

AN IMPROVED ANNUNCIATION STRATEGY FOR CANDU PLANTS

E.C. Davey, M.P. Feher, and K.Q. Guo
AECL, Chalk River Laboratories,
Chalk River, Ontario, Canada, K0J 1J0
(613) 584-3311

ABSTRACT

In large, complex process systems such as nuclear power plants, annunciation is intended to alert operations staff to important changes in plant conditions that may impact on operational goals. Annunciation, along with the routine monitoring of control room displays and field communication, should enable operations staff to keep up-to-date with the current plant conditions and predict future plant states for all phases of plant operation.

Over the past thirty years of nuclear plant operation, the understanding of the needs of operators within the system has improved and the available technology to support them has become more sophisticated. Even so, it is still common to find annunciation systems with deficiencies such as 'alarm flooding' during plant upsets, distracting alarms irrelevant to the operating situation, and alarms with cryptic messages.¹

The opportunity to improve nuclear plant annunciation has been well recognized world-wide for many years. In Canada, nuclear utilities and AECL have co-sponsored a research program to develop enhancements to the initial annunciation system designs. An improved strategy for CANDU annunciation has been developed incorporating concepts that significantly improve performance and are retrofitable to current plants and are being incorporated into new plant designs.

This paper reviews the development approaches taken, discusses the operational principles established to guide the development of annunciation improvements and assess their effectiveness, and describes the processing, presentation and interaction concepts of the improved CANDU annunciation strategy. The paper concludes by summarizing the current program status and plans to validate the effectiveness of these new annunciation concepts in operational settings.

INTRODUCTION

This paper describes an improved strategy for CANDU annunciation. The strategy described is the outcome of a

research and development program undertaken by AECL in partnership with operations, training and engineering staff at CANDU stations in Canada. The success of the concepts embodied in the strategy was due primarily to three factors:

- the operational understanding of the role of annunciation in supporting control room tasks developed by the project team,
- the iterative approach applied to concept development, evaluation and refinement, and
- the access to operations and training staff provided by the Point Lepreau Generating Station (PLGS) in support of concept demonstrations and evaluations.

For the purposes of this paper, 'strategy' is defined as the coordination of human and machine elements to fulfill a role within the control room. In essence, a strategy represents the underlying philosophy of use and operational intent for a system.

A key component to the success of any fielded system is the availability of a complete description of the underlying strategy for the system's operation. While all systems are based on some underlying strategy when they are designed, in many cases, the description of the strategy is incomplete and in some cases not explicitly recorded. The failure to clearly define the strategy of a system can result in design inconsistencies and confusion during initial implementation and the development of future improvements.

In addition, the strategy provides an initial basis for the development of operational training, procedures development and maintenance practices. Without a clear and precise definition of this strategy for guidance, operational practices are likely to be less effective and the implementation of retrofit improvements can become cumbersome and potentially contradictory to the original operational intent.

THE ROLE OF ANNUNCIATION

CANDU nuclear power plants are large, complex electrical generation facilities that are operated under computer control. Overall plant operation is supervised by human operators using computer displays, and conventional instrumentation and controls from a central control room. Annunciation is used to ensure that control room staff are promptly alerted to important changes in plant conditions that may impact on operational goals.

More explicitly, annunciation is defined as a plant function that:

- detects and may predict the occurrence of plant changes,
- alerts users to changes important for the current operating situation, and
- points users to additional plant information to understand and respond to the changes. ²

To *detect* means to identify all changes in plant conditions that may be of relevance to current or future operational goals. In many instances, detection thresholds can be established such that there is adequate time for operations staff to take decisions and action following a change in plant condition and achieve the necessary response goals. In some instances, the consequence of the change in plant state is important enough that operations crews must be provided with advance warning of the impending occurrence to allow adequate time to respond.

To *alert* means to redirect an operator's attention from whatever task is being engaged to a pertinent change in plant state. This redirection can be either physical or visual. A physical redirection means that the operator must physically move to attend to the stimuli. Visual redirection only requires that the operator adjust the direction and/or focus of vision to the stimuli.

