Proceedings of the Korean Nuclear Society Autumn Meeting
Seoul, Korea, October 1995

Processing Alarms in DYNAS: Basic Strategy

I.K. Hwang, J.T. Kim, D.Y. Lee, N.J. Na, S.J. Song, J.C. Park, K.C. Kwon, C.S. Ham, and I.S. Kim*
Korea Atomic Energy Research Institute

Abstract

During transients or major upsets, operators of a nuclear power plant are faced with a significant amount of information which oftentimes exceeds their capability of processing information in such a time-critical situation. To help resolve this problem of information overload, considerable work is underway worldwide to improve its man-machine interface systems (MMISs). The I&C research team of KAERI is developing a DYNamic Alarm processing System, called DYNAS, to suppress unnecessary or nuisance alarms, and at the same time, emphasize vital information. This paper describes our basic strategy to process alarms in DYNAS.

1. Introduction

Recent catastrophic events in process industries suggest that plant information systems, such as the various man-machine interface systems (MMISs) of the control room including the alarm system, should be improved to ensure safe operation of the plant. For example, in the well-known Three Mile Island (TMI) Unit-2 accident, too many nuisance alarms from the alarm system at the early stage led the operators to misdiagnose the plant's status, resulting in large, adverse consequences.

In the light of the need to improve the information for the operators and also advances in the information and computer technologies, considerable research is under way to develop MMISs that will help to enhance the operational safety and productivity of the plant. One of the most important MMISs in this regard is computer-based alarm processing system which uses the information-processing capability of a computer to process alarm signals, sometimes augmented by raw process parameters. These alarm processing systems should be designed such that they should: 1) alert the operators to a deviation in the plant systems or processes; 2) inform the operators about the priority and nature of the deviation; 3) guide the operator's initial response to the deviation; and finally, 4) confirm, in a timely manner, whether the operator's response corrected the deviation.[1]

With these widely accepted functional criteria in mind, the I&C research team of Korea Atomic Energy Research Institute (KAERI) is developing a DYNamic Alarm processing System, called DYNAS, to suppress unnecessary or nuisance alarms, and at the same time, emphasize vital information to assist in the operators' tasks. This paper describes our basic strategy to process alarms in DYNAS, focussing only on the processing techniques. Other aspects, such as how to present the processed alarms, or how to verify and validate the alarm system, shall be reported elsewhere.

*Visiting Scientist under Brain Pool program

2. Representative Methods for Processing Alarms

Alarm processing systems process binary signals from alarms, sometimes augmented by raw plant measurements. In the midst of the increasing interest, a large number of alarm processing systems were designed and installed in the control rooms of nuclear power plants and other facilities.

In a study performed at Brookhaven National Laboratory (BNL), the following 9 representative methods of processing alarms were identified[2]:

(1) Mode Dependency
(2) Status-Alarm Separation
(3) Multi-Setpoint Intra-Relationship
(4) Event-Oriented Method
(5) Causality-Based Method
(6) State Dependency
(7) Hierarchical Relationship
(8) Alarm Generation
(9) Logic-Based Method

This classification of alarm-processing methods was made to characterize the way various alarm processing systems work internally. Generally, an alarm processing system uses only a few of these methods.

In addition, special features of signal validation and diagnosis may be added to an alarm processing system. All of these methods and features are discussed in Ref. 2.

3. Major Alarm-Processing Methods for DYNAS

Using the insights gained from the review of the state of the art in processing alarms, we developed a strategy to build a dynamic alarm processing system. This strategy is based on the following three major concepts:

1) Use cause-consequence relationships that may exist among alarm signals. Causal alarms require more attention from the operator than consequential alarms.

2) Suppress those alarms which are activated when the plant changes its mode or equipment changes its status, but require little attention from the operator.

3) Use hierarchical relationships that exist in large process plants, such as the levels of function, system, subsystem, and component. Also group low-level alarms into high-level information for the operator. Functional alarms also may be used where found effective.

In the sequel, we discuss our strategy for processing alarms for DYNAS, focussing on these three major concepts. Other miscellaneous considerations are discussed later.

