events
- f. to present human operators with event information

Note that we deal here with event databases, as an alarm is only an event of a particular grade of importance. The events will be normally handled in two systems,

- System of interconnected process control stations acquiring process data and handling event databases; i.e. providing functions a) to e)
- HMI system presenting events sorted according to property and time marks to the operators; i.e. functions e) and f)

The I&C systems of today handle functions a), b) and c) in a generally satisfactory way. The main issues of the Pilot Project are to prove the correct and satisfactory event property marking (d), and to find the best way to present events/alarms sorted according to that marking (f).

The natural “meeting point” of all functions will be the event database, as shown in Figure 1.

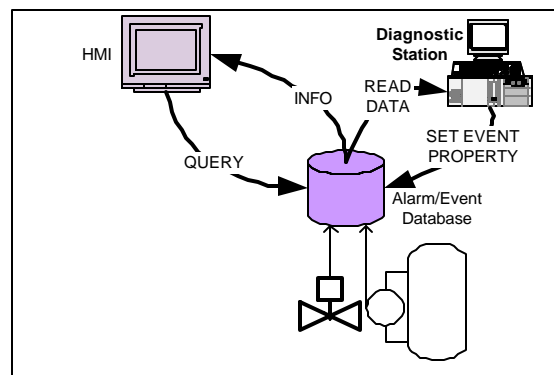


Figure 1 Main components of the alarm handling system

2.2 Properties of events

The kind of event properties, which we are concentrating on in the Pilot Project are the following,

- Primary / secondary alarm
- Consistent / non-consistent alarm
- Relation / membership of the same event group
- End-mark of the event group
- Alarm priority

A primary alarm indicates an initiating event while secondary alarms are those initiated. A primary alarm with its tail of secondary alarms creates a related group (burst) of events. The end-mark will indicate end of that tail. Consistency between event indications may be used to detect sensor faults. The main alarm problem can now be reduced to the question; how to find those properties? We can recognise two basic approaches, through decentralised and centralised handling.

2.3 Decentralised approach

A decentralised approach can be summarised as a system where each process component or sub-system takes care of its own supervision. The plants are normally built in three hierarchical levels; objects (pumps, valves), functional groups (logic controlling groups of pumps and valves) and plant blocks (coordination of functional groups).

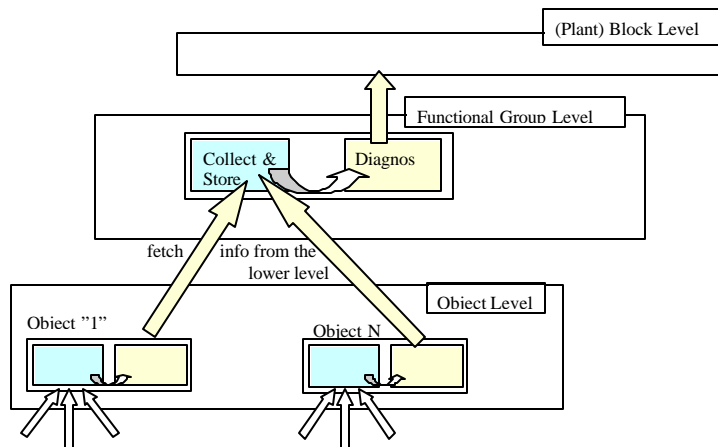


Figure 2 Main principle of decentralised alarm supervision

Each element will be complemented with supervisory logic evaluating pre-defined internal failures as well as failures of the lower level it depends on (Figure 2). Modern I&C systems will allow nearly automatic interconnection of the supervised objects, and it works well on the basic object levels, where each object can be controlled by reusable type-circuits. The problems of building parallel trees of interdependent logic, as well as complex algorithms for searching those trees are practically non-existent. The following problems are anyhow still there,

- Interdependence of low-level objects can be defined on functional group level only. The logic indicating interdependence will often be plant dependent, and accordingly special
- Plant-wide interdependence is still more complex than on the functional group level, and accordingly still more specialised

Building plant dependent logic is generally troublesome, as the supplier will lack the plant information in this degree of detail. The normal result is that high-level logic is left over as a post-commissioning pending action, and operators will only rely on the low-level alarm logic. Additional problems will arise in case the process systems get changed and there is practically no party available to change the logic accordingly.

