A Revival of the Alarm System: Making the Alarm List Useful During Incidents

Jan Eric Larsson[1], Bengt Öhman[1], Antonio Calzada[1], Christer Nihlwing[2],
Håkon Jokstad[2], Liv Iren Kristianssen[2], Jon Kvalem[2], and Morten Lind[3]

1) GoalArt, Scheelevägen 17, 223 70 Lund, Sweden
2) IFE, OS alle 13, 1777 Halden, Norway
3) Ørsted-DTU, Technical University of Denmark, DK-2800, Kongens Lyngby, Denmark
1) Phone +46 46 286 4880, Fax +46 46 286 4882, E-mail janeric@goalart.com

Abstract– *In control rooms there are often problems with information overload, which means that the operators may receive more information than they are able to interpret. The most serious information overload occurs in two types of situations. The first is when the operating state of the plant changes, which often gives raise to a shower of alarms and events. Such an alarm shower is expected, but can be dangerous, because it may hide other alarms originating from unrelated faults. The second problem occurs when a fault causes several consequential faults, leading to a so-called alarm cascade. Because the alarms seldom arrive in correct time order, it can be very difficult to analyze such a cascade, and the information overload occurs in exactly the moment when a potentially dangerous situation starts. In an ongoing project, GoalArt and IFE are cooperating in testing and evaluating GoalArt's methods for alarm reduction and root cause analysis. The testing comprises two specific algorithms, root cause analysis and state-based alarm priority. The GoalArt system has been integrated with the HAMBO simulator so that operators can evaluate the algorithms on-line.*

I. INTRODUCTION

In modern control rooms, there is a constant risk of information overload. In particular, as soon as there is a larger disturbance, the alarm system tends to overflow with alarms. This, in turn, makes the alarm list and the alarm system less useful, especially in situations where it would be most beneficial. In fact, when an incident starts, operators tend to disregard the alarm list, and only when the incident has been taken care of, they return to the list, remove all waiting alarms, and then start using it for monitoring. This effect seems to be more common the better equipped the systems is with alarms, and is well known in nuclear control rooms.

GoalArt has developed a methodology for automated root cause analysis combined with state-based alarm prioritization and suppression, which enables the alarm system to sort the alarm and event information into several categories. Most importantly, the alarms pertaining to the initiating events of a complex fault situation, the root causes, can be selected and shown in a separate list. In this way, large alarm cascades can be reduced to one or a few single alarms.

This methodology is based on Multilevel Flow Models (MFM), which are used instead of other types of knowledge bases. MFM allows for computationally fast and reliable algorithms, and alarm cascades of more than 500 alarms produced by systems comprising a nuclear power plant, can be handled in about one second. MFM was originally conceived by Professor Morten Lind at the Technical University of Denmark, [11-13].

MFM knowledge bases can be constructed with much less effort than needed for other knowledge-based methodologies. In this project, we have built an MFM model for the Hambo simulator, comprising the majority of the status indicators (around 6 500 signals) for the Forsmark 3 nuclear power plant in Sweden. For this we have used around 4 man-months of modeling, testing, and validation time. Another 4 man-months were used by IFE in testing the system. Other techniques would probably have required orders of magnitude more modeling time.

The pilot system has been integrated with the Hambo simulator at Hammlab, Institute for Energy Research (IFE) in Halden, Norway. During the remainder of the project, we will design and implement a human-machine interface and perform operator testing with crews from Scandinavian nuclear plants. The project is sponsored by all Scandinavian nuclear powe r plants together.

We have already seen indications that this new technology means a revival of the alarm list. With our system, the primary list contains the 1-5 originating alarms only, and this list is useful at all time instants during an incident. The alarm list guides the operator to an immediate understanding of the fault situation, and works as a checklist of which faults that remain to take care of. Instead of being ignored, the alarm presentation becomes a primary source of information to the operator during complicated and critical situations.

II. ALARMS AND INFORMATION OVERLOAD

Alarm problems have been known since the introduction of control room technology. There are feasible requirements for alarm handling, see, for example, [4], and research efforts in the eighties and nineties have provided useful results. In spite of this, alarm problems have been more difficult to solve than expected, and are still present today. We propose that there are two reasons for this.

- There are several different types of alarm problems, and each type of problem needs its own solution.
- So far, there has been a lack of methods to solve some of the more difficult problems. For example, consequential alarm cascades needs an efficient method for root cause analysis, a nd previous solutions have demanded a prohibitively large amount of knowledge engineering work.