3.1 Cause-Consequence Relationships

The main process of a nuclear power plant is a sort of continuous process. Hence, a change in the value of a process parameter in a certain location affects the value of the same or some other

parameter in another location, which in turn influences the process condition somewhere else, and so forth. When these changes are significant, exceeding their alarm setpoints, cause-consequence relationships exist among these alarms.

An avalanche of alarms during major plant upsets typically results from these consequential alarms (and also those alarms which follow when the plant or equipment suddenly changes its mode or status). The consequential alarms generally require less attention from the operators in their performing tasks than the causal alarms.

This cause-consequence relationship has been used as a major method in developing many computer-based alarm processing systems. For example, in the alarm system developed for the Oldbury nuclear power plant of the U.K.[3], the causalities were represented in a form of alarm trees. Alarm trees are a set of alarms which are assumed to be in a cause-effect relationship, denoted by an edge between the two alarm nodes. Messages can also be included in the alarm trees. When an alarm node in the tree is activated, any message associated with the alarm will be presented to the operator along with the alarm. As a fault condition propagates through the process, the propagation is followed up through successively higher levels of the tree.

The development of the alarm analysis system using alarm trees was important because it established a springboard from which many computer-based systems to support operators were developed. However, the plant-wide application of the alarm trees was less than satisfactory for the following reasons:

1) The alarm trees were costly to develop. It took approximately ten man-years of effort to construct the alarm trees for the Oldbury plant. Furthermore, the trees are difficult to modify.

2) Hardware problems or variations in plant dynamics too frequently resulted in the suppression of valid information or the display of confusing conclusions.

These hardware problems can be eliminated or significantly reduced now due to the significant advances in the technology of computer hardware and software engineering. Although the large, complex trees turned out to have a low probability of proceeding as predicted, we believe that the use of cause-consequence relationship in a small scale may be useful in processing alarms.

A survey of alarm processing techniques by Lupton et al.[4] also indicates that the cause-consequence relationship, sometimes called direct precursor, has been used in most recently developed alarm processing systems, including Alarm Filtering System (AFS), Dynamic Priorities Alarm System (DPAS), and EdF's N4 alarm processing system.

In this study, we investigated the applicability of several ways that may be used to represent cause-consequence relationships of the process, and thereby, identify such relationships among alarms. The candidates include digraph (i.e., directed graph), logic flowgraph, and process fault tree.

A digraph is a set of nodes connected by signed branches. The nodes represent process variables or certain types of failures, and the branches or directed edges indicate cause-effect relationships between the nodes. The signs on the directed edges represent the direction of deviations of the two process variables from normal values. A positive sign indicates that the deviations occur in the same direction, while a negative sign denotes that the deviations occur in the opposite direction. This digraph also has been used as a tool for diagnostics.

A logic flowgraph is similar to a digraph in the way of representing fundamental causality relations of the process. However, in addition to this causality network, the logic flowgraph methodology (LFM) also introduces another model, called condition network, to explicitly represent the conditions whose occurrence can change or modify the course of process causality

flow in the fundamental causality network. Thus, the LFM can be used to model the complex cause-effect relations existing between plant physical parameters, control variables, protective devices, and failure mechanisms.

A process fault tree means a fault tree constructed focussing on failure conditions of the process, such as high level of a heat exchanger or low suction pressure for a pump. The fault tree is basically a deductive structure, developed top-down beginning from a top event, and asking how the event can occur, as further goes down.

Among these candidates, digraph can be easily used to find cause-consequence relationships among alarms. However, where complex causalities exist in the process (e.g., because of protective devices such as interlocks, or other automatic built-in mechanisms), the logic flowgraph may be used to represent them. In light of the historical lesson from the attempt to use a huge alarm tree, the fault tree may be developed in a small scale, ever this being used. For example, a small fault tree may be built beginning from high level in a tank, ending up with the basic events of high inlet flow and low outlet flow. Then, when all these three alarms are activated, the high-level alarm is a consequential alarm, and one of the other two alarms can be identified as a causal alarm, depending on which alarm between these two first occurred and on some other information.