2.4 Centralised approach

In this approach the plant knowledge is implemented centrally allowing property recognition of all supervised plant and control system events. The centralised knowledge base of the size and complexity of the nuclear power plant may seem scary. The approach may be accepted only if the following criteria are fulfilled:

- Detailed rule-based approach is avoided
- The knowledge base should refer to knowledge of plant processes, and not to technicalities of property extracting algorithms
- The knowledge base should be in form of the plant model
- The graphical representation of the model is preferred
- The model should be structured, corresponding to systems, sub-systems and particular redundancies of the plant
- There should be an easy way to transform existing plant information (normally equipment based) into the model proposed (normally function-oriented)¹
- The model should allow real-time execution of implemented algorithms, automatically generating all sought-after event properties
- The model execution should have excellent real-time properties to handle huge size plant event database.

The above criteria, as compiled by the participants of the Pilot Project, will be used to evaluate the MFM-based methods of alarm reduction and presentation.

3. ALARM ASPECTS IN HMI

3.1 General

The alarm system should serve operators and maintenance with structured information. This simple statement means that the operator should be able to extract only information required for the particular state of the plant operation. In case of a plant transient, the operator will probably get an alarm shower of up to several hundred alarms, and has no time to study the alarm list. The information to be extracted mainly concerns the following:

- What has initiated the transient?
- Which part of the plant is still available?
- Are there high priority alarms, which must be dealt with immediately?

The situation will be still more complicated if the plant gets into unstable conditions. The initiating condition temporarily disappears, and the initiating alarm burst will periodically be replaced by other bursts, not apparently connected to each other. The plant protection system will further complicate the alarm situation especially if faulty sensors initiated it. All those scenarios show that alarm situations have their own dynamics, which must be recognised and addressed accordingly.

¹ Compare with KKS Identification System, levels for functions and equipment

The first action of the operators is normally to find exactly what has happened and what part of the plant is available. If that process would take too long time, the safety responsible operator team leader will decide to take the plant over to a fail-safe state of operation; through reduction of the MW-load, load rejection or through emergency stop of the plant. An unnecessary stop of the plant means lost revenues, especially for emergency stop requiring at least 24-hours to start again.

The primary task of the improved alarm handler will be to provide direct answers for the three queries listed above. The answers should be presented in a clear graphical or verbal formulation, allowing operators to take the right decisions in an orderly way, in an early stage of the event development. The presentation should address the dynamic aspects of the alarm showers mentioned above.

3.2 HMI features to be tested

The following means of HMI addressing alarms will be tested in the Pilot Project:

- Split alarm list
- List of residual / existing alarms
- Tiles
- Sounds, flashing and acknowledgement
- Alarm icons in process display
- Background Information Displays
- Alarm navigation tools / Information menus

The main assumption of the Pilot Project is that HMI features developed in the earlier IFE Halden projects should be tested in the first place, mainly in HAMBO, according to references [4] and [11]. Further sources of possible features to be used in the project are the actual modernisation projects at OKG and Ringhals. Detailed information on the HMI for alarm presentation is available there², here follows only overview of those features.

Split alarm list: The split alarm list is shown in Figure 3. The top window will display primary alarms, while the lower one will display secondary. It is possible to add a third explanatory window displaying the chain of events leading to the particular alarm, allowing comprehension on how the particular alarm has become primary or secondary. The explanatory window may display a part of the MFM-model for that purpose.