In the current project, we have focused on three problems:

- Handling consequential alarm cascades by MFM-based root cause analysis.
- Reducing alarm showers induced by state-changes, using an algorithm called state-based alarm priority.
- Designing new solutions for the alarm presentation based on the new analysis capabilities that the two above-mentioned algorithms could provide to the human-machine interface.

II.I Consequential Alarm Cascades

The most difficult alarm problem concerns consequential alarm cascades and root cause analysis. In a process, a fault usually leads to several consequential faults. This means that a single fault can create a large number of alarms, a so-called *alarm cascade*. Because of timing effects, alarm limit tuning, and physical properties of the process, the root cause seldom appears first. Alarm cascades can be very difficult to analyze, which often means that operators cannot easily figure out what is actually wrong with the process.

Alarm cascades are a well-known phenomenon in most control room settings, for example, in nuclear industry. They are a main source of trouble in complex fault situations, since they appear exactly at the most critical moments, and tend to incapacitate alarm systems by producing a large number of alarms.

A most difficult complication is the case of *multiple, independent faults occurring at the same time*, that is, a fault situation consisting of several independent root causes, combined with all the consequences of the different root causes. In such situations, the analysis of the causality is often very difficult, and we believe that it is easy to commit errors in this analysis.

II.II State-Dependent Alarms

Some alarms are only relevant for specific operating states. In other states, the alarms are irrelevant and disturbing. Typical examples of this are alarm bursts that appear during startup and shutdown, and alarms from switched-off equipment.

Most alarm points have been designed and placed in the process to monitor a specific value, which is important for the process in a certain operating state. For example, a circulation pump is important for the plant during production of thermal energy. But the relevance of the alarm depends on the current operating state. In a stand-by situation, for example, no circulation may be necessary, and the pump is not, and should not be, operating. In a simple alarm system, without suppression logic, this has the effect that there will be several alarms that are activated in states where they are irrelevant. For example, the pump in the example above, may give a low-flow alarm in the stand-by state.

There are two drawbacks of irrelevant alarms:

- Some alarms may actually be missing out on a real fault situation. For example, in one state, it may be important that a valve is open, while in another state, it may be vital that it is closed. If so, a simple, non-dynamic alarm will be erroneous in one of the states.
- Even if the ala rms produced are not erroneous, but just irrelevant, they will fill up alarm lists and swamp the human-machine interface. There is a risk that, if the operators acknowledge the “usual” list of irrelevant alarms, they might miss a relevant fault that occurred in the same time period. A large number of irrelevant alarms may cause the operators’ trust in the alarm system to deteriorate.

The solution to the state-dependency of alarms is to equip the alarm system with a state-estimating algorithm and to assign different dynamic priorities to each alarm depending on the current state. The priority should include complete suppression for irrelevant states.

III. MULTILEVEL FLOW MODELS

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. MFM was invented by Morten Lind at the Technical University of Denmark, [11-13]. Several new algorithms and implementations have been contributed by Jan Eric Larsson at Lund Institute of Technology, [7-10]. MFM development started in the late seventies and has reached industrial application in the beginning of this century, [2-3, 7-13].

MFM provides a good basis for diagnostic algorithms. The work of Larsson [7] describes several algorithms based on MFM. Measurement validation checks consistency between redundant sensor values, and can discover flow leaks, sensor failures, and other measurement errors. The alarm analysis algorithm analyses any (multiple) fault situation and can tell which faults are primary and which faults that may be consequences of the primary ones. The fault diagnosis uses sensor values and queries to the operator to discover the faults of the target system. The failure mode analysis uses MFM with added timing information to predict the consequences of failures. It can be used both during the design phase of a plant and in real-time during actual operation, [17]. The fuzzy alarm analysis works in a way similar to the discrete alarm analysis, but is based on fuzzy logic, which makes it more robust when faced with noisy signals close to decision boundaries, [1].

III.I An Example of an MFM Model

MFM has been thoroughly explained in Lind [11] and Larsson [7-9]. Here a small example will be given, to show the basics of MFM modeling. We will use a part of the main circulation system of a nuclear power plant. A much simplified process graph, from an example in the master's project Ingström [5], is shown in Figure 1.

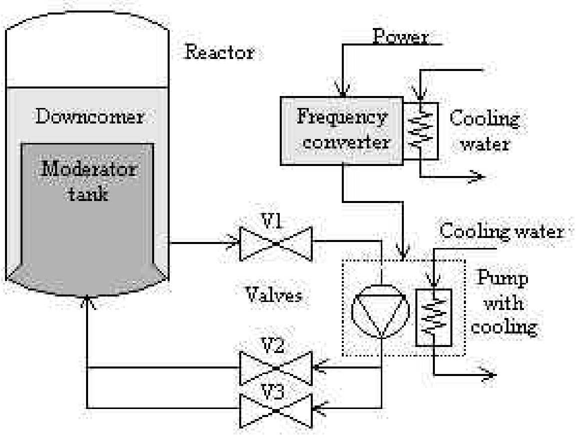

Fig. 1. A process graph of the main recirculation system of a nuclear power plant.

