ADDRESSING THE ALARM ANALYSIS BARRIER - A TOOL FOR IMPROVING ALARM SYSTEMS

E.C. DAVEY, R.A. BASSO and M.P. FEHER

Control Centre Technology Branch
AECL, Chalk River Laboratories
Chalk River, Ontario, Canada K0J 1J0

ABSTRACT

This paper describes a software application tool for the initial specification and maintenance of the thousands of alarms in nuclear and other process control plants. The software program is used by system designers and maintainers to analyze, characterize, record and maintain the alarm information and configuration decisions for an alarm system. The tool provides a comprehensive design and information handling environment for:

- the existing alarm functions in current CANDU plants,
- the new alarm processing and presentation concepts developed under CANDU Owners Group (COG) sponsorship that are available to be applied to existing CANDU plants on a retrofit basis, and
- the alarm functions to be implemented in new CANDU plants.

BACKGROUND

CANDU plants employ a computer-based alarm system to alert operating staff to abnormal conditions and changes in state as a result of the automatic responses of the control system. In current plants, the main alarm system is implemented as part of the digital control computer software. Each of these alarm systems contain a database of several thousand alarms that provide coverage for all plant safety and power production functions.

Over a station's life, there is a continual need to make changes to the alarm system to improve on the existing or add new alarm functionality to better meet operator needs. The impetus for change can be as a result of several factors, for example:

- increased production targets (e.g., tightening of operating margins),
- improvements to station operational practices (e.g., addition of new alarms to provide operators with better support for procedures), and

- compliance with evolving regulatory requirements.

Some of these improvements can be implemented by changes to the information in the alarm system database alone (e.g, adjustment in an alarm threshold). Other improvements require changes or additions to the alarm system functionality as well as changes to the information in the alarm system database. In such cases, extensive changes to the alarm database structure and entries can be required.

AECL in partnership with CANDU utility staff, have developed several improvements for CANDU alarm systems [1,2,3] under COG sponsorship. A prototype system, called the CANDU Annunciation Message List System (CAMLS), has been developed to demonstrate and evaluate the proposed improvements. CAMLS introduces several new alarm system functions, namely:

- dynamic reprioritization of alarms based on plant operating conditions,
- cause-consequence conditioning of alarms to improve relevance,
- combination of similar or channelized alarms into a single summary alarm,
- generation of alarms identifying the failure of expected automatic actions,
- separate presentation of alarms identifying problems in the plant from those identifying only non-problematic changes in state, and
- organization of the presentation of fault alarms by order of importance.

The operational benefits of the CAMLS annunciation concepts have been proven in simulator based evaluations at the Point Lepreau Generating Station. In comparison to the current plant annunciation, CAMLS significantly improves operators':

- awareness of plant state,
- probability of detecting significant alarms and problems,
- probability of detecting alarms and problems independent of the primary or initial upset,
- confirmation of the cause of a trip,
- identification of the cause of an upset,
- access to alarm response procedures and other alarm reference information, and
- overall performance through reduced demands on short term memory and the need to interact with the annunciation system.

To support the implementation of the CAMLS improvements, several changes and additions must be made to alarm information contained in the alarm system database. During the course of the CAMLS development program, it became apparent that a key to realizing the benefits of any improvements in existing plants or in a new plant design would be the availability of an effective tool to support the analysis and categorization of alarm and related information.

THE ALARM SYSTEM DESIGN TASK

The implementation of alarm system changes and improvements requires the incorporation of station specific rules, strategies, and guidelines for classifying, prioritizing, and conditioning alarms to be entered into the alarm system database and/or alarm processing program. This information is collected from the station's operating policies and principles, design documentation, emergency operating philosophy and procedures, operating manuals, and from station staff experienced in both safety and production activities. This is a design task and the effort to analyze and record the alarm design decisions for all plant alarms must be practical, manageable, and not too costly relative to the potential operational benefits.

While it may be possible to manage this design task manually, the large amount of information that needs to be analyzed, consulted, recorded, and reviewed for consensus between several experts makes conventional manual and paper-based management of the information labour intensive, time consuming, and prone to error. Utility staff have stated that they have been reluctant to pursue alarm system improvements due the perceived large and time consuming effort to analyze, record and manage the information for the several thousand alarms in the plant.

BENEFITS OF AN ALARM ANALYSIS TOOL

With utility and design staff expressing considerable interest in alarm system improvements, AECL undertook the development of a software tool to assist alarm system designers and maintainers. The software application is called the CANDU Alarm Analysis Tool (CAAT) and is being developed to:

- reduce by one half the effort required to initially implement and commission alarm system improvements,
- improve the operational relevance, consistency and accuracy of station alarm information,
- record the basis for alarm related decisions, and
- make day-to-day maintenance of the alarm database more cost-effective.