MM/DD HH:MM:SS	SVT Content	Name
11/15 10:02:47	ALM 463 Soolingsalarm	T463Ce
11/15 10:02:40	ALM 462 Soolingsalarm	T462Ce
11/15 10:02:40	ALM 463 Soolingsalarm	T463Ce
11/15 10:02:42	ALM 463 Mavn. temp. efter FV4, strålk 1	T463K513e
11/15 10:02:46	ALM 463 Mavn. temp. efter FV4, strålk 2	T463K514e
11/15 10:02:47	ALM 462 Kond. temp. fore FV3, strålk 1	T462K535e
11/15 10:02:47	ALM 462 Kond. temp. efter FV2, strålk 2	T462K542e
11/15 10:02:49	ALM 462 Kond. temp. fore FV2, strålk 2	T462K536e
11/15 10:02:49	ALM 462 Kond. temp. efter FV2, strålk 1	T462K541e
11/15 10:02:50	ALM 462 Kond. temp. efter FV3, strålk 1	T462K551e
11/15 10:02:50	ALM 462 Kond. temp. fore FV3, strålk 1	T462K544e
11/15 10:02:51	ALM 462 Kond. temp. fore FV3, strålk 1	T462K543e
11/15 10:02:51	ALM 462 Kond. temp. efter FV3, strålk 2	T462K552e
11/15 10:02:52	ALM 463 Mavn. temp. efter FV5, strålk 1	T463K523e
11/15 10:02:52	ALM 463 Mavn. temp. efter FV5, strålk 2	T463K524e

Figure 3
Split list of primary and secondary alarms

² C

Process dynamics will result in a situation where an initially recognised primary alarm will be moved down into the secondary alarm list. This sorting process will be concluded on the reception of the end-mark for the last secondary alarm received. Please note that the feature allowing recognition of the consequential dependence between alarms makes exact time marking less important. In case of multiple primary alarms, it will be required that secondary alarms will display to which event chain they belong.

List of residual/existing alarms: It will be tested if the list of existing alarms can be reduced to primary alarms only. This means that as soon as the alarm is recognised as secondary, it will be removed from the list without acknowledgement. Alarm priority may be recognised through marking in different colours.

Tiles: The alarm display of control rooms are normally in specialised VDU's, arranged in a matrix of alarm display regions. Each region consists of dedicated (static) or assigned (shared) alarm tiles emulating the fixed alarm tiles of a conventional alarm annunciation system. Each tile will consist of fixed lines of text with features added to handle alarm property marks. The following is presently considered:

- Tiles of the primary alarms will be handled as high-priority alarms while secondary alarms will be suppressed
- The tile of a primary alarm should be able to display an explanatory chain of events and show the whole chain of the coupled burst of secondary alarms. Here the COPMA feature can be used for alarms generated both in HAMBO and ALLADIN (IFE Halden ref. [4] and [11]).

Sounds, flashing and acknowledgement: It is presently assumed that no additional features of sounds and flashing will be added for primary alarms. It will be tested if the requirement for only acknowledging primary alarms could be accepted.

Alarm icons in process display: It is assumed that no additional alarm icons will be considered. Only primary alarms will be displayed, while secondary alarms will be treated as suppressed alarms are treated today (ref. [4])

Background Information Report
2002-01-11 17:05:00

Report ID: FD 1024
GDS ID: US-2003-488
MFM Model: Dialysis V 2.0
Location: Poor Virgin Hospital
Renal and Day-Care Center
1100 Main Street
Chicago, Illinois 98744

Failed top goal: Maintain dialysis
Primary cause: Valve V44 blocked
Action / remedy: Replace valve V44

Total faults: 18

For 24-hour support, contact us at:

GoalArt
Tunavägen 39C +46 46 192640 phone
223 63 Lund +46 46 192641 fax
Sweden support@goalart.com

Background Information Displays: Addition of the new features in property marking of alarms allows formulation of practically free queries for display of alarm (group of alarms) background information. The Background Information Display (BID) will be formed as a report, answering standard pre-defined queries or situation dependent queries formulated by the operator or staff of maintenance. Example of such a report is given in Figure 4.