In this system, reactor tank water flows from the downcomer, via the valve V1, to the pump. After the pump, the water flows through the two parallel valves V2 and V3, back to the moderator tank. The pump is cooled by water. There is also a need for a frequency converter for the power to the pump, since the pump is frequency-controlled. Finally, the frequency converter must also be cooled. The purpose of the main water circulation is to control (moderate) the flow of neutrons in the reactor, and to cool it at the same time.

The goals of this system are: "maintain desired water flow through the moderator tank," "cool the pump," "provide electrical energy with the correct frequency," and "cool the frequency transformer."

The functions of the system are, among others, the downcomer's ability to provide water, the pump's ability to transport water, and the heat exchanger's ability to transport heat. An MFM model of this system is shown in Figure 2.

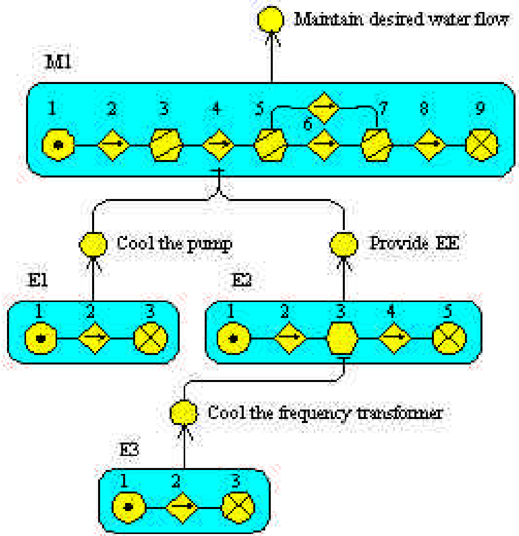

Fig. 2. An MFM model of the main recirculation system of a nuclear power plant.

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 transport of thermal energy from the pump to the cooling water. The network E2 describes the flow of electrical energy from the supply, via the frequency transformer, to the pump. Finally, the network E3 describes the flow of thermal energy from the frequency transformer 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. In the simple example in Figure 1, it can be seen that the cooling water flow E3 is necessary for the proper function of the frequency converter, and that the cooling water flow E1 and the electrical flow E2 are needed to keep the main water flow operating.

It is also important to observe that the given example is a very small toy example. MFM is designed specifically to handle large models with thousands of objects or more.

III.II Advantages of MFM Algorithms

The algorithms described in [7] are based on discrete logic. The MFM algorithms all operate by searching in fixed graphs. All cases are handled by search methods of linear or sub-linear complexity. Together with the discrete logic, explicit means-end concepts, and graphical nature of MFM, this gives several advantages:

- The graphical representation provides strong support for knowledge base overview and consistency.
- 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 alarm analysis on the full Hambo system takes a second on a standard PC.

These advantages have been observed in practice, during the current and previous nuclear projects, [16].

III.III Root Cause Analysis

An MFM-based algorithm called alarm analysis calculates the root cause (or causes) of any alarm cascade, and thereby helps the operators to understand the current fault situation. It reads real-time data from the existing control system and uses multilevel flow models (MFM) for its analysis.

There are two advantages of the MFM-based root cause analysis:

- The algorithm can handle all theoretically possible input combinations, including multiple independent root faults, and circular dependencies. The inputs are limited to low faults, normal states, and high faults. If this limitation is taken into account, and the MFM model gives an accurate description of the physical process, all potential fault scenarios will be correctly analyzed by the algorithm, including those scenarios never seen before.
- Building an MFM model is a relatively easy task, compared with producing a system with similar capabilities using fault trees and a rule-based expert system. The previous nuclear model comprises some 1 000 components and took 1-2 man-months to build. In a previous project, a system of similar size, based on fault trees, took around 10 man-years to build, see [14]. We state no exactly fairness in this comparison, but we believe that MFM modeling is quite efficient.

III.IV State-Based Alarm priority

An algorithm called state-based alarm priority (SBAP) reads real-time data from the existing control system, tracks its current operating state, and gives each alarm a dynamic priority depending on the current operating state. This includes complete suppression of irrelevant alarms. The method is not based on MFM, but uses a graphical editor for tabular input of alarm priority data, see Figure 3.