3.2 Mode and Status Dependency

The operating mode of a nuclear power plant indicates the mode where the plant is operating. For example, technical specifications (TSs) typically define the operating modes based on the reactivity condition, % rated power, and average coolant temperature, as power operation, startup, hot standby, hot shutdown, cold shutdown, and refueling. During a normal startup or shutdown, the plant changes its modes slowly. For example, when a TS-controlled component, such as a safety-injection pump, is out of service longer than allowed in the limiting conditions for operation (LCOs) of the TS, the plant may change its mode from power operation to hot standby, hot shutdown, and cold shutdown where the failed component is repaired. Even during these normal changes of modes, a large number of alarms typically are activated in a plant with a conventional alarm system based on one measurement, one alarm approach, because of the significant changes in the process parameters.

However, where the plant is suddenly tripped because of a certain fault, the process is subject to more abrupt changes than in the case of the normal plant shutdown. As a result, some consequential or extraneous alarms, such as pressurizer pressure low or steam generator level low, may follow after an indication of the reactor trip. If these alarms do not provide any clues or assistance to the operators in their interpreting or responding to the situation, then they may be filtered out or their priorities lowered compared to other important alarms. In fact, a study by Roscoe et al. at Sandia National Laboratories indicates that many alarms can be suppressed by this mode-dependency alone.[5]

The status of equipment means the state where the equipment is placed, such as 'running' or 'tripped' in the case of a pump. When a pump has been tripped , for instance because of a failure in its supporting function, such as pump seal water temperature high, several alarms may be triggered, e.g., low flow and low pressure in the main process line. These consequence alarms can be suppressed in the case of pump-tripped.

These two methods of suppressing alarms, based on the operating mode of the plant or the status of equipment, are similar, the major difference being in the scale of their application. In the mode dependency, alarms are reduced depending on the global status of the plant. In the status dependency, alarms are reduced depending on the local status of the equipment. Because these methods depend on the mode or status, they can be applied only when the plant changes its mode or equipment changes its status. Suppose a main feedwater pump is tripped during normal operation,

with the power operation mode retained at a lower power level. In this case, we may not apply mode dependency (unless a more refined definition of the operating modes is made), but the alarms triggered following the pump trip can be prioritized using status dependency.

The status dependency has been used as a major technique in developing Alarm Processing System by Domenico et al.[6] Both mode and status dependencies are being used to process alarms in DYNAS.

3.3 Hierarchical Relationships and Functions

Hierarchy is an inherent characteristic of a large process plant. For instance, a hierarchical relationship can be easily found in nuclear power plants: the levels of subcomponent (e.g., valve stem, plug, diaphragm or pump shaft), component (e.g., valve, pump, sensor or controller), subsystem, system (e.g., reactor coolant or main feedwater system), function (e.g., core heat removal or containment integrity), and plant. In conventional alarm systems, most of the alarms are component-level alarms indicating low-level information, because the systems were built from a rudimentary concept, i.e., the one measurement, one indication approach. The hierarchical relationship can be used to differentiate alarms that differ in hierarchy, or to generate high-level alarms from low-level alarms.

Typical examples incorporating the hierarchical relationship can be found in the advanced alarm systems that are designed by the Japan's Toshiba Corporation and Hitachi, Ltd. In Toshiba's ABWR (advanced boiling water reactor) control room, referred to as A-PODIA (Advanced Plant Operation by Display Information and Automation), the plant-level alarms present alarms related to overall plant status, the status of safety systems, and the status of important parameters on a large overview display. System-level alarms indicate the status of each system and are located as fixed tiles on the main operation console. Finally, equipment-level alarms are presented via cathode ray tubes (CRTs). Hitachi's ABWR control room, called NUCAMM-90 (Nuclear Power Plant Control Complex with Advanced Man-Machine Interfaces for the 1990s), also employs the concept of hierarchy.

A typical alarm system generating high-level functional alarms is SAS-II[7] developed at the OECD Halden Reactor Project. The very high level alarms of SAS-II describe the status of critical safety functions to assist the shift advisor in his observation and evaluation task after plant disturbances leading to scram.