To *point* means to provide direction for the operator to the relevant supporting information to deal with the detected anomaly. Annunciation should offer the operator the pertinent information in an understandable, concise, and context-sensitive manner. This means that annunciation should support human information-processing and decision-making behaviours and limitations. Through observation and discussion with many different operating personnel it was found that it is not sufficient to alert an operator to a device and then tell them to go elsewhere (i.e., point) to get the necessary information to understand the nature and use of the information alerted to. Thus, the 'point' must be more than just a redirection, it must

provide meaningful information to support the appropriate operational tasks.

OPERATIONAL ISSUES WITH CURRENT CANDU ANNUNCIATION

CANDU control rooms are organized on a system-basis and each panel contains annunciation indicators at the top and conventional indicators (e.g., edge meters, status lamps), computer displays, and equipment controls (e.g., handswitches and analog controllers) throughout the balance of the panel area. Operators use the computer displays as their primary source of information during supervision of stable plant operation and execution of startup, shutdown and power-change manoeuvres. ³

Annunciated information is displayed to operations staff by two centrally located computer displays and a limited number of window annunciators at the top of each panel. The computer displays enable changes in the status of more than 6000 analog, contact inputs and calculated variables to be individually annunciated. These displays have a presentation capacity of about 20 messages each. If more annunciation messages are available for display at one time, the most recent messages overwrite the oldest ones.

The annunciation system supports operations staff well during normal operating conditions at full power, and for minor equipment failures or process upsets.

During major plant upsets (e.g., reactor or turbine trip), operations staff use the panel window annunciators to track changes in the plant safety and production state, until the annunciation message presentation on the computer displays re-stabilize. The result is operational practices that rely on the hard-wired window tiles to support the initial upset response and safety concerns. The problem with this approach is that the tiles are limited in number, and primarily safety-related. Thus, they do not provide full annunciation support during upsets for all tasks associated with state identification, diagnosis, root cause determination, planning, and other tasks associated with stabilization of the production side of the plant.

DEVELOPMENT OBJECTIVES

The objectives for the improved CANDU annunciation strategy were to establish a framework and requirements that resulted in:

- a design that supports operational tasks involving annunciation with the underlying goal of enhancing safety and production,

- a design that is complementary to other operational activities required of the operator, and
- a design that supports human attentional demand and short- and long-term memory limitations, and information-processing and decision-making behaviours.

In developing the strategy, the project team was expected to take into account the successful aspects of current CANDU annunciation design and operations experience, plus the experience and lessons learned from international annunciation projects. Thus, the strategy defined was expected to represent a statement of the 'ideal' tempered with the realities of variations in utility operation philosophies, human factors issues and limitations, and foreseeable and practical technological innovations.

For example, to be of practical application, the strategy was expected to offer an improved vision of annunciation for both current stations and for future plants. While all elements of the strategy could be applicable to future plants, stations are expected to consider only a subset of the strategy elements for their retrofit.

DEVELOPMENT SCOPE

The project scope was focused in two ways:

- work centered on improving computer-based control room annunciation, and
- plant upsets were used as the reference operating situations for development.

Computer-based annunciation is the primary means of annunciation used in day-to-day plant operations. Other annunciation media are used on a less frequent basis (e.g. annunciator tiles, off-normal lights). It was felt that, to be useful for both the retrofit of current stations and new station designs, the project work should first address the computer-based annunciation medium. This is an area where advances in technology could lead to improvements over the existing system. It was also assumed that a full and complete understanding of the use of this medium would be invaluable if the development and design of other annunciation forms was to be undertaken.

Experience has shown that plant upsets provide an exceptional challenge to annunciation functions and tasks. Upsets are an area of plant operations where substantial operational benefits could be realized in the short term from annunciation improvements.

BASES FOR STRATEGY DEFINITION

Four sources of information were used as the basis to identify the functional requirements, information needs, and resulting design concepts illustrative of a new annunciation strategy:

- operational principles that annunciation should support,
- plant operational strategies and practices,
- models of supervisory control and human decision-making, and
- human perceptual and cognitive performance capabilities and limitations.