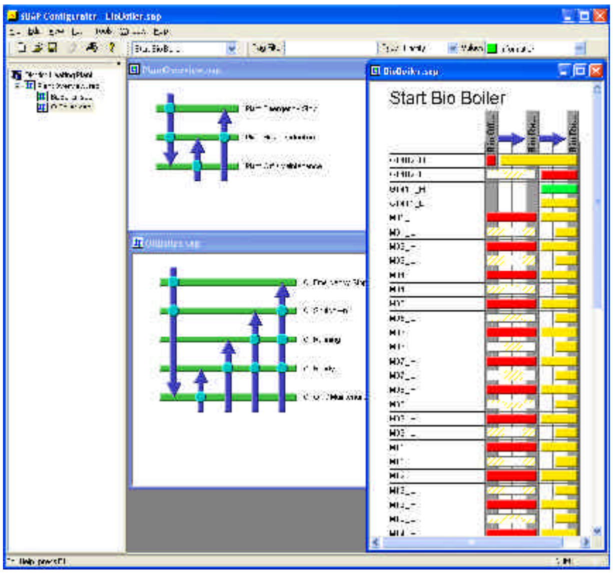

Fig. 3. Screen layout from SBAP Configurator.

The runtime part of SBAP estimates the current operating state of a plant or sub-process, and assigns a priority to each active alarm, including complete suppression if the alarm is irrelevant in the current situation. The main advantages of this method and tool are:

- It is a fairly easy task to use the graphical building tool to enter all the state-dependent priority information. In the project, we have assigned dynamic priorities to some 6 500 signals in 2-3 weeks of work time.
- The graphical tool gives a good overview of the varying priorities in successive operating states. In this way, it becomes easier to validate the entered knowledge.

IV. HUMAN- MACHINE INTERFACE

The current project involves test and evaluation of the new algorithms for root cause analysis and state-based alarm priority. But in order to use this new functionality, and to test and evaluate it in the project, we also need to present the new information in an efficient way. The new information available is:

- Knowledge on root causes and consequences, that is, the entire causal chain of alarms and events.
- A dynamic priority, varying with plant state, and including a priority value of "irrelevant"," where such alarms should be suppressed.

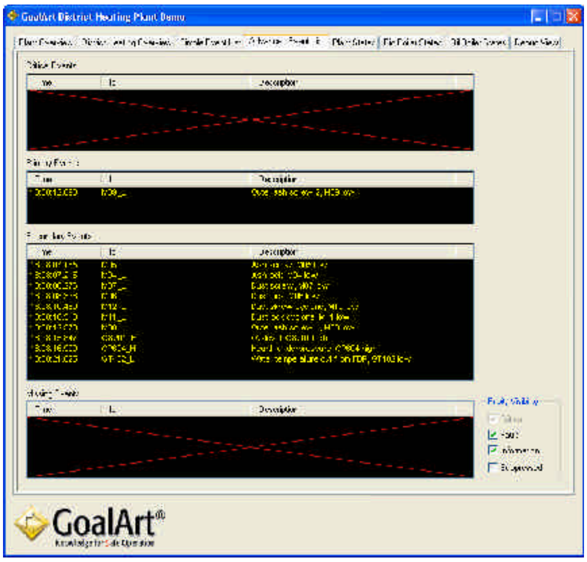

Fig. 4. Alarm list with four sub-lists, showing critical alarms, root causes, consequences, and missing but expected alarms.

In the previous project, a new type of alarm list was tried out, [16]. It contains four separate lists, one for alarms with critical priority (root cause or consequential), one for root cause alarms, one for consequential alarms, and one for expected but missing alarms (which are also calculated by SBAP), see Figure 4.

In the current project, the next step is to develop new ways of presenting the diagnostic information calculated by the root cause analysis and state-based alarm priority.

V. TASKS OF ALARM SYSTEMS

An alarm system should provide operators and maintenance personnel with structured information. This simple statement means that the operator should be able to extract exactly the information required for the particular state of the plant operation. In case of a plant transient, the operator will probably get an alarm cascade of several hundred alarms, and will have no time to study the complete alarm list. The information to be extracted concerns the following:

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

The situation will be more complicated if the plant moves 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 recognized and addressed accordingly.

The first action of the operators is normally to find out exactly what has happened and what parts of the plant are available. If that process would take too long time, the operator team leader responsible for safety will decide to take the plant over to a fail-safe state of operation, through reduction of the 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 system 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 will address the dynamic aspects of the alarm cascades mentioned above.