The CAAT achieves these benefits by:

- enabling utility users to customize the application via configuration menus and design rule entry to specify the station rules to be followed for alarm database definition (e.g., priority assignment rules),
- presenting a framework for making alarm design decisions that promotes an operations perspective, as well as consistency and completeness of alarm database entries (e.g., each alarm should be examined for operational relevance in each plant operating region),
- storing both the design rules and the results of their application within a common database so that the effects of changes to design rules on the alarm database can be consistently applied and immediately observable,

- substantially simplifying information recording and searching tasks by automating the repetitive and labour-intensive task aspects in comparison to conventional paper-based methods,
- providing electronic access via plant information system servers to the supporting information to assist with making specific design decisions (e.g., alarm response procedures, historical plant parameter and annunciation logs), and
- enabling the electronic comparison of design decisions among multiple station analysts to determine overall alarm database consistency and identify outstanding discrepancies.

In performing analysis and design tasks, the CAAT assists users in accessing, sorting and recording relevant information, design rules, decisions, and provides reports in support of system maintenance, analysis of design changes, or regulatory inquiry.

The core functional requirements for the CAAT are generic and thus applicable to any nuclear plant and other process control industries. It is already being used to support the analysis and management of alarm information for three CANDU plants to support the demonstration and validation of CAMLS alarm improvements.

TOOL FUNCTIONALITY

CAAT provides a computer-based design environment for performing analysis, design and review tasks associated with the alarm database for a CANDU plant. It assists users in accessing, sorting and recording relevant information, design rules, decisions, and provides reports in support of system maintenance, analysis of design changes, or regulatory inquiry. CAAT supports the recording, tracking and review of design decisions concerning specification of:

- plant modes (i.e., plant operating regions) and supporting parameters within which to define alarm relevance and priorities,
- plant alarms including the:
  - condition and threshold(s) that define when the alarm should be generated,
  - type of alarm (i.e., fault or status),
  - format and contents of alarm message text, and
  - relevance of the alarm for each operating mode (i.e., plant operating state),
- appropriate priorities for each alarm in each relevant operating mode (i.e., dynamic prioritization),
- situations under which individual or groups of alarms are suppressed (i.e., conditioning),
- situations where several similar alarms can be combined into a single message for presentation (i.e., coalescing),
- alarms that alert operators to expected conditions that fail occur (i.e., expected-but-not-occurred alarms), and
- supporting alarm details including:

- source instrumentation references,
- flowsheet references,
- group affiliations (i.e., system, parameter group, function), and
- response procedures.

CAAT supports tasks associated with both specification of the information for an alarm system and the transfer of the information to alarm databases of operational alarm systems.

Alarm Database Specification

Development of an alarm database involves two types of developer tasks. The first task (i.e., criteria definition) defines the database structure (e.g., names and number of plant modes). This activity establishes the database architecture and selection options for specific information categories. The second task involves entering information into a database for individual and groups of alarms or related supporting information.

CAAT enables a developer to look at alarm information in several ways to support the work approach chosen, for example information can be grouped to view:

- all information with respect to an individual alarm,
- all alarms with respect to a specific alarm category,
- the priorities for each relevant mode for an alarm,
- all alarms with respect to a specific conditioning or expected-but-not-occurred initiating trigger,
- all groups of alarms that are replaced by a single coalesced alarm,
- alarms judged not be relevant for a specific plant mode, and
- all alarms with respect to an operating manual or procedure.

In addition, the following facilities are provided to support developers in establishing operational relevance, completeness and accuracy of alarm entries:

- selection of alarm entries from predefined lists of possible values to simplify the manual task of database entry and promote database integrity,
- the use of text fields to record the rationale for specific alarm information choices,
- search of the alarm database to identify alarms with similar specified properties,
- copying of database information for one alarm to new entries for similar alarms to facilitate working on multiple related alarms simultaneously,
- comparison of database entries for specified alarms, and
- indication of database completion for each type of information stored.

CAAT provides the ability to track different versions of the same database and support development of multiple annunciation databases to meet the needs of developers and maintainers at multi-unit stations. More specifically, it permits developers to:

- define a name for each alarm database,
- create a new version of a database once a user completes a modification session,
- permit a user to select which database version to work with (e.g., rollback the database to a past configuration),
- maintain a record of the names and database users and the times when a database is modified and the reasons for the change, and
- permit only one user to make modifications to a database version at one time.