A. Principles

To anchor the development of the strategy to operational realities, the following set of guiding principles for annunciation were established:

- Information must be provided in situational context.
- The context is to be based on the physical state of the plant as defined by contiguous operating envelopes.
- The presented importance of information must be consistent with operator needs and the situational context.
- No operationally relevant information is to be suppressed.
- All information, relevant and irrelevant, must be available on demand.
- Direct support for operator tasks must be provided.
- Operator interaction with annunciation must fit with the demands of other tasks in the control room.

B. Operational Strategies for Upsets

Canadian utilities are formalizing the strategies to be used by operations personnel in responding to plant upsets. 4, 5 The development of these strategies has proceeded as an outcome of the formalization of emergency operating procedures (EOPs), and the need to operationally integrate EOPs and the annunciation response procedures within plant operating manuals to support control room response to specific upset scenarios. The upset response strategy developed at the Point Lepreau Generating Station (PLGS) was used as a reference for the definition of control room functions and tasks.

Using the PLGS response strategy, a model of the tasks of operators and/or automatic systems in response to plant upsets was developed. This model provided a framework for identifying the functional requirements and associated information needs for an improved annunciation strategy. This model identifies six phases of operational response:

- response to changes in plant state consistent with operational goals (i.e., pre-trip operation),
- execution of special safety system functions,
- stabilization of plant processes and systems,
- diagnosis of fault conditions,
- correction of fault conditions, and
- restoration of power production capability.

The post-trip activities are representative of the plant upset response and recovery strategies. The pre-trip activity was added by the authors consistent with our understanding of normal operation of the plants.

C. Models of Supervisory Control and Human Decision-making

Models of supervisory control and human decision-making were used to provide practical perspectives from which to examine and further categorize components of the operational strategy phases.

CANDU operational practice assigns the control room crew full responsibility and authority to control all aspects of plant operation. To achieve specific safety and production requirements, most middle and lower level plant functions must be highly automated. Thus, to carry out their responsibilities and meet production and safety goals, operations staff must actively supervise a highly automated process system. Plant functions are assigned preferentially to the plant operations crew or automation. In reality, functions are rarely allocated exclusively to an operator or automation. In most cases, the performance of the function is shared on some basis. Thus, with this supervisory control model, there is a need for annunciation to support plant operators to monitor the success of automated functions and take over performance of automated functions if they should fail.

Several models of human decision-making have been proposed in the literature. For the purposes of categorizing the characteristics of operator decision-making that are

important to support for each specific upset response phase, we adopted the use of the Swain and Weston model of human operator behaviour.⁶ This model is consistent with other decision-making models such as those of Rasmussen and Rouse.^{7, 8}

D. Human Capabilities and Limitations

In supervisory control, the tasks of the operator are primarily cognitive as opposed to physical. As a consequence, annunciation features should be limited to those that support and are compliant with the cognitive capabilities and limitations of humans during the decision-making process. Five areas were selected to focus cognitive compliance in annunciation feature selection:

- attention,
- short-term memory,
- long-term memory,
- situation awareness, and
- goal-based decision-making.

DEVELOPMENT APPROACH

The development approach consisted of a process of using annunciation principles, operational strategies for upset management combined with models of supervisory control and human decision-making to define a set of functional requirements and information needs for an improved annunciation strategy. The functional requirements represent the system's performance goals and objectives, while the information needs represent the information required to coordinate human and machine tactics, thereby defining the performance requirements of both. An objective of this synthesis was to define functional requirements and information needs that were both meaningful and measurable. In this way, future validation of the concepts developed could be achieved by testing to meaningful and measurable performance requirements. The final stage in strategy development was to identify candidate design features that satisfied the identified functional requirements and information needs and provided compliance with human performance capabilities and limitations.

ELEMENTS OF THE IMPROVED STRATEGY

The elements of an improved annunciation strategy can be described with respect to design features of two annunciation facilities:

- A. A console-based interrogation workstation that provides electronic access to both real-time and historical annunciation message logs, annunciation message detail, and links to related information (i.e., procedures, parameter displays, and flowsheets) to support control room staff in responding to annunciated conditions.
- B. Central annunciation message list displays that alert operations staff to plant changes and provide continuous presentation of the most recent changes.