Alarm navigation tools / Information menus: Suitable navigation tools, normally in the form of background information menus, should enhance all alarm information. Normally, standard Windows features will be used, or standard tools provided today by the vendors. It will be evaluated in the project if those tools can handle new range of alarm properties.

Figure 4 Example of BID for the completed alarm burst

4. THE CONCEPT OF MULTILEVEL FLOW MODEL

4.1 Introduction

Multilevel Flow Models (MFM) are graphical models of *goals* and *functions* of technical systems. The goals describe the purposes of a system or subsystem, and the functions describe the capabilities of the system in terms of flows of *mass*, *energy*, and *information*. MFM also describes the relations between the goals and the functions that *achieve* those goals, and between functions and the sub-goals, which provide *conditions* for these functions. Morten Lind at the Technical University of Denmark invented MFM (see [8]). New features and implementations were contributed by Jan Eric Larsson at Lund Institute of Technology, (see [5]).

MFM provides a good basis for diagnostic algorithms. Three algorithms based on MFM; measurement validation, alarm analysis, and fault diagnosis are introduced in [5]. Other algorithms have been developed later, such as fuzzy alarm analysis, (see [1]), failure mode analysis, and sensor fault detection (both see [10]).

4.2 An example of an MFM model

A small example here will show the basics of MFM modelling. We will use a part of the main circulation system of a nuclear power plant. A much simplified process graph, from an example given in ref [3], is shown in Figure 5.

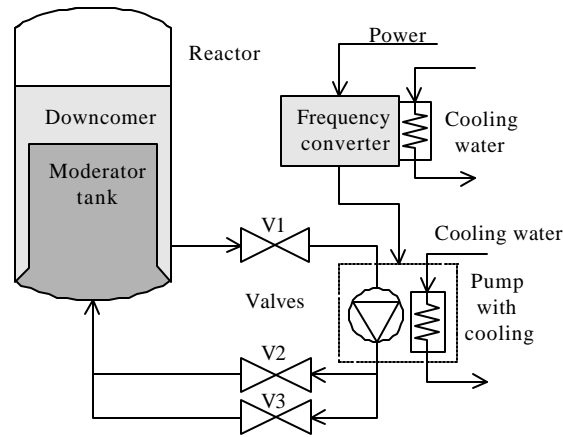


Figure 5 A process graph of the main recirculation system of a nuclear power plant

In this system, reactor tank water driven by the main circulation pump flows through the downcomer, valve V1, the pump(s), and back through the two parallel valves V2 and V3, to the moderator tank. The pump is frequency-controlled, and both the pump and frequency converter are water-cooled. The goals of this simple system are: “maintain desired water flow through the moderator tank,” “cool the pump,” “provide electrical energy with the correct frequency,” and “cool the frequency converter”.

The functions of the system are, among others: the ability of the downcomer to provide main circulating water, the ability of pump to transport water, and the coolers ability to transport the heat. An MFM model of this system is shown in Figure 6.

In the MFM model, there are four flows. The flow network M1 describes the water flow from the downcomer to the moderator tank. The network E1 describes the heat transport from the pump to the cooling water. The network E2 describes the flow of electrical energy from the supply, via the frequency converter, to the pump. The network E3 describes the flow of electrical energy from the supply, via the frequency converter, to the pump.