Alarm Database Use

The CAAT database contains information to support existing CANDU annunciation systems as well as the CAMLS annunciation improvements developed under COG sponsorship. Once the information for an alarm system is created, it can be downloaded directly to a specific annunciation system for use. The initial CAAT implementation provides the capability to download annunciation information directly to an annunciation system incorporating the CAMLS improvements. The capability to download alarm database information into existing CANDU Digital Control Computer (DCC) annunciation software modules has not been implemented. The need for such a capability will be established as part of annunciation retrofit discussions with specific stations.

Once an alarm database is created and used to support a fielded annunciation system, periodic changes to the database will likely be required to accommodate changes in plant configuration, reference material, operational practices or procedures. The same properties of the tool that assist with initial alarm specification should support annunciation system engineers, safety analysts, and operations staff in reviewing database entries and defining new database entries as required.

OPERATIONAL ENVIRONMENT

CAAT is intended for office use at CANDU stations or in design organizations. For alarm information definition and maintenance, the tool can be used in a standalone configuration or connected via a network LAN to station or design databases to access supporting sources of information or print reports. When information from CAAT is required by an annunciation system it can be downloaded by authorized station personnel to the specific system via a LAN or serial port connection.

SYSTEM ARCHITECTURE

The system architecture used to implement CAAT is illustrated in Figure 1.

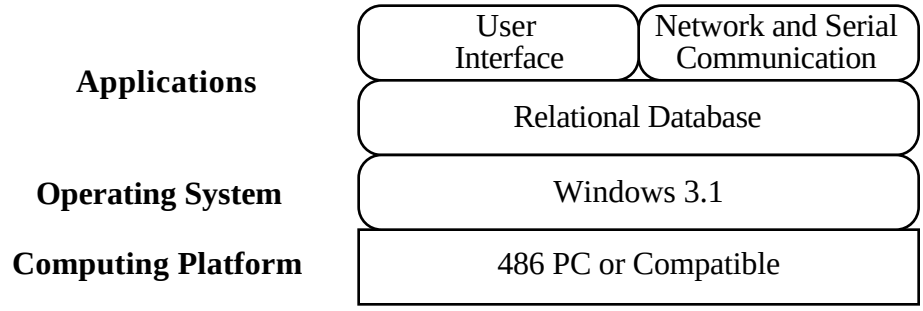

FIGURE 1: SYSTEM ARCHITECTURE.

Three application modules are used:

- a user interface module that manages a user's requests to create, modify or view database information and organizes the presentation of database information,
- a relational database module that stores the alarm information, and
- a network and serial communication module that enables downloading of information from the alarm database to other systems.

CAAT was designed to operate from a Microsoft Windows 3.1 compatible computing platform as this is a common environment for most utilities.

DEVELOPMENT STATUS

The core functionality of CAAT was developed and demonstrated during 1994. During this development period, key functions of the tool were proven and the effectiveness of CAAT in supporting alarm system designers was assessed through the analysis of alarms to demonstrate and validate the CAMLS annunciation concepts. To date the tool has been used to analyze alarms for the Darlington, Gentilly 2 and Point Lepreau Generating Stations. AECL is continuing to work with utility and design staff to refine CAAT functionality to better meet designer and maintainer needs.

CONCLUSIONS

AECL has developed an alarm system design tool (CAAT) that provides a computer-based design environment for performing analysis, design and review tasks associated with the alarm database for nuclear and other process control plants. Use of CAAT in place of conventional approaches is expected to substantially reduce the time spent by alarm system developers to define the information elements for a new application and result in a more consistent, better documented and more easily licensible design.

The support concepts implemented within CAAT are expected to be essential to the cost-effective implementation and maintenance of future CANDU annunciation improvements. For example, several CANDU stations are considering annunciation system upgrades based on the

CAMLS concepts. In addition, AECL has adopted the CAMLS annunciation concepts for use in future CANDU stations. It is expected that CAAT will play a key role in the implementation of CAMLS improvements to current station alarm systems and future designs.

REFERENCES

1. K.Q. GUO, S.H. BHUIYAN, M.P. FEHER AND E.C. DAVEY. (1994). Developments in Improved Alarm Annunciation. Paper presented at the 1994 Canadian Nuclear Society conference, Montreal, Quebec, June 6-8.

2. M.P. FEHER, E.C. DAVEY AND L.R. LUPTON. (1994). A User-oriented Approach to Improving Alarm Annunciation. Paper presented at the 1994 American Nuclear Society summer conference, New Orleans, Louisiana, June 20-24.

3. E.C. DAVEY, M.P. FEHER AND K.Q. GUO. (1995). An Improved Annunciation Strategy for CANDU Plants. Paper to be presented at the 1995 American Nuclear Society meeting on 'Computer-based Human Support Systems: Technology, Methods and Future', Philadelphia, Pennsylvania, June 25-29.