A. Interrogation Workstation

The console-based interrogation workstation provides operators with the on-line capability to group and sort annunciation messages from the current central annunciation displays or historical annunciation logs. With this capability, annunciation message information can be customized on-line to better support specific control room tasks. For example, following a trip, one view of the annunciation log could show only those messages associated with safety system trip parameters, thus providing a concise indication of the first-out trip parameters.

In addition, electronically linking annunciation messages with support information such as response procedures can improve and shorten the time currently required to access and search paper-based manuals for the relevant support information.

B. Central Annunciation Message List Displays

Improvements to the central annunciation message list displays were achieved in three distinct areas:

- processing - automated information processing by the system to improve the context and relevance of alarms,
- presentation - display of alarm information to support operator perception, discrimination, interpretation, diagnosis, decision-making and actions in response tasks, and
- interaction - communication between the operator and the system to support operators attentional and physical needs.

The techniques developed in each of these areas are summarized below.

1. Processing.

Plant Mode Determination

Plant modes are regions of plant operation that are characterized by specific parameter values and/or equipment configurations. Each plant mode defines a 'context' against which the relevance and importance of individual annunciation messages can be judged. For example, four control modes representing different reactor power regions (e.g., > 65% FP, 5% to 65%, -3 decades to 5%, and <-3 decades) and two conversion modes representing turbine-generator states (e.g., generating or motoring) were used during the concept demonstration stage.

Using plant modes to establish operating contexts, the priority of annunciation messages can be assigned to best fit their importance for each specific operating context.

Prioritization by Consequence and Response

The importance (i.e., priority) of an alarm can be determined by two factors: the consequence to the plant and the type of operator response. The consequence component is determined by relating each annunciation message to a list of consequence factors (e.g., danger to people or the environment, significant reduction in generation, damage to a production component) across several timeframes. The response component is determined by relating each annunciation message to the nature of operator response and the timeframe available for response.

This approach provides a consistent and formal method for message prioritization, supports the practical assignment of different priorities for a plant condition across plant modes, and provides a framework to make use of the potential changing importance of a plant condition with time.

Relevance Conditioning

Conditioning is a temporary suppression of annunciation messages from central annunciation displays and is applied to messages that are not needed in responding to a specific situation. Conditioning can be initiated in three ways, by plant modes, events, or process and equipment states.

Event-based conditioning suppresses consequential messages based on their time of occurrence and the period that they remain active following a specific event. Events are well defined situations such as a stepback or reactor trip. Annunciation messages that are candidates for this

type of conditioning are associated with process disturbances that are normally self-stabilizing following an event.

State-based conditioning suppresses consequential messages based on their occurrence as a result of a specific process or equipment state. Annunciation messages that are candidates for this type of conditioning remain active for as long as the causal process or equipment state remains valid and are generally not needed by operators to assist in responding to the process or equipment state.

Expected-but-not-occurred Message Generation

During plant operation, many status annunciation messages are generated as a result of automatic actions in response to changes in equipment states or events. Operators need to be aware that these actions have taken place, because, in general, operator intervention is needed should a missing action not occur. If the required action fails to occur, current annunciation systems do not alert operators to the failure.

This annunciation component alerts operators to failures in automatic actions that could occur following an event or change in equipment state, by generating an annunciation message specific to the failed action.

Rate and Margin Message Generation

The purpose of this annunciation component is to provide advance warning of conditions that can lead to upsets or operating difficulties by including rate and margin calculations for more plant parameters. There are many instances where operators must make judgments of this type from the observation from trend displays or a time-sequence of digital values. However, it is well known that humans do not accurately judge rates or margins on a quantitative basis in real-time. This annunciation component should assist control room staff by standardizing rate and margin determinations in support of plant operations.

Dynamic Thresholding of Annunciation Setpoints

The annunciation threshold value for many plant parameters is ideally a function of the operating context. For example, the alarm threshold for low boiler level annunciation is a function of reactor power. At present, this capability is applied to a very limited extent in current CANDU plants. Application of this technique on a more widespread basis is expected to improve the detection of

conditions requiring operator attention while reducing the occurrence of irrelevant annunciation messages.