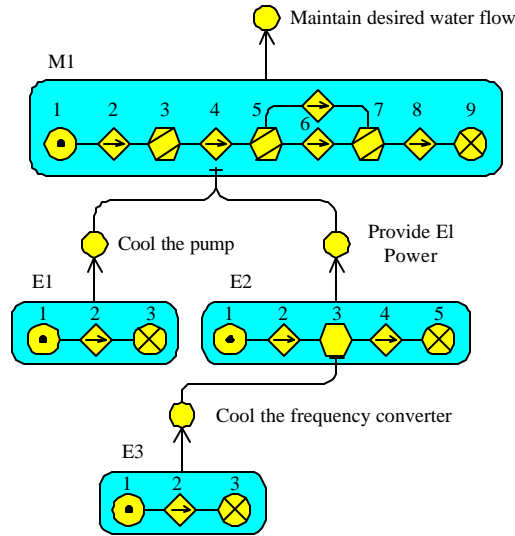


Figure 6 An MFM model of the main recirculation system

Finally, the network E3 describes the heat transfer from the frequency converter to the cooling water. Thus, M1 is a model of a mass flow, and E1 to E3 are models of energy flows. In the network M1 the functions are, from left to right: 1) a source of water, realized by the downcomer; 2) a transport, realized by the valve V1; 3) a balance, realized by the pipe between V1 and the pump; 4) another transport, realized by the pump; 5) another balance, realized by the forking pipe between the pump and the two parallel valves V2 and V3; 6) two transports, realized by the valves V2 and V3; 7) a balance, realized by the pipe sections between V2 and V3, and the moderator tank; 8) a transport, realized by the pipe that runs into the moderator tank; and finally, 9) a sink, realized by the moderator tank. The networks E1 to E3 contain energy flow functions describing the flows of electrical and thermal energy.

It should be noted that MFM describes how different flows enable each other. It can be seen in Figure 6 that the cooling flow E3 is necessary for the proper function of the frequency converter, and that the cooling flow E1 and the power supply E2 are required by the pump.

5. MFM-BASED DIAGNOSTICS

5.1 Algorithms based on MFM

Over the years, Larsson and his research group have developed several algorithms based on MFM. The algorithms are as follows:

Quantitative Sensor Validation: This algorithm uses quantitative process measurements to detect inconsistencies between redundant sensor values. In this way, it can detect faulty sensors and leaks. It can also provide guesses about the correct values, which can be used as “validated” values instead of the faulty ones.

Discrete Sensor Validation: This algorithm uses discrete (alarm) values to detect inconsistencies between redundant indications. In this way, it can detect faulty sensors and leaks. It can also provide guesses about the correct values, which can be used as “validated” values instead of the faulty ones.

Alarm Analysis: This algorithm sorts discrete status indicators, such as events and alarms, into primary and consequential. In this way, it can pinpoint the root causes of large alarm showers correctly, and it allows for alarm suppression without risking suppression of the primary cause.

Fault Diagnosis: This algorithm uses discrete process measurements to search from observed fault indications to root causes. The result is a complete explanation of a fault situation. The algorithm uses fault observations to guide the search and avoiding unnecessary measurements.

Action Planning This algorithm uses the results of the other algorithms to generate fault reports in different formats, including recommendations on corrective action plans.

Failure Mode Analysis: This algorithm calculates future consequences of actions, given a process state and one or several proposed faults or actions. In this way, it is an on-line planning support tool.

All the algorithms above use the same MFM model, that is, the MFM model is the “knowledge database” for the algorithms. This has some obvious advantages:

- A single modelling effort will provide the database needed for a whole set of different diagnostic tasks.
- The same MFM model can be used throughout the life cycle of the process, for different design and supervision tasks.
- Adding new features of the (modernised) process to the MFM-model will ensure inclusion of those features in the plant diagnostics

5.2 Advantages of MFM algorithms

The algorithms described in Larsson [5] are based on discrete logic where the “sensor” values are *low*, *normal*, or *high*, and the resulting values are *consistent* or *inconsistent*, *working* or *failed*, *primary* or *consequential*, etc. In other words, MFM uses a linguistic interpretation of logic variables, just as do rule-based expert systems and systems based on fuzzy logic. In addition, the MFM algorithms all operate by searching in fixed graphs. We have aimed at always producing algorithms that can handle the full MFM syntax, including closed loops in the flows and in the means-end dimension, as well as every kind of multiple fault situations. In addition, these complex cases should be handled by search methods of linear or sub-linear complexity. So far, all of our presented methods fulfil these requirements. Together with the discrete logic, explicit means-end concepts, and graphical nature of MFM, this gives several advantages:

- The explicit description of goals and functions gives a small semantic gap between the diagnostic task formulation and the knowledge representation.
- The graphical representation provides strong support for knowledge base overview and consistency, and there is no need for a specialized knowledge engineering tool.
- The high level of abstraction makes knowledge acquisition, knowledge engineering, and knowledge base validation and support considerably easier than with standard rule-based systems or fuzzy logic systems.
- The graphical nature of the models allows the algorithms to have good real-time properties, such as an easily computed worst-case time, low memory demands, and high efficiency.