VI. THE HAMBO SIMULATOR

The HAMBO simulator is an experimental simulator located at IFE in Halden, Norway, and the simulator is used for performing human performance experiments, as well as testing of operator interfaces, alarm systems, and other operator support systems. The simulator's reference plant is the Forsmark 3 nuclear power plant in Sweden. Within the project, we have covered around 6 500 status signals, which is a major part of the simulator, using both MFM-based root cause analysis and state-based alarm priority. The project also includes development and testing of new ways of alarm presentation, using the extra information available from the root cause analysis and state estimation. Concerning the existing alarm system of HAMBO, see [6, 15].

VII. CONCLUSIONS

The aim of the alarm project is to reach a full integration of the alarm analysis and state-based alarm priority in the HAMBO simulator, so that the new algorithms can be tested under realistic circumstances online with real operator crews. In this way, one will be able to obtain measures of the usefulness and efficiency of the alarm reduction and situation assessment provided by the specific alarm algorithms.

The operator testing will take place mainly during the spring of 2007. However, we have already seen from early demonstrations, that our system can help to revive the alarm list, making it a dynamically available tool for monitoring and diagnosis, while incidents develop. We have good hopes that the operator testing will corroborate these early indications. If so, the alarm list will turn into a useful tool in complex and critical fault situations.

ACKNOWLEDGEMENTS

The authors would like to thank Anu Uus at GoalArt for proofreading, feedback, and valuable advice, and our nuclear partners in Scandinavia for the enthusiasm they have shown for our methods and for testing them in the two nuclear projects.

REFERENCES

[1] F. Dahlstrand, *Methods for Alarm Reduction with Multilevel Flow Models of Industrial Processes,* Licentiate thesis, Department of Information Technology, Lund University, Lund, Sweden, (2000).

[2] A. Gofuku, T. Ohi, and K. Ito, "Qualitative Reasoning of the Effects of a Counteraction Based on a Functional Model," Proceedings of CSEPC 2004, Sendai, Japan, (2004).

[3] A. Gofuku and Y. Tanaka, "A Combination of Qualitative Reasoning and Numerical Simulation to Support Operator Decisions in Anomalous Situations," Proceedings of the 3rd IJCAI Workshop on Engineering Problems for Qualitative Reasoning, (1997).

[4] IEC 62241/CD "Nuclear Power Plants – Main Control Room – Alarm Functions and Presentation", CD (2001).

[5] D. Ingström, "MFM Modeling and Alarm Analysis of the Barsebäck Nuclear Power Plant," Master's thesis, Department of Information Technology, Lund Institute of Technology, Lund, (1998).

[6] T. Karlsson, "The Alarm System for the HAMBO BWR Simulator", Halden Report, HWR702, (2000).

[7] J. E. Larsson, *Knowledge-Based Methods for Control Systems*, Doctor's thesis, TFRT – 1040, Department of Automatic Control, Lund Institute of Technology, Lund, (1992).

[8] J. E. Larsson, "Diagnostic Reasoning Strategies for Means-End Models," *Automatica*, **30**, 5, (1994).

[9] J. E. Larsson, "Diagnosis Based on Explicit Means-End Models," *Artificial Intelligence*, **80**, 1, (1996).

[10] J. E. Larsson, "Diagnosis Reasoning Based on Explicit Means-End Models: Experiences and Future Prospects," *Knowledge-Based Systems*, **15**, 1-2, (2002).

[11] M. Lind, "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).

[12] M. Lind, "Modeling Goals and Functions of Complex Industrial Plant," *Applied Artificial Intelligence*, **8**, 2, (1994).

[13] M. Lind, "Plant Modeling for Human Supervisory Control," *Transactions of the Institute of Measurement and Control*, **21**, 4-5, pp. (1999).

[14] A. B. Long, "Technical Assessment of Disturbance Analysis Systems," *Nuclear Safety*, **21**, 38, (1980).

[15] D. Roverso, "ALLADIN Run-Time and HAMMLAB Applications", Halden Report, HWR691, (2000).

[16] J. Tuszynski, J. E. Larsson, C. Nihlwing, B. Öhman, and A. Calzada, "A Pilot Project on Alarm Reduction and Presentation Based on Multilevel Flow Models," Proceedings of the Enlarged Halden Programme Group Meeting, HPR-358, Storefjell, Gol, Norway, (2002).

[17] B. Öhman, Real-Time Diagnosis of Industrial Processes Using Multilevel Flow Models, Licentiate thesis, Department of Information Technology, Lund University, Lund, Sweden, (2001).