Similar Message Coalescing

Coalescing is a technique that combines the presentation of annunciation messages concerning several similar changes in plant processes or equipment status into a single summary message thus reducing the number of messages annunciated to operators. Two types of coalescing have been defined.

Aggregate coalescing involves the use of a single message to convey the current status of a plant parameter where the parameter state is indicated by multiple sensor values. This form of coalescing is appropriate for reducing the number of messages from systems with channelized sensors.

Generalized coalescing involves the use of a single message to convey a higher-order state or fact derived from the individual values of several plant parameters. This form of coalescing is appropriate for presenting summary information that operators would be required to deduce from the observation of a group of similar messages.

Signal Validation

Signal validation is a term used to describe a number of techniques that can be applied to ensure the integrity of individual plant signals. CANDU plants currently employ several techniques such as median selection to improve the tolerance of parameters used in control system algorithms to individual sensor noise or failure.

To support the plant mode determination and cause-consequence conditioning algorithms, additional signal validation techniques beyond increasing signal redundancy may be needed to provide the required level of signal assurance. Initial examination has identified that a combination of the analytic redundancy and parity space techniques could provide a practical approach to improving signal validation for key plant parameters.

Chatter Filters

Alarm chattering is a potential source of alarm flooding. It occurs when an annunciated condition oscillates between states repetitively within a short time cycle (e.g., several minutes). Several techniques have been developed and implemented in current CANDU plants to deal with message chattering in annunciation message list

displays (e.g., the use of deadbands on annunciation thresholds, and dither filters). These techniques are effective in managing message chattering but they result in less accurate information being presented to operators via annunciation displays concerning the changes in the plant.

Message chattering itself may not necessarily be a problem, but the effects that message chattering cause in terms of audible annoyance and message list flooding with current central annunciation implementations are a problem. Through fundamental changes in the way operators are alerted to changes in alarm state and how the state of each message is presented, the main annoyance of chattering conditions can be eliminated from the central message list system. Consideration is being given to continuing with the use of a form of chatter filter should the storage and recall of alarms in history be affected by an increased volume of messages.

2. Presentation.

Separation of Fault and Status Information

Current CANDU central annunciation displays combine all messages into a single pseudo-chronological list. Operators must mentally sort and track the two basic types of information contained in these lists (i.e., fault and status indications) to support the real-time tasks of determining the fault state of the plant and maintaining an awareness of non-fault changes to the plant configuration.

By providing separate displays for these two message streams, operators no longer have to mentally sort messages. In addition, messages in each display can be presented in a way that is most meaningful to the tasks they are associated with. For real-time upset management, operators are more concerned with the state information conveyed by fault and status messages than their relative sequence of occurrence. Tasks (e.g., some aspects of diagnosis which do not require fast response) which may require relating the relative sequence of occurrence of fault and status messages can be supported by alternative displays that combine both information streams.

Colouration of Messages by Priority

Colour is used for two purposes in current CANDU annunciation messages. Most of the message is presented in a colour that reflects the major system the message is affiliated with. The first character of the message indicating the annunciation state (i.e., active or cleared) is coloured to indicate the message priority/category grouping. In practice, the single character priority

indication is visually swamped by the system affiliation colour indication.

Assigning the message priority colour to the full message has been shown to be much more visually effective in conveying message importance.

Full Text Messages

Current CANDU messages are limited to 40 characters by display hardware. Within the message only 19 characters are available to explain the annunciated condition as the remaining 21 characters are used for the message state, basic system index, and computer address fields. As a consequence, past designers have employed acronyms and abbreviations to convey overall message meaning. Interpretation of messages of this type presents an additional mental burden for operators and increases the likelihood of interpretation errors. International experience with annunciation message systems has identified the same concerns for system performance.

Presenting annunciation messages in full message text (i.e., limited use of acronyms and abbreviations) should improve interpretation and readability.

One-step Access to Supporting Information

Current CANDU annunciation messages contain basic system index codes that provide indirect links to operating manuals and flowsheets where detailed information and response procedures associated with the annunciated condition can be found. This support information is currently provided in the control room in paper-based manuals. Searching for the relevant information for a single alarm, either on a flowsheet or operating manual typically requires from one to several minutes.