- The high level of abstraction allows the algorithms to be very fast. A worst-case fault diagnosis on the Guardian system [7], for example, takes less than 80 microseconds on a 500 MHz Pentium Computer.

These advantages have been observed in practice, during the test developments for food processing industry and for the emergency room of the Guardian project, see [5], and [7]. MFM was then compared to the several other modelling methodologies and further corroborated in an alarm analysis project for the Barsebäck NPP (see [10]). There are at least two other full-scale evaluations run in parallel with the Nuclear Pilot Project³.

6. PROOF OF THE ALARM CONCEPT THROUGH THE NUCLEAR PILOT PROJECT

6.1 Parties involved

The parties involved in the project are

- Swedish NPPs: OKG, RAB and BKAB, with the main concern on the modernisation of the control rooms, allowing efficient and safe handling of plant events/alarms
- GoalArt, with the main task to build MFM models of selected parts of the NPP process, and providing new property marks for the events
- IFE Halden, concentrating on the presentation of events stamped with property marks

IFE Halden provides the final testing environment in form of a BWR model (1200 MW Oscar 3 unit), as developed and implemented in the HAMBO project, ref. [4].

6.2 Project structure and objectives

The objective of the Pilot Project is to evaluate GoalArt's claims (chapter 5.2) and prove conformance of the MFM-based methods with the criteria of chapter 2.4. The project will emulate the process of industrial I&C implementation in the simulated power plant environment. The project runs in three stages:

1. MFM-modelling and off-line testing
2. Preparation and commissioning of the GoalArt's test diagnostic station
3. Testing and evaluation at IFE Halden HAMBO simulator

The project started in June 2002 and will be concluded in January 2003

6.3 Scope of the tested MFM-model

The first stage of the project concerns centralised knowledge base of the diagnostics, the MFM-model. It was decided that water-steam systems of the Oscar 3 block would be modelled, including the following

- System 42X: Steam system, excluding auxiliary turbine systems (424)
- System 46X: Condensate and Feeding Pumps, excluding auxiliaries (464)
- System 312: Main Circulation System, as a part of water-steam circuit

The models will be prepared with MFM-editing tool, MFM-Builder, which supports all stages of both model building and model implementation for the run-time environment. Model implementation support includes testing facilities, allowing off-line simulation of pre-arranged

³ Medical equipment for GAMBRO, and conventional power industry for Vattenfall Development.

event sequences. It was further agreed that test sequences would be prepared by the power plants and IFE Halden, with GoalArt responsibility to prove the results.

The tested and approved MFM-model will be implemented in a run-time environment of the separate PC; GoalArt's test diagnostic station.

6.4 Test environment

The success of the project depends in a great degree on the environment in which the testing can be done (see Figure 1). "Free" access to the process, allowing initiation of all possible initiating events will be ensured through coupling of the GoalArt's test diagnostic station to IFE's BWR simulator (HAMBO, ref. [4]). The technical problems of the coupling were already solved in the ALLADIN ([11]). An IP-consumer will be created accordingly, allowing GoalArt's station to read tags from the signal database of the model and to add the generated property marks to the signals. GoalArt's station will further be allowed to add new event signals to the simulator signal database.

IFE's part of the work will also be to include procedures for reading the new property marks of events and to construct / adapt HMI features outlined above.