However, functional alarms may be generated at a low level also. For instance, the alarm system of Kori Unit 4 contains the following alarms about the lubrication of the main feedwater pump (MFWP) turbine: a) lube oil discharge cooler header temperature high, b) lube oil filter differential pressure high, c) lube oil tank level high/low, and d) lube oil conditioner level high/low. These four alarms may be grouped as "MFWP turbine lubrication trouble". This trouble may lead to tripping of the associated MFWP, which in turn may trigger many alarms. The presentation of the functional alarm, instead of the four lower-level alarms, may help to reduce cognitive workload for the operator in such a situation. A more detailed information, such as lube oil filter differential pressure high, can be presented to the operator upon his demand, when he is ready to investigate the lubrication problem of the MFWP turbine.

3.4 Other Miscellaneous Considerations

In addition to the three major concepts discussed above, other miscellaneous considerations are also taken into account, such as multi-setpoint interrelationship and status-alarm separation which can be rather easily implemented. For example, the multi-setpoint interrelationship shall be used where multiple setpoints (e.g., low and low-low) are associated with a process parameter. When

the low-low alarm is activated, the low alarm requires less attention from the operator. The status-alarm separation also can be easily implemented. All we need to de is to identify those status alarms which simply indicate status of equipment, system, or the plant. Then, they can be presented to the operator, separately from other alarms.

The alarm system developed by incorporating the methods and concepts discussed herein can be further enhanced by adding the special features of signal validation and diagnostics.[2] Signals from the instrumentation system of the process need to be validated to avoid false alarms, which can corrupt the processing of alarm signals, and as a result, may cause misleading information presented the operator. Diagnosis can be performed by manipulating raw process parameters that will be readily available through a modern data acquisition system.

4. Concluding Remarks

The basic strategy for processing alarms in DYNAS has been discussed. This strategy is being applied to the condensate and feedwater systems of a pressurized water reactor. Once this prototype alarm processing system, DYNAS, is developed using G2 real-time expert system shell incorporating both production-system (i.e., IF-THEN-ELSE types of rules) and objected-oriented (e.g., slots, objects, classes, and inheritance) knowledge representation schemes, it shall be tested and evaluated against several representative failure scenarios with Kori simulator first, then with the NORS simulator at the Halden Reactor Project, Norway.

References

[1] W.L. Rankin, K.R. Ames, and R.J. Eckenrode, "Near-Term Improvements for Nuclear Power Plant Control Room Annunciator Systems." NUREG/CR-3217, PNL-4662, April 1983.

[2] I.S. Kim, "Computerized Systems for On-Line Management of Failures: A State-of-the-Art Discussion of Alarm Systems and Diagnostic Systems Applied in the Nuclear Industry," *Reliability Engineering and System Safety*, **44** (1994) 279-295.

[3] F.P. Lees, "Process Computer Alarm and Disturbance Analysis System: Review of the State of the Art." *Computers and Chemical Engineering*, **7** (1983) 669-694.

[4] L.R. Lupton, P.A. Lapointe and K.Q. Guo, "Survey of International Developments in Alarm Processing and Presentation Techniques," NEA/IAEA International Symposium on Nuclear Power Plant Instrumentation and Control, Tokyo, Japan, May 1992.

[5] B.J. Roscoe and L.M. Weston, "Human Factors in Annunciator/Alarm Systems: Annunciator Experiment Plan I," NUREG/CR-4463, SAND85-2545, May 1986.

[6] P.D. Domenico, E. Mah, D. Corsberg et al., "Alarm Processing System," Proc. on Expert Systems Applications for the Electric Power Industry, Orlando, FL, June 1989.

[7] F. Øwre, S. Nilsen, and E. Stokke, "A Computerized Safety Assessment and Post-Trip Analysis System for the Forsmark Unit 2 Control Room Integrating a Real-Time Expert System and a Modern Graphic Display System." Eighteenth Water Reactor Safety Information Meeting, Rockville, Maryland, October 22-24, 1990.