Electronically linking annunciation messages with support information such as annunciation response procedures can improve support material access and use in executing response tasks. A display for the selection of alarm messages and subsequent presentation of message detail will be provided on the operator's console in future CANDU plants.

3. Interaction.

Single Button Operator Interaction with Annunciation

Several studies have identified that the need for several manual actions to interact with every message that is annunciated can be counterproductive during upset response. The management of these responses for every

message creates a burden of secondary tasks that divert mental and perceptual resources from the primary upset management tasks.

By introducing a single tone for audible alerts, the requirement for a horn silence response is removed. In addition, the acknowledge and reset functions can be effected through a single button.

Interaction Only for Fault Messages of Highest Priority

A further way to reduce the burden of secondary tasks in attending to annunciated conditions is to remove the need to acknowledge every fault message. In practice, low priority messages are only noted and not acted upon if higher priority fault messages are active and operators are already attending to the annunciation displays. Thus, there is no strong need to require operators to acknowledge every fault message. Such an approach reduces the need for operator interaction with the annunciation system overall and maintains an essential message acknowledgment feature that is adjusted to message priority.

No Interaction Required for Status Messages

Status messages indicate non-fault changes in the plant's configuration state. In almost all cases, these messages provide feedback to the operator to assist him/her in diagnosis and decision-making associated with managing overall plant operation and correcting fault conditions. For most messages, there is no action required beyond mentally noting the condition has occurred.

While there still is a need to bring these messages to an operator's attention, there is no strong need to require him/her to physically attend to each message via a manual acknowledgment action. Removing the need to manually attend to each of these messages frees up an operator's mental resources to focus more on the upset management task.

CONCLUSION

Six prototypes incorporating many of the design concepts presented in this report were developed and successfully demonstrated at CANDU stations during 1993 and 1994. Station staff have indicated that the proposed approach could address many of the problems associated with current annunciation systems, resulting in a potential savings of over \$2 million a year per unit in reduced unforced outages.

Future work will help to quantify the benefits of individual components of the strategy, identify concepts

that may be most practical, useful, and feasible for implementation for each CANDU station, and establish phased implementation approaches specific to interested stations.

REFERENCES

1. J.M. O'Hara and W.S. Brown "Nuclear Power Plant Alarm Systems: Problems and Issues," *Proceedings of the Human Factors Society 35th Annual Meeting*, pp. 1233-1237, Human Factors Society, San Francisco, California (1991).
2. E.C. Davey, K.Q. Guo, S.A. Russomanno, J.R. Popovic and P. Archer "Towards Defining the Functional Role for CANDU Annunciation," *Proceedings of the IEEE Fifth Conference on Human Factors and Power Plants*, IEEE, Monterey, California, 1992.
3. E.C. Davey, E.J. Sheehy and T.T. Fiegel "Characterizing CANDU Annunciation Through Task Analysis", *Proceedings of the American Nuclear Society Winter Meeting*, ANS, San Francisco, California, 1993.
4. D.B. Reeves, J.J. McCarthy and K. Malyon "An Upset Response Strategy for the Point Lepreau G.S. CANDU 600," *Proceedings of the Canadian Nuclear Society Conference*, CNS, Montreal, Quebec, 1994.
5. D. Boulay, R. Dufresne and R. Pageau "Abnormal Event Management - Gentilly-2 Approach," *Proceedings of the Canadian Nuclear Society Conference*, CNS, Montreal, Quebec, 1994.
6. A.D. Swain and L.M. Weston "An Approach to the Diagnosis and Misdiagnosis of Abnormal Conditions in Post-accident Sequences in Complex Man-machine Systems," Part of *Task, Errors and Mental Models*, L.P. Goodstein, H.B. Andersen and S.E. Olsen editors, John Wiley & Sons, New York, New York, 1988.
7. J. Rasmussen *Information Processing and Human-Machine Interaction - An Approach to Cognitive Engineering*, Elsevier Science Publishers, Amsterdam, The Netherlands, 1986.
8. W.B. Rouse "Models of Human Problem Solving: Detection, Diagnosis, and Compensation for System Failures," Part of *System Design for Human Interaction*, A.P. Sage editor, IEEE Press, New York, New York, 1985.