7. OTHER DIAGNOSTIC TOOLS AVAILABLE

It was decided that the Pilot Project would concern the kernel of the GoalArt diagnostic, MFM-model, as applied to the alarm system. The MFM has anyhow a lot of other applications, all based on the availability of the executable form of the plant knowledge base. That form can be used for plant structuring or in case of existing plants for extracting the structure in a clear, graphic form. MFM-presented structure will allow unfolding I&C structure over the plant systems in the most efficient and demonstrable form (ref. [9]). The following tools are here available:

*Reliability Analysis*⁴: This algorithm uses known measures of availability or reliability for each component to calculate reliability of subsystems and systems, either off-line during design and evaluation or on-line during operation.

Verification of Redundancy: This algorithm checks CMF and SFC⁵.

Verification of Safety Classification: This algorithm checks separation between redundant trains of safety-classified systems and dependencies between safety and non-safety systems.

The following complementary diagnostic tools work independent of the MFM:

State Based Alarm Priority: This tool allows efficient assignment of alarm priorities depending on the plant operating state. For example a great number of alarms can be suppressed (given priority 0) during plant off-load state. This priority setting is accordingly dynamic and will complement the alarm analysis tool based on MFM. The secondary alarm may after all get higher priority than the primary one.

Trend Analysis: Statistical analysis of historical signal data (trend data) will provide early warning of faults independent of set alarm limits.

Alarm Cleanup: As alarm settings are in the real world often set erroneously, or not maintained there is a need for constant check-up and cleanup. This algorithm uses comparison of redundant

⁴ Patent is pending

⁵ Common Mode Failure; Single Failure Criterion

status indications and alarms to detect erroneously set alarm limits, that is, to pinpoint alarms that are activated when they should not be, and alarms, which are silent when something is wrong.

8. CONCLUSIONS

The GoalArt and IFE Halden in cooperation evaluate powerful tools for handling alarm situations at nuclear installations. The MFM-based concept has been tested previously but not on installations as critical as a nuclear. The Pilot Project, when successful will provide basis for the next evaluation and implementation stage, namely on a training simulator of selected NPP. The MFM concept, if accepted by the operators would then be ready for real control room installations.

9. REFERENCES

- [1] Dahlstrand, F., "Methods of Alarm Reduction with Multilevel Flow Models of Industrial Processes", Licentiate Thesis, Department of Information Technology, Lund Institute of Technology, Lund, 2000.
- [2] IEC 62241/CD "Nuclear Power Plants – Main control room – Alarm functions and presentation", CD 2001
- [3] Ingström, D., "MFM Modeling and Alarm Analysis of the Barsebäck Nuclear Power Plant," Master's thesis, Department of Information Technology, Lund Institute of Technology, Lund, 1998.
- [4] Karlsson, T., "The Alarm System for the HAMBO BWR Simulator", Halden Report, HWR702
- [5] Larsson, J. E., *Knowledge-Based Methods for Control Systems*, Doctor's thesis, TFRT-1040, Department of Automatic Control, Lund Institute of Technology, Lund, 1992.
- [6] Larsson, J. E., "Avoiding Human Error," Proceedings of the International Conference on Control and Instrumentation in Nuclear Installations, Bristol, England, 2000.
- [7] Larsson, J. E. and B. Hayes-Roth, "Guardian: An Intelligent Autonomous Agent for Medical Monitoring and Diagnosis," *IEEE Intelligent Systems* vol. 13, no. 1, pp. 58–64, 1998.
- [8] Lind, M., "Representing Goals and Functions of Complex Systems — An Introduction to Multilevel Flow Modeling," Technical report, 90-D-38, Institute of Automatic Control Systems, Technical University of Denmark, Lyngby, 1990 a.
- [9] Mårtensson, T., "Structuring of Instrumentation and Control Systems Based on Multilevel Flow Models", Master's thesis, Department of Information Technology, Lund Institute of Technology, Lund, 1998.
- [10] Öhman, B., "Real-Time Diagnosis of Industrial Processes Using Multilevel Flow Models", Licentiate Thesis, Department of Information Technology, Lund University, Lund, 2001
- [11] Roverso, D., "ALLADIN Run-time and HAMLAB Applications", Halden Report, HWR691